Unclassified **DSTI/ICCP/IIS(2005)1/FINAL**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development **02-Dec-2005**

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/ICCP/IIS(2005)1/FINAL
Unclassified

Working Party on Indicators for the Information Society

SCOPING STUDY FOR THE MEASUREMENT OF TRUST IN THE ONLINE ENVIRONMENT

English - Or. English

JT00195481

Document complet disponible sur OLIS dans son format d'origine
Complete document available on OLIS in its original format

FOREWORD

This report was presented to the Working Party on Indicators for the Information Society (WPIIS) in April 2005 and to the Working Party on Information Security and Privacy (WPISP) in May 2005. It was recommended to be made public by the Committee for Information, Computer and Communications Policy (ICCP) in October 2005.

The report was prepared by Sam Paltridge, Sheridan Roberts and Brigitte van Beuzekom of the Economic Analysis and Statistics Division of the OECD's Directorate for Science, Technology and Industry. The authors wish to thank colleagues in the Division for Information, Computer and Communications Policy and delegates of the WPIIS and WPISP for their contributions.

The report is published under the responsibility of the Secretary-General of the OECD.

Copyright OECD, 2005.

Applications for permission to reproduce or translate all or part of this material should be made to:

Head of Publications Service, OECD, 2 rue André-Pascal, 75775 Paris Cedex 16, France.

TABLE OF CONTENTS

INTRODUCTION

A fundamental element in enabling the benefits ICT can bring to economic and social development is the confidence users have in platforms, applications and services. Creating an online environment which builds trust amongst the users of ICT networks is an increasing priority for business, industry and governments and has been on the OECD agenda since the late 1990s.[1] The aim of this report is to undertake a review of the data available from official, semi-official and private sources which can assist in informing developments and progress in this area. There is a need to be able to use relevant data to assess the effectiveness of public and private initiatives aimed at building trust among users. This is increasingly important as access to, and use of, the Internet continues to grow across the OECD area.

At the close of 2003 there were 260 million fixed access Internet subscribers – a figure which was up from just over 100 million in 1999.[2] With multiple users of each of these accounts, in homes and businesses, the number of people accessing the Internet was, of course, much greater. By the end of 2003, nearly a third of all subscribers used broadband platforms to access the Internet, thus enabling connections with higher performance and "always on" capabilities. This proportion is expected to increase rapidly over the next few years. In addition, the first high speed platforms for cellular wireless access have been introduced and are expected to further increase access to and use of the Internet.

As ICT networks develop, the new capabilities create an increasing range of opportunities and challenges. The always-on connectivity enabled by broadband access, for example, increases the need for home and small business users to protect their connections with tools such as firewalls that were once only in the domain of corporate networks. Moreover, the higher performance of broadband means that compromised systems have a greater capability to harm those of others. One example is the emergence of so called, "botnets". This phenomenon occurs when a number of compromised machines act in concert, without the knowledge of their owners, to inflict harm on the connections of other users or to retransmit spam. A host of other threats exist and include: "phishing", "spyware", viruses, various forms of "spoofing" and "Web page hijacking". On the other hand, broadband connections enable the ICT industry to provide continuously updated and improved technologies, direct to users, to prevent harm to, or misuse of, their systems. The automatic updates to preventative technologies such as firewalls and anti-virus software, that always-on connectivity facilitates, are cases in point.

OECD governments have agreed on a number of initiatives aimed at building a culture of trust and security. At the international level, examples include the OECD's *Security Guidelines*, *OECD Policy and Practical Guidance for Online Privacy* and the *OECD Guidelines for Consumer Protection in the Context of Electronic Commerce*. The private sector has also been active. Numerous initiatives have been put into place from partnerships such as the Anti-Phishing Working Group through to the implementation of tools that aim to build trust directly with users such as privacy statements, trust marks and secure servers.

This report reviews the available statistical resources that can throw light on these issues and aims to contribute to further development of relevant statistics. On the latter point, it needs to be borne in mind that there will always be practical limitations in terms of the number and nature of indicators which can be collected by official statistical agencies. The topic of ICT generates many claims for information across a range of areas. Trust, while very important, "competes" for inclusion against other important areas requiring ICT-related information.

To date, the main approach of official statistical agencies has been to gather data from surveys of households and businesses on the use of ICT. In this context, information about trust is often collected, for example, by specific questions on IT security or on perceived "trust" barriers to Internet use or Internet commerce. The value of this information is rooted in the traditional strengths of national statistical offices which include: transparent and well defined methodologies, integrated conceptual frameworks, large sample sizes and relatively high response rates.

A range of government agencies also collects data which are relevant to informing questions about trust and security. In particular, these can include law enforcement and consumer protection agencies. These data are generated by the routine work these agencies engage in, surveys they undertake, or other mechanisms they have created for business and consumers to report incidents. Measuring e-crime is a growing area of activity, particularly crime related to identity theft.

The publication of data measuring the security of information systems and networks operated by governments, while few, are increasing. The Federal Information Security Management Act (FISMA), of 2002, requires security assessments and a continuing cycle of risk assessment in all Federal agencies in the United States.[3] The United States General Accounting office (GAO) regularly reports on implementation and provides data in this respect.[4] In Canada, under the Government Security Policy (GSP), Federal Departments are required to conduct active monitoring and internal audits of their security programs, and report the findings to the Treasury Board of Canada Secretariat. In the Netherlands, the Ministry of Economic Affairs publishes a number of more general quantitative and qualitative benchmark studies regarding the trends in the ICT sector, including e-security, (*e.g. Netwerken in cijfers* (TNO) and the Digital Economy (Statistics Netherlands)). Furthermore, the TNO published in March 2005 a study commissioned by the Ministry of Economic Affairs aimed at finding indicators that could support the Ministry in its task of policy making in the field of e-security. In Finland, the Ministry of Finance publishes an annual review of ICT use within the Government including a range of indicators on network and service security among its agencies.

The private sector is often best placed to generate data that can inform questions on trust and security in respect to business and other users. This grouping could also include not-for-profit bodies that receive funding from government and are tasked with Internet security. One reason for this is that, by its very nature, the Internet enables data on incidents to be communicated directly to providers of tools such as firewalls and anti-virus software. One of the strengths of these data is that they are automatically generated and can be made available in real-time to the users of these products via vendors' Web sites. On the other hand, the information collected may, in some cases, only reflect the situation of customers of a specific firm. This may, therefore, only permit limited conclusions to be drawn from these data in respect of the entire market. Technologies with enhancements such as Web browsers which aim to share information between users on threats, such as fraudulent Web sites, can also generate real-time information on trends in respect to security.

Private sector companies and government agencies also play a role through the creation of associations which sponsor or pool statistics from their own domains. Examples are the Anti-Phishing Working Group in the United States and the Association for Payment and Clearing Services (APACS) in the United Kingdom.

This report is in two parts. The first part deals with official statistics and the second with private and semi-official sources. The Annexes show examples of available data and references to other sources. For the future, OECD work on measurement of trust in the online environment could be developed along several lines. One approach is to continue to periodically revise the questions in the OECD model surveys of ICT use by business and households, of which this report contains the latest proposed revisions, and encourage their adoption by member countries in their own surveys. For many countries that would still

leave a potential gap in respect to the evaluation of issues surrounding trust, related to the online use and supply of government services, in the public sector.

The OECD Public Governance and Territorial Development Directorate's (GOV) survey of e-government is one potential source of information but this is limited to countries undergoing peer reviews and for the year in which such studies are undertaken. A further limitation is that issues surrounding trust, while undoubtedly of high importance, compete with other areas of high policy interest in such surveys. A potential alternative is a model survey of ICT supply and use aimed at the public sector. This would, however, need policy makers to identify those areas of trust they view as having the highest importance for measurement in the public sector, the development of a model survey and for a country or countries to volunteer to test the questions. It should be noted that National Statistical Offices have cited difficulties in collecting ICT related information from government organisations. The main difficulties are: defining government units and the heterogeneity of those units, for instance, differences in how ICT functions are organised and changes in organisational structures over time. These factors make it very difficult to make a valid comparison of data across regions, tiers of government and time.

Few OECD countries currently measure issues surrounding trust in relation to the public sector. One exception is Canada which asks about the existence of a privacy statement on organisations' Web sites and makes data separately available for the public and private sector. Another example comes from Hungary. From 2003, the Hungarian Central Statistical Office enhanced its survey of government organisations (state administration and municipalities) to include questions on ICT usage; IT security; number of online public services with integrated back-office processes; and public procurement processes that are fully carried out on line. The Hungarian survey also includes questions on computers (number, age, value), ICT training and ICT investment in the public sector.

One of the conclusions which can be drawn from the data gathered together in this report is that the direct economic costs of phenomena related to trust, such as security and privacy, are growing rapidly. The available evidence all points toward a large increase in e-crime, such as identity theft or online fraud, as being inextricably linked to the rise in ICT use. The literature on the economics of trust is relatively new but a developing field and one which could benefit from work involving member countries.[5] Moreover, much of the statistical data which are available from non-official sources on, for example, the economic cost of incidences (*e.g.* viruses or denial of service attacks), do not have transparent and well-documented methodologies. Notwithstanding this, they are frequently the premise of broader national or international estimates that are used to make demands on public and private resources.

A first step in improving data availability would be to seek international agreement on definitions of concepts, such as e-crime or security, where work is underway in some official statistical agencies. One option could be to hold an OECD workshop or expert group meeting, at a future date, in respect of the measurement of trust. Such a workshop could bring together representatives from official statistical agencies together with existing entities, such as law enforcement, consumer protection agencies and the private sector, working in this area. A goal of the workshop could be to build on existing experience and develop an internationally agreed definition of concepts related to trust in the online environment.

PART 1: OFFICIAL STATISTICS ON TRUST IN THE ONLINE ENVIRONMENT

Introduction

The topic, trust in the online environment, is a broad one and includes: IT security, privacy and trust issues such as consumer protection. Its measurement can be considered in terms of these three sub-topics. However, in practice most of the work in official statistics has been in the area of IT security, with some barriers data also collected on concerns relating to privacy and trust.

IT security

IT security is a challenge both for Internet users and for those measuring ICT use. In official statistics, it is generally considered as a demand-side measurement issue and questions may be included in the household and business ICT use surveys undertaken by many OECD countries. For businesses, the usual measurement approach is to include questions in a survey of business ICT use or a separate IT security enquiry directed at businesses. For households, questions are typically added to a household ICT use survey.

Questions on IT security usually deal with respondents' encounters with IT security problems, their origins or consequences, and preventative measures in place. For businesses, financial cost might also be asked about. Additionally, in both household and business surveys, IT security is often included as a response item on questions about barriers to e-commerce and Internet access.

Other trust issues

Issues related to trust that go beyond security are less often the subject of official statistics. However, there are some data on businesses' confidence-building practices from countries which conduct Eurostat's *Community Survey on ICT Usage and E-commerce* and Statistics Canada from its *Electronic Commerce and Technology Survey*. There are also data from a number of countries on privacy and trust concerns as impediments to e-commerce and Internet access. Household questionnaires may include items on concerns about privacy or about children accessing the Internet.

Official statistics on trust

Business surveys of ICT use

Questions are asked by several countries including Australia, Canada, Japan and those of the European Commission (via the Eurostat model questionnaire).

The Eurostat questionnaires for 2004 and 2005 have a number of questions on IT security and other trust topics. They are:

- Internal security facilities in place.
- Communication via digital signature, etc.
- Updates to security facilities in the last three months.

- Whether ICT security problems were encountered in the last 12 months and, if so, what those problems were.

- Barriers and limitations to Internet selling ("security problems concerning payments" and "uncertainty concerning legal framework for Internet sales (*e.g.* contracts, terms of delivery and guarantees))"; and

- Confidence building practices for Internet-commerce ("use of trustmarks", "alternative dispute resolution mechanisms (resolution via an impartial outsider)" and "customer service/complaints mechanisms").

Some individual European countries, such as Denmark and Norway, have more detailed questions in their national surveys. For instance, Denmark (2004) asked several questions on IT security, including:

- IT security measures in use.

- Whether they have been updated in the previous three months.

- Whether it is possible to communicate with the business using digital signature/PIN, etc.

- Where the business has obtained information about IT security; and

- The extent to which the business has experienced a number of specified problems (*e.g.* unauthorised access to systems or data).

Australia (in 2002-03) asked five IT security questions. They were:

- IT security measures in use.

- Experience of particular IT security incidents.

- Where such incidents originated (internal, external).

- Consequences of those incidents; and

- To whom the incidents were reported.

Australia also has a barriers to Internet selling question which includes a response category "security concerns".

Canada (2003 and earlier) asked whether the business' Web site is secure and whether it has a privacy policy statement. Canada has a barriers to Internet commerce question which includes the response category "security concerns".

Japan's Communications Usage Trend Survey for Enterprises (2003) has questions on:

- The harm done in relation to networks.

- Measures taken to protect the security of data and networks.

- Frequency of update of virus definition files; and

- Measures taken to protect personal information.

It also has a question on problems associated with use of computer networks which includes items on IT security and other concerns, and a similar question on the problems associated with electronic commerce.

Dedicated surveys of IT security

The US Census Bureau conducted a pilot *Computer Security Survey* in 2001 and found that the information was generally available but was difficult to collect because of low response rates. The survey was very detailed, including questions on infrastructure, embezzlement, fraud, theft of information, denial of service, sabotage, viruses and similar attacks, networks affected and reporting of incidents.[6] Data were not published from the survey because of low response rates.

Household surveys of ICT use

Questions are also asked of households but the coverage is less extensive than for businesses. European Commission countries (via the Eurostat model questionnaire), Japan and the United States ask questions in this area.

The Eurostat questionnaire for 2005 has questions on IT security and other trust topics. They are:

- Protection of the Internet access device used at home (virus checking program and firewall).
- Updates to home protection security.
- Individual use of online authentication (password, PIN or digital signature).
- Security problems encountered by individuals (*e.g.* computer virus, fraudulent payment); and
- Three barriers questions with trust items, one directed to households (why the household does not have Internet access) and two to individuals (limitations and barriers to purchasing over the Internet).

The three barrier questions have also been retained in the 2006 questionnaire. The other questions, however, have been omitted with Eurostat citing collection difficulties.

Japan's Communications Usage Trend Survey of Households (2003) has a number of questions on trust. It asks about:

- Harm incurred by Internet users in the last 12 months, including: virus infection, nuisance e-mail, unauthorised access and slander on the Web.
- Counter-measures taken against computer viruses or unauthorised access, including: anti-virus software, back up files and data, and use of a firewall.
- A barriers question on Internet purchasing which includes several trust categories, such as "I am concerned about disclosure of credit card information"; and
- A barriers question on areas of dissatisfaction for both Internet users and non-users.

In 2003, the United States took a different approach, asking about perceptions of Internet security: perceptions on level of concern about providing personal information (comparing Internet and telephone)

and concern about material children are exposed to on the Internet (compared with television). In the comparison with telephony, 49.8% of all respondents were more concerned about providing information over the Internet. Some 42.4% felt about the same and only 7.8% were less concerned in providing information over the Internet than the telephone (Annex 1, Table 1). In the comparison with television 70% of all respondents were more concerned about children's exposure to material on the Internet (Annex 1, Table 2).

Examples of official data

Annex 1 of this report includes some of the available IT security data collected and published by: the Australian Bureau of Statistics (Business Use of Information Technology Survey), Statistics Canada (Electronic Commerce and Technology Survey), Eurostat (Community Surveys on ICT Usage and E-commerce), Japan (Communications Usage Trend Survey) and the United States Census Bureau (Current Population Survey, Computer and Internet Supplement).

Future developments: the OECD model surveys of business and household use of ICT

Business model survey

The OECD model survey of ICT use by businesses is currently being revised, with changes expected to be finalised during 2005. It is proposed to add a separate module on IT security measures which businesses have in place (at the end of the reference period) and IT security incidents experienced (during the reference period). This follows from similar collection activities by member countries, as described above.

In addition, a question has been proposed on whether the business' Web site has: a security policy statement, a privacy policy statement, a security seal or a privacy seal.

Barriers questions in the existing model include items on security. The revised model survey has only one barriers question (on e-commerce) and that includes items on security, privacy and trust (refer Annex 2 for details).

The model questions have been reproduced at Annex 2 along with a summary of comments received from member countries on those questions and potential further topics.

Household model survey

The OECD model survey of ICT use by households/individuals is also being revised, with changes to be finalised in 2005. It is proposed to add three new (non-core) questions on IT security topics.

Barriers questions including items on security and privacy currently exist in the model survey and will be retained.

The proposed model questions have been reproduced at Annex 2 along with a summary of comments received from member countries on those questions and potential further topics.

PART 2: STATISTICS ON TRUST IN THE ONLINE ENVIRONMENT FROM SEMI-OFFICIAL AND PRIVATE SOURCES

There is a growing body of statistics from semi-official and private sources in areas related to trust in the online environment. Semi-official is the term here applied to statistics from government and its agencies but excluding national statistical offices. Private sources include all other data which do not fall within the categories of official or semi-official. This includes, for example, industry statistics generated by companies providing services and applications such as anti-virus software. Data from both semi-official and private sources can take the form of surveys of users of ICT professionals, consumer complaints, crime or fraud statistics as well as a range of *ad hoc* statistics generated by industry or the Internet community on specific phenomenon affecting trust in the online environment. The following sections endeavour to provide an overview of available data by way of examples from across the OECD area.

Perception, opinion and usage surveys

Several surveys have been undertaken in recent years by semi-official and private entities in relation to trust in the online environment. Two of the leading endeavours in this area have been undertaken by the European Commission (2004) and the other for the United States by the Pew Internet & American Life Project (2000). The OECD's GOV Directorate survey of bodies within the public sector delivering e-government services is another example. The OECD's GOV Directorate survey of bodies within the public sector delivering e-government services, which is conducted as part of its peer reviews of national e-government programmes, is another example. The OECD survey is one of the few that surveys perceptions in the public sector, on an international basis, in relation to trust.

The OECD GOV Directorate E-Government Survey

The OECD's Public Governance and Territorial Development Directorate identifies changing societal and market needs, and helps countries adapt their governmental systems and territorial polices. GOV supports improved public sector governance through comparative data and analysis, the setting and promotion of standards, and the facilitation of transparency and peer review. As part of this process GOV conducts peer reviews of member countries' e-government programmes (Mexico, Finland, Norway and Denmark have been reviewed so far). Part of the review process involves sending a questionnaire to public sector bodies in the country being reviewed. Two questions in the survey relate directly to perceptions relating to trust in the delivery of government services in the online environment. These questions are:

- (Question 3.5) Do you think that online processes in your organisation have the equivalent level of protection as the same processes offline with regard to (a) privacy, (b) security and (c) consumer protection.

- (Question 7.4) Do the following factors constrain customer demand for the online services provided by your organisation, and if so how important are they (g) Perceived lack of online privacy protection in comparison with the same offline service (f) Perceived lack of online security protection in comparison with same offline service.

The results for Denmark are available. They show Danish officials perceive the delivery of e-government services to have the equivalent or higher level of protection as the same processes offline with

regard to privacy, security and consumer protection (Annex 3, Figure 1). They indicate the perceptions Danish officials have in respect to privacy and security being barriers to the use of e-government, as well as enabling comparisons to be made between other areas of potential constraints (Annex 3, Figure 2). In respect to security and privacy more than 60% of respondents stated that they were not currently acting as constraints to the delivery of e-government services. Just under 20% felt security and privacy were an important or very important constraint and the remainder felt they were somewhat important in this respect.

The European Commission's Eurobarometer

The European Commission has been monitoring the evolution of public opinion in the Member States since 1973. The surveys and studies, undertaken by the European Opinion Research Group, address a variety of topics concerning European citizenship: enlargement, social situation, health, culture, information technology, environment, the Euro, defence and so forth. These studies are available on the Web site for the Public Opinion Analysis sector of the European Commission.[7]

In 2003, the Directorate General for Health and Consumer Protection requested a special Eurobarometer survey on public opinion regarding e-commerce. The survey, *European Union Public Opinion on Issues Relating to Business to Consumer E-commerce* (reference: 201 EB60.0) was conducted in September 2003.[8]

This one-off study primarily assessed the EU public opinion on issues relating to e-commerce with how EU citizens perceived security on the Internet and their concerns in this regard. The survey divided respondents into two categories: those who had used Internet for e-commerce (16%) and those who had not used Internet for e-commerce (83%). Questions were then put to respondents, in the two different categories. (Annex 3, Tables 1 and 2.)

In 2003 the main reason EU citizens nominated for not making purchases over the Internet was that they did not have access to Internet (57%). Security concerns ranked only third (25%), after not being interested in buying anything over Internet (28%). By way of contrast security of payment was the leading concern of EU citizens who did have access to the Internet (48%). Other issues relating to trust included: the ability to get a refund (38%), delivery (36%), credibility of the information on Internet (27%).

Eurobarometers on security and privacy

Worthy of note in the special Eurobarometer survey were specific questions relating to security and privacy. Respondents were asked whether they had heard of "Internet trust marks", statements about the security of payments and statements about the protection of personal data. (Annex 3, Tables 3, 4 and 5.) Questions on these issues can inform policy makers of public awareness of some of the leading safeguards which are aimed at building trust.

"Internet trust marks" are seals, granted by a third party, that are affixed to e-commerce Web sites. They indicate, for example, that the online vendor has chosen SSL or other payment processing solution to protect the communication of credit card and other confidential information. The results from the Eurobarometer survey indicated that the general public had a relatively low awareness of the concept with only 10% of respondents, on average across the EU area, having heard of trust marks. From the 10% who had heard of trust marks just over half (56%) had noticed them on Web sites they had visited. Just under half (49%) of those that had heard of trust marks believed that they made Web sites more reliable. The Eurobarometer survey also asked respondents whether they were more or less likely to trust domestic or foreign trustmarks. Some 18% of those polled across the EU area said they would be more confident about

trust marks if they were not based in their own countries. Slightly more (21%), however, took the opposite view believing that "foreign" trust marks would generate less confidence.

While awareness of security statements on payments (21%) and privacy statements (24%) was higher, across the EU area, they also recorded a relatively low recognition. However, as with trust marks, greater recognition of these safeguards exists among those who have access to the Internet or make purchases over the Internet than in proportion to the total population.

A Special Eurobarometer was also undertaken in 2003 to assess the views of EU citizens on data protection.[9] At that time, the survey found that 72% of respondents had not heard of tools or technologies designed to limit the collection of personal data when using the Internet (so called Privacy-enhancing Technologies or PET). Only 6% of respondents reported using such tools. Some 30% of those that had heard of such tools and technologies but not used them said they did not believe they would have adequate skills.

Industry surveys

Surveys commissioned by industry provide a further source of information about the public perception of trust in the online environment. One example is a survey conducted by Harris Interactive, on behalf of Verisign, in September 2004.[10] According to this survey 31% of Americans cited security concerns as a key factor that deters them from doing more shopping on line.[11] Shipping costs (48%) and the inability to touch an item before buying it (46%) were nominated as the top deterrents, followed by the difficulty of returning items.[12]

While not directly comparable to the results of the Eurobarometer survey, there appears to be a higher awareness of trust marks in the United States. The Harris Interactive survey reported that 74% of people in the United States, who have ever made an online purchase, seek a trust mark when determining whether or not to make a purchase from an e-commerce site.[13] This may, however, be due to the important function of privacy notices and trust marks in the US regulatory approach to privacy. By way of contrast EU respondents may not have confidence in the functioning of the omnibus privacy legislation approach in EU member states. Another result worthy of note was that only 28% of the online shoppers surveyed by Harris Interactive, had heard of phishing.

In September-October 2004, one of the most unique surveys of the use of online safeguards was undertaken by AOL and the National Cyber Security Alliance (NCSA).[14] In this survey consumers of broadband and dial-up connections were the subject of in-person interviews after which a scan was run on their home computer. Introductory questions included asking respondents how safe they felt their computer was from viruses, hackers and online threats as well as if they used their home connection for sensitive transactions or storing sensitive information. Users were then asked questions related to their use of safeguard tools (*e.g.* firewalls, anti-virus software, anti-spyware) and their computers were then scanned to test the actual results against the responses. In some categories there were wide divergences between perceptions and the scan results. From the users with virus protection 71% said they were updated daily or weekly. By way of contrast the scan showed that 67% of anti-virus programs had not been updated in the past week. There were also wide divergences in the case of spyware in respect to what users believed was on the computers or had given permission for installation and what was found by scans. Some 53% of users surveyed thought they had spyware or adware on their machines whereas scans revealed 80% of machines had such programs installed.

One of the longest-running private surveys of consumer's views on Internet payments systems is undertaken at the University of Karlsruhe in Germany. Begun in 1998, the survey is supported by companies such as Deutsche Telekom, FirstGate Internet and WEB.DE. The most recent survey results at

the time of writing were reported in November 2004.[15] Among the questions asked is which type of entity consumers trust to be the provider of online payment systems. In 2004, respondents answered in the following order: banks (84.4%) credit card companies (59%), ISPs (17.1%), telecommunication carriers (14%), independent third parties (12.2%) and no preference (10.9%).

Industry usage surveys

An interesting question in the assessment of trust in the online environment is the extent to which users are willing to allow secondary use of their personal information in return for other benefits. One academic study undertaken in 2005, for example, held an experiment with sealed-bid auction to see what monetary value users associate with "location privacy" in respect to mobile services.[16]

A number of firms track the usage of panels of voluntary Internet users. In return these users may benefit from direct financial inducements, such as discounts, or access to services (*e.g.* free anti-virus updates). Such monitoring, sometimes called "researchware", can be a very useful commercial source of information about online usage including informing issues of trust.[17] The results are also available by country allowing international comparisons, albeit on a proprietary basis.

One emerging issue in the use of researchware is the extent to which some online businesses are willing to allow their customers to be monitored by third parties when balanced against their own security concerns. In Australia and New Zealand, for example, some banks have begun blocking users from using their online banking facilities if they have third party monitoring software installed on their computer.[18] The Banks in question have indicated that third party researchware is a breach of the terms and conditions for their Internet banking service.

The Pew Internet & American Life Project

The Pew Internet & American Life Project is a non-profit research centre studying the social effects of the Internet in the United States. In 2000, The Pew Internet & American Life Project undertook a study called *Trust and Privacy On-line: Why Americans Want to Rewrite the Rules*.[19] The results of the survey revealed a range of concerns held by Internet users, ranging from access to personal information through to interception or tracking of communications. (Annex 3, Table 6.) A comparison of results, from an earlier Pew study undertaken in 1998, showed increasing concern in respect to privacy and viruses. (Annex 3, Table 7.) The survey showed that about half of all Internet users were aware of "cookies" but only a relatively small percentage of users block their use (Annex 3, Table 8.) A "cookie" is a small data file that can be stored on a user's local computer for a multitude of different purposes *e.g.* for storing information about the user that is pertinent to a Web site, such as customising user preferences or for tracking a user's behaviour on one or more Web sites.

Consumer Reports

Consumer Reports are published by the Consumers Union, an independent consumer information and advocacy group in the United States. In August 2005, Consumer Reports published the results of a nationally representative survey of more than 3 200 households with at-home Internet access.[20] One of the findings was that one-third of respondents said a virus or spyware had caused serious problems with their computer systems and/or financial losses within the past two years. Based on the 2005 survey, Consumer Reports has begun to compile annual "State of the Net" tables aimed at assessing the likelihood and impact of four leading online hazards. The 2005 report identified, Spam, Viruses, Spyware and Phishing as the major threats, gave an assessment of whether they were getting better or worse and provided data on their incidence, average cost per incidence and total national cost.

Surveys of security professionals and law enforcement agencies

The annual Computer Security Institute and Federal Bureau of Investigation (CSI/FBI) "Computer Crime and Security Survey" is perhaps the largest and most extensive study of its type. In 2004 the survey recorded responses from 494 computer security practitioners in the United States, from corporations, government agencies, financial institutions, medical institutions and universities.[21] The survey asks participants a range of security-related questions including asking them to quantify losses related to different types of incidents. In 2004, from a total of USD 141 million reported by respondents, viruses and denial of service attacks were responsible for the largest losses. The CSI/FBI survey asks respondents to quantify security expenditure as a percentage of their total IT expenditure. In 2004, 46% of respondents reported that their organisations allocated between 1% to 5% of their total IT budgets for security. The survey also reports a range of indicators including security expenditure per employee, total amount of security outsourced and whether organisations evaluate the return on investment from security expenditure.

The E-Crime Watch Survey is conducted among security and law enforcement executives by CSO magazine in co-operation with the United States Secret Service and Carnegie Mellon University Software Engineering Institutes Computer Emergency Response Team (CERT) Coordination Center. Respondents to the 2004 survey reported "e-crime" losses of USD 666 million for 2003.[22] The survey also asks respondent to try to quantify losses by their area of impact in areas such as operation losses, financial losses and so forth. In the 2004 results the survey noted that 32% of respondents did not track losses due to e-crime or intrusions and of those that do track this measure around half do not know their total losses.

In 2005, the United States Department of Homeland Security and the Department of Justice plan to survey 36 000 businesses to examine the type and frequency of computer security incidents. The goal of the survey is to improve data on cybercrime to assist policy analysis for government and the private sector and provide statistically relevant national data on cybercrime across all businesses in the United States, especially those in critical infrastructure sectors.

In Australia, AusCERT undertakes an annual "Computer Crime and Security Survey", adapted from the CSI/FBI survey of the same name.[23] This allows comparisons between trends for the two surveys. The survey is sent to security professionals in Australia's 350 largest enterprises (including government and educational institutions). In 2004 there were 199 responses (83%). The results of this survey include quantified time and financial losses stemming from computer crime. In 2004, the total losses reported by respondents were USD 12.6 million compared to just under USD 5 million in 2002.

In the United Kingdom, the Department of Trade and Industry, sponsors the "Information and Security Breaches Survey". This survey is used to make comparisons between the experience of the United Kingdom and the results of the CSI/FBI survey in United States.[24] The National Hi-Tech Crime Unit in the United Kingdom also sponsors surveys of business on the incidence and impact e-crime.[25] In 2003 the most widely experienced computer related crimes were virus attacks and denial of service attacks. Total losses, for the 167 companies interviewed for the 2003 survey were put at USD 365 million with the largest part (62%) attributable to financial fraud. The 2004 survey of the National Hi-Tech Crime Unit estimated the total cost of e-crime to businesses in the United Kingdom at USD 4.5 billion.[26]

In Germany, once a year, monitoring is performed by the Federal Office for Information Security with a view to awareness of their products. IT security officers, data protection officers and journalists are polled in representative surveys. In 2004, "awareness monitoring" was also carried out among the target group of private PC users in this context. The results are considered within the context of project planning by the Federal Office for Information Security. Polls among experts and citizens are also planned for the future.

In Finland, the Ministry of Finance publishes an annual review on ICT use within the Government.[27] The Ministry of Finance has been undertaking these reviews since 1975 as a part of its role in steering and management of government ICT and information security. The publication consists of statistical information on the total expenditures on information technology, on information technology personnel, on information technology equipment, and on information management as well as information security in government agencies. Further information on this survey, together with the indicators available, refer to Box 1.

In Spain, the Spanish association of electronic and communications enterprises, (ASIMELEC) has undertaken a survey focused on ICT security in the telecommunications and Information Technologies in Spain.[28] The goal of this study was to analyse the level of knowledge and investment with regard to security among the Spanish IT and communications industry. The study concluded that the level of information security and awareness among businesses of the need for online security was insufficient. The study reported that that only anti-virus software and firewalls were widely used among Spanish businesses.

Industry surveys of security and ICT technical professionals provide a further source of data. Symantec, an information security firm, has undertaken a number of surveys of security professionals in respect to their own actions in regard to security and privacy. One early example was a survey of the respective use of firewalls by consumers and IT professionals.[29] A further example was a comparative study in 2004 of the attitudes and behaviour in relation to privacy of security professionals in the United States, the United Kingdom and other European Union countries.[30]

Firms such as Deloitte Touche Tohmatsu undertake surveys of security professionals in areas such as financial services.[31] Questions include whether the firms see security as an area of competitive advantage, internal reporting structures through to trends in investment levels. In the Nordic region PLS RAMBOLL Management have undertaken a survey of firms in respect to e-business.[32] Financial support for the survey includes a contribution from the Nordic Council of Ministers. In addition to questions of security the survey reports on compliance with prevailing legislation such as data protection, rules on marketing and so forth.

Box 1: **Finland's ICT use in government survey, security and trust online indicators**

Government agencies that provide information for the annual survey of ICT use include Ministries and Administrative Agencies operating within the governmental budget. In total these entities have about 123 000 persons working in 2 606 different units. In 2004 the total expenditure on ICT in these governmental agencies was EUR 588 millions. The number of full time IT personnel in these agencies, at the end of 2004, was about 4 000. The share of IT personnel in the total personnel in governmental agencies was 3%. At the end of 2004, there were 160 828 personnel computers in Finnish governmental agencies, which is 1.3 work stations per person. For customer use there were about 16 000 work stations. There were 3 433 file-sharing and printing servers. The number of multi-user database and application servers was 4 840. In 2004 the survey recorded that all organisations had a Web site, 78% offered electronic forms over the Internet and half offered public services.

The 2004 survey showed positive developments in different areas of information security in Finland among government users. Examples were found in administrative and technical information security, instructions and information security plans, co-operation between units, privacy protection, protection against attacks/viruses and contingency planning. In particular, the organisations participating in co-operational projects led by the Ministry of Finance and the Government Information Security Management Board (VAHTI) have shown significant development and impacts. This development is measured by several different indicators:

- Percent of organisations having an *information technology management plan*.
- Percent of organisations having *information security plans* as well as percent of organisations having *contingency plans.*
- Percent of organisations having *a person responsible for IT security*. Percent of organisations having this person *reporting to head management*.
- Percent of organisations having a *co-ordinating body for information security containing different units*.
- Percent of organisations having their *information security instructions* scoping all the important areas of information security.
- Percent of organisations having *the e-mail policy accepted by the Top Management and staff informed.*
- Percent of organisations having *descriptions of online registries on their Web pages*.
- Percent of organisations having the *privacy protection policy on their Web page.*
- Other indicators: *participation in international ICT security co-operation.*
- Nearly all *organisations* had an *anti-virus system in use in all computers*.
- Nearly all organisations carried out "anti-virus checks" and "virus-deletions" before delivering e-mail to users.
- Other mechanism followed: *cryptography in different areas*, IDS: *in use/planning/no.*

The survey also included questions on problems caused by IT security attacks or virus programs and so forth. Examples of these are:

- *Percent of organisations where External IT security attacks had caused special actions in the previous 12 months.*
- *Percent of organisations where, due to a virus, a system or a part of it had been out of use at some stage in the previous 12 months.*

The survey typically asks respondents to answer "in use", "planning" or "no", in relation to eGovernment and the security of interactive eGovernment applications for the following:

- Percent of organisations having their own *interactive eGovernment service in use* and percent of organisations planning these.
- Percent of organisations having *PKI-based authentication or digital signatures in use of their interactive eGovernment applications*. Percent of organisations planning this kind of services.
- Percent of organisations having *one-time password based authentication standard in use of their interactive eGovernment applications (standard used first in banking sector and currently widely in different sectors, called TUPAS)*. Percent of organisations planning to implement this kind of service.
- Percent of organisations delivering their *interactive eGovernment services to mobile user interfaces* and percent of organisations offering their customer channel to pay online in their interactive eGovernment services.

Consumer complaint and Internet fraud statistics

Consumer complaint data provides one source of data on the problems related to e-commerce. In the United States there are a number of Web site complaint centres. One of these, the Consumer Sentinel, which is maintained by the Federal Trade Commission (FTC), has an international scope and widest coverage in terms of volume of complaints. In addition, the Consumer Sentinel provides definitions of the issues it is trying to measure, something that is not always evident on other Web sites which often have little, if any, methodological information on the statistics presented. One observation, across Web sites reviewed for this study, is that that the top ranking complaint issue was almost invariably fraud related to Internet auctions and that the number of complaints filed is growing with time.

Consumer Sentinel

The Consumer Sentinel database, maintained by the Federal Trade Commission, contains more than one million consumer fraud complaints that have been filed with federal, state, and local law enforcement agencies and private organisations.[33] On line since 1997, Consumer Sentinel is aimed at sharing information to make law enforcement stronger and more effective. An international, multi-agency joint project, Consumer Sentinel also enhances cross-border consumer education and prevention efforts.

Complaints can be classified in two categories: identity theft complaints and fraud complaints. Fraud complaints can further be broken down into Internet-related fraud complaints and other fraud complaints. Internet-related fraud complaints have grown significantly in recent years increasing from 55 727 in 2001 to 166 617 in 2003 (Annex 3, Figure 3). In 2003 Internet auctions were the greatest source of fraud complaints (Annex 3, Figure 4). These data do not include identity theft, which may be perpetrated via the Internet, but for which there are no separate data. A fraud complaint is considered "Internet-related" if it concerns an Internet product or service, the company initially contacts the consumer via the Internet, or the consumer responds via the Internet.

The Consumer Sentinel also tracks cross-border fraud trends. A fraud complaint is "cross-border" if: *i)* a consumer in the United States complained about a company located in Canada or another foreign country, *ii)* a Canadian consumer complained about a company located in the United States or another foreign country, or *iii)* a consumer from a foreign country complained about a company located in the United States or Canada. Company location is based on addresses reported by the complaining consumers and thus, understates the number of cross-border complaints. In some instances the company address provided by the consumer may actually be a mail drop rather than the physical location of the company, and in other cases, the consumer does not know whether the location is in the United States or abroad. The number of cross border complaints, reported by the Consumer Sentinel, increased from 5 225 in 2001 to 21 181 in 2003 (Annex 3, Figure 5). These data are also available by location (Annex 3, Table 9).

The Internet Fraud Complaint Center

The Internet Fraud Complaint Center (IFCC) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C).[34] The IFCC's mission is to address fraud committed over the Internet. The IFCC provides a reporting mechanism that alerts authorities, in the United States, to a suspected criminal or civil violation. For law enforcement and regulatory agencies at all levels, the IFCC offers a central repository for complaints related to Internet fraud, works to quantify fraud patterns, and provides statistical data of current fraud trends. Statistics from the IFCC are available in annual Internet Fraud reports as well as reports with a special focus such as Internet auction fraud.[35] The data reported by the IFCC reflect the same trends as the Consumer Sentinel data. Incidents of Internet fraud are increasing and fraud related to Internet auctions is the largest single category (Annex 3, Figures 6 and 7).

National Fraud Information Center and Internet Fraud Watch

The NFIC was established in 1992 by the National Consumers League, a non-profit consumer organisation in the United States, to fight the growing menace of telemarketing fraud by improving prevention and enforcement.[36] In 1996, the Internet Fraud Watch was created, enabling the NFIC to offer consumers advice about promotions in cyberspace and route reports of suspected online and Internet fraud to the appropriate government agencies.

The NFIC also collects Internet fraud complaints, compiles the data and makes it available on its Web site. The total number of complaints registered by the NFIC is much lower, (37 183 complaints in 2003) than for the Consumer Sentinel and the IFCC. One reason for this is because it has a more limited geographic scope (only the United States) than some of the other complaint centres. In 2004 Internet auctions were again the major source of consumer complaints, followed by non-delivery and the so-called "Nigerian 419 advanced fee fraud".[37] Worthy of note is that phishing was ranked fourth on the list of Internet scams in 2004. It was not on the same list in 2003.[38]

Econsumer.gov

In 2001, responding to the challenges of multinational Internet fraud, and working to enhance consumer protection and consumer confidence in e-commerce, 13 countries unveiled econsumer.gov, a joint effort to gather and share cross-border e-commerce complaints.[39] By 2004 the project brought together consumer protection agencies from 19 countries: Australia, Belgium, Canada, Denmark, Finland, Hungary, Ireland, Japan, Korea, Latvia, Lithuania, Mexico, New Zealand, Norway, Poland, Sweden, Switzerland, the United Kingdom and the United States.

The project has two components: a multilingual public Web site, and a government, password-protected Web site. The public site provides general information about consumer protection in all countries that belong to the ICPEN (International Consumer Protection Enforcement Network), contact information for consumer protection authorities in those countries, and an online complaint form.[40] All information is available in English, French, German, and Spanish. Using the existing Consumer Sentinel network, the incoming complaints are shared through the government Web site with participating consumer protection law enforcers. The Web site also reports statistics including Internet-related cross-border fraud.[41]

Online retail sales, security and fraud

In Symantec's 2004 report on Internet security, e-commerce was listed as the industry most targeted by fraudsters for the first half of that year, with nearly 16% of attacks against it considered deliberate, up from 4% reported the previous six months.[42] At the time, Symantec reported that this may indicate a shift in motivation from hackers seeking notoriety to professional criminals seeking illicit financial reward. In part it may also reflect the growing use and significance of e-commerce.

While still small compared to overall retail sales, the volume of electronic commerce is increasing across the OECD area. In the United States the volume of online retail sales tripled between 1999 and 2004.[43] Data from industry sources also demonstrates an increase in e-commerce. In 2003, Europe's Visa Card holders spent more than USD 14 billion on online retail transactions which was double the previous year.[44] This represented 1.5% of total expenditure by European Visa card holders in 2003. In the United Kingdom, the Association for Payment and Clearing Services (APACS) reported in April 2004 that one in ten credit card payments are now made online.[45] During the same year APACS further reported that 22 million Internet users in the United Kingdom either make purchases or bank on line, with half of them doing both. According to APACS 6.7 million online shoppers each made an average of 6.5 purchases in

2000. By 2003, they report the number of online shoppers had tripled and that they each made an average of 11.2 purchases on line.

Little data are available publicly on the financial cost of fraud or security breaches related to on line retail activity. Visa reports, on a quarterly basis, the total amount of fraud related to all transactions made by its card holders. These data do not break out the amount related to online fraud. In June 2004, fraudulent transactions represented 0.05% of the total volume of Visa transactions in the United States.[46] This figure has consistently declined from 0.18% of total transactions in 1992.[47] MasterCard doesn't comment on specific fraud statistics. However, the company said that the fraud levels it witnessed in 2001 were at historically low levels compared with a peak in the early 1990s.[48]

Crime statistics

In some countries data are available from legal proceedings on crimes related to the use of ICT. Germany provides a case in point.[49] In that country statistics are generated by the courts based on criminal offences specified under the German Penal Code. These include offences committed in relation to ICT under the articles on spying on data (Art. 202a), computer fraud (Art 263a), falsification of evidence documents (Art. 269), alteration of data (Art. 303a) and computer sabotage (Art 303b). For the purpose of quantification the foregoing represent one way to group ICT-related offences.[50] Working with this grouping 96% of ICT crime primarily relates to computer fraud according to Article 263a of the German Penal Code. The number of convictions under this Article rose by 71% from 1 561 in 1995 to 2 670 in 2002. The other categories also recorded sharp increases during this period, but from much smaller bases.

The rise in the number of cases recorded in Germany is undoubtedly related to the expanding use of ICT and the subsequent introduction of additional services in that country. Data available from ICT Household surveys helps place the increase in abuse of ICT in the overall concerns of users or potential users. For households that are not on line, data gathered by the German Federal Statistical Office indicate that economic and knowledge-based factors are viewed as greater barriers to the use of the Internet than trust and security.[51] This does not, of course, necessarily mean that people take security and trust less seriously. It may only indicate that other factors are viewed as even greater barriers. In addition trust and security concerns may rise with knowledge and experience from use. Survey results from offline households indicated lack of need (69%) as the main reason for not having an Internet connection. Additional reasons cited included the cost of equipment or access (33% and 29% respectively) and lack of knowledge (31%). Reservations about data protection and security were cited by only 12% of offline households as the reason for not having an Internet connection.

United States government law enforcers also make data available in respect of their actions against cybercrime. One example is Operation Web Snare, an initiative of the United States Department of Justice.[52] Operation Web Snare was targeted at a variety of online economic crimes including identity theft, fraud, computer intrusions and some intellectual property crimes. More than 160 investigations were opened as part of Web Snare, which ran from June to August 2004. During this time investigators identified more than 150 000 victims with estimated losses of more than USD 215 million. More than 140 search and seizure warrants were executed as part of the operation, and prosecutors obtained 117 criminal complaints, informations, and indictments. The resulting charges led to more than 150 arrests or convictions.

Identity crime and e-crime

In Australia the Australian Bureau of Statistics (via the National Crime Statistics Unit – NCSU) and the Australian High Tech Crime Centre (AHTCC) are developing e-crime definitions.[53] A definition of e-crime proposed by this work is: *"A criminal offence where a computer or other (similar) electronic device*

is used as a tool to enable or enhance the commission of an offence, or is the target of an offence".[54] Under this defintion "enabled" refers to crimes committed directly against computers that would not exist without the use of computers. In the case of "enhanced" crimes, the defintion refers to traditional crimes that are facilitated by the use of information technology. The NSCU cite, as a primary information requirement, the need to estimate the size of e-crime in terms of economic impact (including security costs and lost time), number of incidents and number of victims. They have also recommended international collaboration for the purpose of developing standards and data collection methodologies for e-crime statistics.

There are legal definitions in respect to identy crime (*i.e.* identity theft and identity fraud) in a growing number of OECD countries.[55] There are also some data on identity crime but they contain large differences, in the orders of magnitude relative to the size of the economies concerned, suggesting variations in the defintions used. The FTC, for example, has calculated the cost of identy theft in the United States, for consumers and businesses, at around USD 50 billion in 2003.[56] In the United Kingdom the annual cost to the British economy of identy theft has been put at USD 2.5 billion per annum.[57] Estimates also range widely within countries. In Australia, in the absence of authoritative statistics on the cost of "identity fraud", estimates range from under USD 1 billion (Securities Industry Research Centre of Asia-Pacific) to more than USD 3 billion per annum (Commonwealth Attorney-General's Department).[58]

There are very little data available on the proportion of financial losses coming under the heading of identity crime that are attributable to e-crime. In the United States the Federal Deposit Insurance Corporation (FDIC) say the losses steming from "account hijacking" (*e.g.* using information gained from phishing, spyware and so forth) is believed to be a relatively small part of the overall cost of identity theft.[59] That being said, the FDIC notes there is a reluctance on the part of financial institutions to publish losses in the belief that the public relations problems associated may generate worse financial losses. The FDIC also cites separate surveys by Gartner, a private information technology research firm, and the American Bankers Association which rank the Internet as one of the prime sources for indentity theft. The FDIC also points towards the threat of identidy theft in relation to undermining trust in e-commerce.

European Network Information and Security Agency (ENISA) and other European country security initiatives

In Europe, the European Network Information and Security Agency (ENISA), a new European Union agency, was set up in March 2004 to "help deliver high EU-wide standards of security in electronic communications, and to build the "culture of security" necessary for the single market to deliver its full benefits to European citizens, consumers, enterprises and public sector bodies." [60] Ensia's remit also includes collecting and analysing data on security incidents in Europe and emerging risks.[61] ENISA plans to publish reports, assessments, recommendations, results of studies, views and other documents of public interest regarding the Agency's field of activity.[62]

Governments in a number of European Countries have set up Web sites to increase awareness of ICT security. In the Netherlands, the National Alerting Service aims at providing individuals and SMEs with timely information with regard to security related incidents.[63] The National Alerting Service does this by distributing early warnings and alerts. The National Alerting Service has been commissioned by the Ministry of Economic Affairs, and resides within the Computer Emergency Response Team for the Dutch government. In the United Kingdom "Itsafe" is a government service, aimed at providing both individual users and SMEs with advice to help protect computers, mobile phones and other devices from malicious attack as well as activities such as phishing.[64] In Australia the Australian High Tech Crime Centre (AHTCC) performs similar functions.[65] The OECD's Culture of Security Web site contains links to such Web sites across the OECD area.[66]

Selected Internet threats/attacks/incidents and data availability

Phishing and pharming

Phishing is the term applied to the use of "spoofed" e-mails and fraudulent Web sites which are designed to deceive users into revealing personal information. Examples of the type of information sought by "phishers" include credit card numbers, account names, passwords, personal identification numbers and so forth. This information is then used by the phishers to conduct fraudulent activities both online and offline.

The most common form of phishing is for a user to receive an e-mail with a "spoofed" address. Spoofing is a term applied to any falsification of an Internet identifier such as an e-mail address, domain name or an IP address. In the case of e-mail the header is forged to indicate it originated from somewhere other than the actual source. Pharming uses the same kind of spoofed identifiers, but uses in addition malware/spyware to redirect users from authentic Web sites to the fraudulent sites that replicate the original in appearance (typically through DNS hijacking or cache poisoning).[67] Spoofing may also be emerging in relation to phishing via Internet telephony.[68]

In a phishing attack the deception will generally involve substituting the name of a trusted party (*e.g.* name of a bank) in place of the true identifier. For example, a user might receive an e-mail from support@phisher.com which would outwardly appear to the user as an e-mail from support@yourbank.com. The phishing e-mail would then attempt to lure the user to a fraudulent Web site that may in turn imitate the legitimate "yourbank" Web site.[69] The user would then be encouraged to divulge sensitive information directly or, in the case of an unprotected PC, unwittingly transfer malicious code that will subsequently generate a transfer of information. A so-called "Trojan horse", for example, can potentially record account names and passwords when users next attempt to log on to a legitimate site by monitoring keystrokes.[70]

Phishing statistcs

The most authoritative set of data on "phishing" is produced by the Anti-Phishing Working Group (APWG).[71] The APWG is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and e-mail spoofing. The APWG has over 1 100 members being comprised of more than 700 companies, 8 of the top 10 banks in the United States, 4 of the top 5 Internet service providers in the United States and more than 100 technology vendors. Also among the members of the APWG are law enforcement agencies from Australia, Canada, the United Kingdom and the United States.

The APWG makes a wide range of data available on categories such as:

- Number of unique phishing attacks reported in December 2004 (1 707).
- Average monthly growth rate in phishing attacks July through December 2004 (24%).
- Countries hosting the most phishing Web sites in December 2004 (Annex 3: Table 10).
- Number of brands hijacked by phishing attack in December 2004 (55).
- Contain some form of target name in URL (24%).
- Average lifespan of a phishing site (5.9 days).

- An estimate that some 75 million to 150 million phishing e-mails are sent every day on the Internet (Spam filters and other technologies mean that the majority of these messages do not ever reach consumers). [72]

Data on phishing Web sites may become increasingly available from tools designed to guard against suspicious activity. A number of ISPs and security companies, such as Earthlink and GeoTrust, now offer toolbars which identify phishing sites (and block them) or authenticate actual sites.[73] eBay has also introduced a free toolbar for buyers. Among the services offered by the "Account Guard" toolbar are warnings that are triggered when users are on a potentially fraudulent Web site.[74] In addition, Microsoft has announced it plans to incorporate anti-phishing safeguards into future versions of Internet explorer.[75] A common factor between such tools is that they can report usage data back to their creators and, therefore, allow the sharing of non-personal data among users.

Netcraft, a security company based in the United Kingdom offers a free toolbar which provides detailed information to its users and signals when caution is required. Netcraft's tool compares information from their ongoing surveys of the Internet against the information known about a specific Web site. For example, if a user visited a Web site purporting to be their local bank but the site was hosted in an unlikely location and had only been in operation for two days, the tool bar would indicate that to the user. Netcraft's toolbar is also beginning to generate data on the hosting of phishing (or pharming) sites by country (Annex 3: Table 11). It is important to note that for both the APWG and Netcraft data, the actual phishers may not be located in the country where the Web site is being hosted.

Not all phishing and pharming sites use spoofed Internet identifiers. In some cases unsuspecting consumers may be directed toward Web sites with deceptive content rather than misrepresented Internet addresses. These fake sites are frequently used in connection with specific forms of fraud such as the "Nigerian 419 advanced fee fraud". In March 2005 one database contained over 3 000 active or inactive sites of fake banks, and so forth, with new entries being added daily.[76] While the domain names, in these instances, are not spoofed the information given by the registrants is invariably false or misleading.

In some instances data on phishing are produced as a by product of the measurement of other phenomenon. Brightmail, a firm acquired by Symantec in June 2004, measures the amount of spam filtered by their software and received by several million of their decoy accounts. Brightmail stated, at the beginning of 2004, that its software was used to filter more than 80 billion messages each month or the equivalent of 15% of all Internet e-mail worldwide. At that stage, Brightmail indicated that some 5% of all the spam they processed resulted from phishing attacks. The company said that phishing had increased worldwide from 300 million messages in August 2003 to over 2.9 billion messages in March 2004.

The cost of phishing

Estimates for the cost of phishing vary widely. At one end of the scale some individual financial institutions, while not willing to reveal their own financial losses, say the sums are relatively modest. The United Kingdom's Association for Payment Clearing Services (APACS) is a non-statutory Association of institutions delivering payment services to end customers. In March 2005, APACS put the cost of online baking fraud (primarily made up of phishing), to its members in the United Kingdom, at USD 25 million for 2004.[77] This was the first time APACS had collected data in relation to phishing.

A study conducted by the Ponemon Institute and sponsored by NACHA (the United States based Electronic Payments Association) and TRUSTe, an online privacy non-profit organisation, revealed that 76% of consumers in the United States were experiencing an increase in spoofing and phishing incidents and that 35% receive fake e-mails at least once a week.[78] The report, in September 2004, estimated the total monetary loss to victims of these incidents to be approximately USD 500 million in the United States.

Gartner has also attempted to quantify the cost of phishing in the United States. Gartner's results suggest a larger scale of problem. In a study published in May 2004, Gartner estimated direct losses from identity theft fraud against phishing attack victims, in the United States, had cost banks and credit card issuers about USD 1.2 billion during 2003.[79]

Other studies with a broader geographical coverage are also at odds over losses due to phishing. According to the TowerGroup the global losses from phishing via e-mail were in the vicinity of USD 137 million in 2004.[80] The TowerGroup said the actual number of phishing attacks totaled more than 31 000 globally in 2004 and that they expect this to rise to over 86 000 in 2005.

This raises the question of why estimates of the direct losses attributed to victims of phishing vary so greatly. In part this may be because financial institutions, while taking the threat seriously, are reluctant to publicly reveal their losses. In addition some firms may simply not know the scale of losses if they go unreported by their customers. Taken together these factors may mean that it would be very difficult for industry to determine a definitive figure for the direct financial losses attributable to phishing.

The APWG report that by hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince up to 5% of recipients of spoofed e-mails to respond. In the United Kingdom, APACS has commissioned research which showed that 4% of Internet banking users would respond to an e-mail, supposedly from their bank, asking them to click on a link and re-enter their security details.[81] Based on survey data, Gartner estimates that about 19% of those attacked, or nearly 11 million adult Internet users in the United States, have clicked on the link in a phishing attack e-mail.[82] Gartner further report that 3% of those attacked, or an estimated 1.78 million adults in the United States, reported giving phishers their financial or personal information in 2003.

The Ponemon Institute study, based on a national sample of 1 335 Internet users across the United States, recorded that seven out of ten respondents had unintentionally visited a spoofed Web site.[83] The study reported that more than 15% of spoofed respondents admitted to being "phished" in that they had provided private information. In total, the study found, a little more than 2% of all respondents believed that they experienced a direct monetary loss resulting from the phishing attack.

In Consumer Reports 2005 "State of the Net", the authors stated the overall incidence was of Phishing was rare but rapidly increasing with 1 in 200 respondents losing money from their account. Consumer Reports further stated that the average cost per incidence was USD 395 producing a national total of USD 147 million in losses for the United States.

Spoofing statistics

An experimental project is being undertaken by the Advanced Network Architecture Group (ANA) at MIT which is attempting to measure in aggregate filtering and "Spoofing" of IP Addresses on the Internet. While the MIT ANA data is believed to be the most comprehensive of its type the project is still under development. The data made available is representative only of the blocks of IP addresses and autonomous systems (ASes) of the volunteer networks from which ANA has received reports. For this reason, ANA present the data both in terms of what they have observed as well as their global estimates for spoofable Internet identifiers. ANA is also working on correlating these data with geographical locations with the first results expected to be reported in 2005.

A further area under investigation, related to Internet addressing and identifiers, is Domain Name System (DNS) cache poisoning.[84] In March and April 2005 the SANS Internet Storm Center reported a number of such attacks. In these instances an authoritative nameserver is configured to return a false NS authority record. This information is then cached and further queries for names, in the "poisoned zone" go

to the incorrect nameserver which in turn provides false information. The Measurements Factory is developing an automated scanning procedure to detect DNS cache poisoning and intends to provide weekly statistics to the DNS Operations, Analysis, and Research Center (DNS-OARC) members and network operators.[85]

Spyware

A category of software that may have serious implications for security and trust is commonly called "spyware". The Federal Trade Commission's working definition of spyware is "software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge."[86] The FTC believes that while this is a useful starting point, it would like to see a greater consensus among industry on the definition of spyware and disclosure of information to consumers.[87]

One intiative in this direction has been undertaken by the Anti-Spyware Coalition (ASC) – a group composed of anti-spyware software companies, academics, and consumer groups.[88] In August 2005, the ASC released a consultation document with a proposed categorisation of spyware and closely related phenomena.[89] This document also contained a glossary defining terms used in discussions about spyware. PTS, the communications regulator in Sweden, has also undertaken a report on spyware and closely related phenomena. The report addresses questions of definitions and what sets spyware apart from related phenomena such as viruses.[90]

Whereas a virus will seek to harm a user's system or to use that system to cause harm to others, spyware seeks to monitor the use of the system (*e.g.* keystrokes or Web pages visited) or to extract information from the system (*e.g.* scan hard drive). As with phishing, this information might contain credit card numbers, account names, passwords, personal identification numbers and so forth. This information is then remitted to the party responsible for inserting the spyware.

Spyware is a broader category than phishing, albeit some of the techniques used are the same. One major distinction is that phishing almost certainly has a criminal intent. Spyware may, of course, also be used in cases of fraud or identity theft. In addition, some spyware applications may fall into the category of causing irritation to users, being perceived as intrusive by users or impairing system performance (*e.g.* unauthorised use of a user's bandwidth, system crashes or instability). One trial, using infected machines, found that 8% of outbound traffic was due to Spyware.[91] Spyware may also probe a system for an opening that may be exploited by hackers.[92]

Spyware statistcs

In his opening statement at an FTC Spyware Workshop in April 2004, the Director of the Bureau of Consumer Protection, Howard Beales, remarked: "Given the novelty of Spyware, little empirical research and analysis has been done to assess its prevalence and its affects in any kind of systematic way. Anecdotes, however, abound. And evidence suggests that consumers are worried about Spyware and what it may cause. Consumers have downloaded free versions of the two most widely-used anti-spyware programs over 45 million times, and many Internet service providers have begun to offer Spyware detection capabilities to address customer concerns about such software." [93]

A range of data from industry sources is available on spyware. The most common are data derived from programmes that seek to prevent spyware from being downloaded by a user or that seek to remove spyware from a user's system. According to one source there are over 100 anti-spyware scanners available for download. [94] One of the largest of such databases is maintained by PestPatrol, owned by Computer

Associates International. PestPatrol defines pests as "any unwanted software." Pestpatrol has also published an extensive glossary of different sub-categories.[95] Based on these definitions PestPatrol makes a range of indicators publicly available from their operations (Annex 3, Figures 8, 9, 10 and 11).[96] McAfee also makes an extensive range of statistics available from users of their products anonymously pooling data.[97]

McAfee detected fewer than 2 million "adware or spyware" products in August 2003. By March 2004, the total number had increased to just more than 14 million.[98] By way of another example, Eartlink is an ISP that makes anti-spyware software available to its users and publishes statistics.[99] Earthlink's data also records large increases over time in the amount of spyware they have detected. Symantec's bi-annual report provides analysis and discussion of trends in Internet attacks, including malicious code created to expose confidential information.[100] The report for the period July to December 2004 documented a steep increase in this phenomenon.

In 2005, Microsoft released a test version of a new anti-spyware program and made it freely available to Windows users. The software has the capability to let users remit information anonymously to Microsoft and, by February 2005, the company was receiving half a million reports per day.[101]

The cost of spyware

Some security experts warn that spyware is already causing some financial institutions to scale back the range of services they offer to users and to damage trust in respect to electronic commerce.[102] At the same time little data are available that would inform an estimate of the cost of spyware, as a proportion of overall identity crime, to business and consumers. Some indirect indicators are available. In 2004, McAfee reported that spyware became a larger technical support problem than viruses in terms of customer calls. The experience of other companies appears to confirm that together spyware and viruses generate the largest losses and most concern to users.

According to Dell, the world's largest supplier of personal computers, "…a record number of customers contacting Dell with computer performance issues caused by spyware and viruses shows how pervasive the problem is among home technology users. Up to 20% of the calls received by Dell's consumer desktop technical support team are for spyware and virus-related issues, far surpassing any other performance issue."[103] One panellist at the FTC Workshop reported that the average call to an ISP helpdesk lasts 6 minutes whereas the average for a call involving spyware is 25 minutes.[104] At the same time, Microsoft says that over one-third of the users reporting crashes in their applications are actually dealing with spyware problems.[105] Occurences such as these generate costs for business and consumers as well as impacting on the confidence users have in suppliers of equipment and services to which they may attribute problems generated by spyware.

In March 2005, it was reported that Police in the United Kingdom had thwarted an attempt to use spyware against a Bank, in an attempt to illegally transfer USD 423 million.[106] In this instance the perpetrators used "keylogging" software that enabled them to track internal entries on computer keyboards. That criminals are successfully earning revenue from spyware would appear to be reflected in the fact that they are also making unsolicited offers to software developers. In February 2005, the Internet Storm Center reported offers that would return USD 0.25 per installation of a program (*e.g.* a game) that included three pieces of embedded spyware.[107]

As the market for Internet advertising has increased, the economics of the grey area between spyware and adware appears to have increased in attractiveness. Webroot, an anti-spyware company, has put the average return from a "spyware or adware" installation at USD 2.40 per year.[108] This revenue is gained from charging fees from pop-up advertising, redirecting users to Web pages and so forth. Accordingly to

Webroot's estimates, the three programmes in this category with the largest installed base worldwide may generate close to USD 0.5 billion per annum.

Economists have also begun to explore the returns on investment (ROI) in security against various forms of Internet phenomenon from spam to spyware, from the perspective of attackers (ROA).[109] While this work is producing econometric models, which can be employed for such analysis, the availability of data tends to be a limitation.

In Consumer Reports 2005 "State of the Net", the authors stated the overall incidence of Spyware was undergoing "explosive growth" with 1 in 6 respondents experiencing a major, often costly problem. Consumer Reports further stated that the average cost per incidence to consumers was USD 250, producing a national total of USD 3.5 billion in losses in the United States.

Viruses, worms, trojans and incidents

Numerous organisations and companies make statistics available about their security operations in respect to ICT networks. McAfee, for example, makes statistics available in relation to its operations on a global basis. These include a map of the world showing the extent of virus activity by country.[110] The McAfee data, on the most prevalent viruses, are also broken out by region. Symantec's Web site provides a synopsis of the latest virus-related threats discovered by Symantec Security Response, including information on: Category Rating (risk), Name of Threat (threat), the day on which the threat was identified (discovered), and the day on which a virus definition was added to protect against the threat (protection).[111]

Data along similar lines is also available from sources that are not vendor specific. Since November 2000 DShield has provided a platform for users of firewalls to share intrusion information.[112] DShield is a free service that although originally a volunteer-based service is now supported by SANS Institute. By pooling information from users, who download applications reporting firewall activity, DShield is able to put together geographical information on attacks and incident trends.[113] The same data are available at the Internet Storm Center operated by SANS.[114] One indicator SANS make publicly available from the data collected is the monthly "survival time". The "survival time" is the average duration between attempted intrusions (*e.g.* worms) reported by the firewalls of participating users.[115]

The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the US Commerce Department's Technology Administration.[116] NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST's Computer Security Division maintains a searchable index of computer vulnerabilities (ICAT Metabase). ICAT links users into a variety of publicly available vulnerability databases and patch sites, thus enabling users to find and fix the vulnerabilities existing on their systems. ICAT is not itself a vulnerability database, but is instead a searchable index leading to vulnerability resources and patch information. ICAT does, however, make available statistics on vulnerabilities including in a time series format.[117] The CERIAS Cassandra Tool, at Purdue University, is one site that aims to simplify users keeping up-to-date with statistics in the ICAT database.[118]

A further source of data on threats and vulnerabilities in this area comes from the growing number of Computer Emergency Readiness Teams (CERTs) around the world. Worldwide, there are more than 250 organisations that use the name "CERT" or a similar name and deal with cyber security response.[119] The US-CERT, for example, is a partnership between the Department of Homeland Security and the public and private sectors. Further examples from the public and private sector include, AUSCERT (Australia), CanCERT (Canada), CERT-IST (France), JPCERT (Japan), KrCERT (Korea) and APCERT (Asia Pacific Computer Emergency Response Team) is a coalition of CSIRTs (Computer Security Incident Response Teams), from 12 economies across the Asia Pacific region.[120]

A number of the CERTs provide statistics on their operations. The US-CERT provides incident statistics in areas such as denial of service attacks, malicious code and so forth.[121] The Japanese CERT provides reports from a distributed arrangement of sensors which observe worm infections and probes of vulnerable systems.[122] The data are used as a basis for JPCERT activities on publishing alerts and advisories and security awareness programs. Korea's CERT also publishes an extensive range of statistics on incidents.[123]

In its 2004 Global Security Index Report, released in February 2005, IBM identified cellular mobile phones and PDAs as a new frontier for viruses, spam and other potential security threats.[124] In 2004, the first "worm" targeted at mobile telephones appeared. The so-called Cabir worm spreads via Bluetooth.[125] By February 2005, according to F-Secure a Finnish security company, the Cabir virus had spread to 14 countries.[126] In the same month a number of high profile invasions of privacy occurred in respect to cellular mobile telephones.[127] In March 2005, F-Secure announced they had found the first virus capable of spreading via multimedia messaging services, which contain photos, sound or video clips, over mobile phones.[128]

CAIDA, the Cooperative Association for Internet Data Analysis, provides tools and analyses promoting the engineering and maintenance of a robust, scalable global Internet infrastructure. CAIDA is housed at the San Diego Supercomputing Center (SDSC), an extension of the University of California at San Diego (UCSD).[129] Among the tools developed by CAIDA are those which assist in security-related investigations and network management. CAIDA's work in this area includes the collection of data and analysis of denial of service attacks, Internet worms, pollution of root servers and so forth. This research includes developing tools which enable visualisations of phenomena such as infected hosts.[130]

The cost of viruses and worms

There are no authoritative figures on the economic cost of computer viruses, worms, Trojan horses and so forth. A number of sources produce estimates of the cost to business and consumers in respect to individual attacks. These figures are widely cited in the media, but not always without some skepticism in respect to methodology and results.[131] For the most part the methodologies used to create these figures are not made public. An additional point, made by critics of such data, is that when its producers are security firms or working for security firms, they are not viewed as independent or impartial sources. Notwithstanding this, the cost of some attacks is most likely significant even if not readily quantifiable. The SANS Institute, for example, estimated the clean up cost of two worms at over USD 1 billion each in 2003.[132] For the same year Trend Micro, a leading security company, estimated the global cost of viruses to be USD 55 billion compared to USD 30 billion in 2002.[133] Prevx, a software security company, put the total cost of the ten most damaging worms at USD 17.2 billion for the year 2004.[134] Some other sources put the global costs even higher than those mentioned but the results of these figures, and those cited above, are not verifiable.

Respondents to the CSI/FBI survey, in the United States, and the AusCERT survey, in Australia, report losses stemming from viruses, worms and trojans. Under this category, in the 2004 surveys, respondents reported losses in the amounts of USD 55 million (United States) and USD 5.6 million (Australia). While both surveys have respondents from a cross section of large companies, educational institutions and government in their respective countries they do not, of course, reflect the cost to the entire economy. They do, however, assist in placing into better perspective some of the estimates for the cost of viruses at the higher end of the scale.

In Consumer Reports 2005 "State of the Net", the authors stated the overall incidence was of Viruses was rising with more targeting of confidential information with 1 in 4 respondents experiencing a major,

often costly problem. Consumer Reports further stated that the average cost per incident to consumers was USD 312, producing a national total of USD 5.5 billion in losses in the United States.

Botnets (zombie machines)

"Botnets" is the term given to machines connected to the Internet which have been compromised in such a way that they can be directed to act in concert by an external party without the owner's knowledge or authority. Botnets may be used, by the party which has commandeered the machines, to mount denial of service attacks against particular sites on the Internet or for retransmission of spam, phishing and so forth.

The available data on botnets are mainly reported by security firms or organisations monitoring and combating the phenomenon. The Honeynet Project, for example, is a non-profit research organisation of security professionals that deploys systems, applications, and services for attackers to interact with around the world. The object is to learn about the tools and behaviour of the attackers and share this information among the security community. In March 2005, the German Honeynet Project released a detailed study of botnets.[135] Some of the botnets monitored by the Honeynet Project included up to 50 000 hosts. They also reported on how information is exchanged by botnet controllers, some of their characteristics (*e.g.* skill level) and aims, as well as witnessing attackers stealing each other's compromised hosts. The US CERT has also proposed the creation of a botnet tracking program which, as well as being a tool to identify and deal with such threats, would gather and archive statistical information.[136]

CipherTrust's "ZombieMeter" tracks worldwide botnet activity, in relation to messaging, in real-time.[137] CipherTrust monitors messaging activity through data received from the Company's network of appliances which protect client's e-mail systems around the world. The ZombieMeter enables vistors, to the CipherTrust Web site, to view updates regarding botnet activity in relation to the origination of messages and the number of machines affected by country.

The average number of computers Symantec was detecting, during daily botnet scans the first half of 2004, increased from 2 000 to 30 000. On occasion the number of infected computers tracked by Symantec reached 75 000.[138] Each botnet may contain many thousands of machines. In 2004, for example, the Internet Storm centre reported that Telenor, a Norwegian based telecommunication carrier, took action against a botnet containing 10 000 compromised machines.[139] For the first half of 2004, Symantec reported that it is common to see attacks with up to 30 000 infected machines.[140] For the second half of 2004, Symantec reported a decrease in the size of botnets, which they attributed to the release of Windows XP Service Pack 2.

Symantec's "Internet Security Report Threat Report" for the second half of 2004 contained a new indicator in relation to botnets.[141] The indicator was the percent of "bot-infected" computers by country (Annex 3, Table 12). Symantec noted that by identifying the global distribution of infected computers, this indicator can assist in building an understanding of the level of security awareness of Internet users in a given country. The results showed the greatest number of infected computers were in the United Kingdom (25.2%), the United States (24.6%) and China (7.8%). Weighting the data on infected computers, by population or the number of broadband subscribers, for all OECD countries can also be informative (Annex 3, Table 13). On both measures the United Kingdom has the highest rate of infection. Placing that country to one side, on a per capita basis, Portugal, Sweden, Canada and Denmark have the largest number of bot-infected computers. When set against the total number of broadband subscribers in their country, Portugal, Greece, Spain and Sweden have the largest number of bot-infected computers after the United Kingdom. This is, of course, only a partial indicator as the number of dial-up subscribers with infected computers would also come into play. Further analysis needs to be undertaken in respect to the impact dial-up might have on these data but it is generally acknowledged that the rise of botnets has coincided with the increase in the number of always-on Internet connections.

Symantec has suggested that the large share attributed to the United Kingdom may be due to rapid broadband growth in that country. While undoubtedly a factor, this raises the question of why other countries such as France, which have a similar broadband penetration and are experiencing comparable growth rates with broadband to the United Kingdom, have a much lower share of bot-infected computers.

The most likely explanation for the different rates of infection between countries, are factors within the prevailing culture of security. In some countries ISPs supply their customers with security as part of their service. In Finland, for example, all the ISPs supply heavily discounted or free personal firewalls and Anti-Virus software to their customers. This may be a factor in why Finland performs best among the Nordic countries in respect to the number of bot-infected computers relative to broadband subscribers. That some countries, elsewhere in the OECD area, do even better than Finland suggests that other factors, from the prevailing culture of security in a country, are also involved. The most important of these is likely to be the security awareness and responsiveness of users, to apply tools such as firewalls and anti-virus software, even when made available by ISPs. In this respect it is worth pointing to the very low rates of infection in Japan, Belgium, Korea and the Netherlands. All these countries have high rates of broadband penetration and low infection rates suggesting high relative use of firewalls and anti-virus software by users.

Symantec gather the data on bot-infected computers from their monitoring of 20 000 sensors located in networks in over 180 countries. Attacks from infected computers are recorded and matched against other databases such as for malicious codes and those enabling the assessment of originating addresses. Significantly, the data are not specific to Symantec customers, as are some indicators, so there should not be a geographical bias. The capture of computers is believed to be opportunistic rather than targeted towards any particular country with a view to use within that country. Accordingly, this indicator may be one of the best currently available for international benchmarks of security awareness and action by Internet users.

The cost of botnets

In 2004 a number of cases of extortion were reported whereby the owners of e-commerce Web sites were threatened with denial of service attacks. Online gambling Web sites have been one of the primary targets but also firms engaging in Web-based financial transactions.[142] In one case, National Hi-Tech Crime Unit, hackers targeted the Web site of an online bookmaker in the United Kingdom with a denial of service attack. The hackers told the bookmakers that they would cease if the bookmakers transferred USD 40 000 to an account in a Latvian bank.[143] The bookmaking firm agreed and transferred money several times, but when the attacks continued they contacted the National Hi-Tech Crime Unit. According to the case brought against the alleged culprits, in Russia, the total losses suffered by the victims of this particular gang were put at USD 3 million. This was an estimate of lost business and payments made to the alleged extortionists. Losses would however be difficult to quantify in many cases. Recent academic research suggests there is a lasting negative impact on Web sites that become unavailable due to denial of service attacks.[144] The research suggests sites with a low switching cost are worse hit by such attacks.

In 2004 well-known companies such as Akamai and Doubleclick were also subject to denial of service attacks.[145] In one well-reported case an individual, currently on the FBI's most wanted list, is alleged to have hired hackers, using botnets of between 5 000 to 10 000 machines, to launch denial of service attacks against his company's competitors.[146] Some estimates put the total amount of spam retransmitted from botnets at between 40% to 80%.[147] In 2005 it was reported that botnets were being used to compromise Google's "Adwords" advertising campaign by inflating the number of times an advertisement is displayed.[148]

Security professionals report that botnets can be hired over the Internet via electronic mail, Web pages and IRC (Internet relay chat) networks.[149] One such offer indicated a botnet with 5 000 machines could be

hired for USD 300.[150] A number of security professionals quoted in various media reports indicate that botnets with 1 000 machines are available for around USD 100 per hour.[151] The demands of extortionists can vary depending on the potential losses hackers feel they can inflict on a business by bringing down their Web site. In one case an attacker told an agent of the National Hi-Tech Crime Unit, posing as another hacker, that he demanded USD 5 000 to USD 10 000 to cease attacks depending on the size of the site.[152] Some businesses report extortion demands of between USD 30 000 to USD 50 000 in the face of denial of service attacks.[153]

Modem hijacking

Modem Hijacking is the term given to the phenomenon when an Internet user unintentionally downloads programs which cause their modem to log off from their existing ISP and to dial telephone numbers in foreign countries resulting in long distance telephone charges or service connection fees.[154] This occurs without the knowledge or consent of the user with some services charging up to USD 500 per minute.[155]

The executable programs which are downloaded when modem hijacking occurs are referred to as Web dialers or rogue dialers. Between August 2003 and August 2004 McAfee reported that they had detected around 250 000 Web dialers and 4 million affected computers.[156] In 2004, BT introduced a new scheme aimed at combating this phenomenon. During the first four months of operation BT dealt with 45 000 cases where their customers' bills had been inflated by modem hijacking.[157] Similar examples abound across the OECD area. In 2004, the Finnish Consumer Agency dealt with a case where users undertaking a test on the Internet were logged out of their ISP connection and reconnected to a Danish provider.[158] In February 2005, the Internet Storm Center was reporting occurrences of modem hijacking in Italy.[159] In that instance the ISC reported that an Italian entity, masked by a domain purchaser in the United States, had in place dialers that would retrieve additional code from a site in Moldavia and then try to dial various telephone numbers in the South Pacific.

While data are available on modem hijacking from companies such as McAfee and BT in respect to their own operations there are little systematic data available on this phenomenon. One example of a service devoted to the education of users on telephone fraud is Canada's "Phone Busters". Phone Busters is a joint initiative between the Royal Canadian Mounted Police, the Ontario Provincial Police and the Competition Bureau of Canada. A range of statistics and news related to "phone fraud" are available on the Phone busters Web site.[160] The problem of modem hijacking should not impact on broadband users unless they also use a dial-up connection.

Click fraud and "search spam"

As the World Wide Web has evolved, advertising has become one of the key ways business has found to seek a return on investment in providing services. Providers of popular services such as Web based e-mail, search engines, blog hosting and so forth increasingly rely on revenue from advertising. One model involves advertisers or merchants paying the owners of other Web sites to host advertising links back to their Web site. Payment is made every time a user "clicks through" to that site. Additional payments might be then made if the user "clicking through" goes on to buy a product or service.

Another model involves advertisers or merchants purchasing key words from search engines with the highest bidder having their advertisement ranked first alongside the results of search engines. Overture, for example, provides a tool which allows advertisers to see how many times a word was search for in the previous month.[161] In January 2005 the key word "refinance" was searched for 582 803 times. The highest price an advertiser was willing to pay in February 2005 was USD 12.04 followed by USD 12.03 and so on.

If the advertiser did not cap their expenditure to a certain amount and recorded a 5% click through rate, the total sum payable to Overture would be USD 350 847.

As the Internet advertising market has grown so have the financial incentives for targeting different segments by fraudsters or others with malicious intent. "Click fraud" generally occurs when an individual clicks through a paid-for link with the intention of increasing the amount payable to themselves.[162] Under the Overture system, it can also occur when an individual, for whatever reason, seeks to inflate the cost to the advertiser or knock them out of the search engine ranking once their monthly allowance has been used. This could either be done manually using low-cost contractors or using automated software or a botnet. The phenomenon is already attracting the attention of academic researchers aimed at understanding the effectiveness of "link spam".[163]

Click fraud may vary depending on how the search engine ranks advertisements. In contrast to Overture, for example, Google is reported to take click-through-rates (CTR) into account when deciding the rankings of search ads. Under this system extra impressions without click-throughs can result in an advertisement being demoted or even disabled. The alleged practice, in relation to Google results, is for fraudsters to "…. take advantage of Google's system by disabling their own ads, making a flurry of queries on their chosen keywords, and then re-enabling their ads. By doing this, they drive down the CTR on competitors' listings, then swoop back in to claim higher rankings."[164] The practice in relation to Google has been called "impression spam".

A growing number of media reports indicate that click fraud is a threat to ad-buyers' confidence.[165] At the end of 2004, the Chief Financial officer of Google was reported as telling an investor's conference that quick action needed to be taken against click fraud because of its potential to threaten that company's business model.[166]

The measurement of e-mail spam is not considered in this report as work is being undertaken elsewhere. "Search spam" or "content spam" is, however, also emerging as a problem for the owners of Web sites, blogs, forums or other online media which offer the opportunity for visitors to post comments or other information. The aims of content spammers may be multiple including, in addition to the traditional motivations, lifting their ranking in search engines with a view to click through revenue or influencing the secondary market for domain names.[167] A further motivation may be the transmission of malicious code. If content spammers can lift their Web site ranking in search results, there is a greater likelihood that users will click through to those sites and have their systems infected.[168] Developments such as these have the potential to impact on the confidence users have in tools such as search engines. New forms of spam are also emerging in areas such as instant messaging (*i.e.* spam over instant messaging or "spim"), blogs (so called "comment spam") and spam on cellular mobile telephones or Internet telephony.

Measurement of click fraud and search spam

The Interactive Advertising Bureau, a United States based trade group, has defined a set of guidelines for the measurement of online campaign advertising and audit.[169] The IAB's measurement task force is working on standards to measure click throughs and to eliminate fake ones.[170] A further source of information on the phenomenon of click fraud and content spam is available from the Search Engine Marketing Professional Organization (SEMPO). SEMPO's annual publication on the state of search engine marketing contains survey results ranging from the size of the market for search engine advertising search through to the opinions of search engine advertisers and marketing agencies on potential threats such as click fraud and content spam.[171] Worthy of note is that those surveyed in 2004 ranked "Content Spam" as a greater threat to advertiser confidence than click fraud.

In February 2005, the Pew Internet & American Life Project released the results of a survey they undertook on the phenomenon of "spim".[172] The study reported that some 42% of America's 134 million online adults use instant messaging and almost a third of those instant message users (30%) have received "spim".[173] In the same month, the first results were released of a survey of mobile users and their attitude to spam undertaken by the University of St.Gallen and "bmd wireless" and ITU (International Telecommunication Union).[174] The study reported that 83% of telecommunication industry respondents believe that mobile spam will be a critical issue in the near term.

E-commerce infrastructure security and certification

Secure sockets layer (SSL)

Netscape developed the Secure Socket Layer (SSL) protocol for encrypted transmission over TCI/IP networks. The most common use of SSL is to provide a secure end-to-end link for e-commerce transactions, with major e-commerce uses of secure server software including encrypted credit card transactions in retail applications and restricted access to privileged information both within organisations and between organisations. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.[175] As SSL is built into all major browsers and Web servers, simply installing a digital certificate enables their SSL capabilities.

The use of SSL, by e-commerce sites, has become an important tool in building trust between themselves and their customers on the Internet. The FTC, for example, recommends that consumers look for indicators (*e.g.* a lock icon on the browser's status bar or a URL for a Web site that begins "https") that a site is secure before providing personal or financial information to a Web site.[176] Merchants such as Amazon.com or hotel chains, such as those owned by European Accor Group (*e.g.* Sofitel, Novotel, Mecure), use secure servers as a routine part of their activities. E-commerce sites owned by such companies will commonly display information such as the following example, from lastminute.com on their Web site:

> "Our secure server technology means that any data you transfer through lastminute.com will be completely safe from prying eyes. Every credit card purchase you make at lastminute.com is done through our Secure Server Technology. This provides many security features, including:
>
> - Authentication: this assures your browser that your data is being sent to the correct computer server, and that the server is secure.
>
> - Encryption: this encodes the data, so that it cannot be read by anyone other than the secure server.
>
> - Data integrity: this checks the data being transferred to ensure it has not been altered."[177]

A necessary component in the establishment of secure Web sessions via the SSL is the public key certificate. By digitally signing the certificates it issues, the Certification Authority binds the identity of the certificate owner to the public key within the certificate, and thereby vouches for the trustworthiness of the certificate. Online vendors such as lastminute.com frequently display the Certificate Authority's mark on their site.[178] Secure servers can be used without a digital certificate (*e.g.* for the transfer of information between a closed user group). However, the fact that a site has taken the trouble to go through the certification process tends to indicate that they are engaged in the transfer of sensitive information with external parties such as occurs in the case of e-commerce.

Certificate Authorities include companies such as Versign, GeoTrust, Comodo and Entrust. Verisign has by far the largest market share of any certificate authority. In July 2004, together with its subsidiary Thawte, Verisign was responsible for 39% of all SSL certification (Annex 3: Table 14). Verisign's overall market share is, however, greater than that because it also signs some certificates as RSA Data Security. Verisign's largest competitors GeoTrust and Comodo had respectively issued 19% and 11% of all SSL certificates at the same date. Versign's position as the leading global player in part derives from the fact that early versions of the Netscape and Microsoft browsers would only accepts certificates from Verisign. Current versions of these browsers allow users to add or remove certificate authorities. This has enabled greater competition in the certification market particularly at the national level where companies with trusted local brands have entered the market.

The cost of certification has fallen dramatically although Verisign's brand commands a premium for its certification.[179] In September 2004, Verisign charged USD 349 for an annual secure site 40-bit SSL encryption service and USD 895 for a 128-bit service. Some competitors bundle SSL certification with other services and charge prices as low as USD 25 to promote the use of their other products (*e.g.* hosting services).[180] In September 2004, GoDaddy, a large domain registrar, charged USD 29.95 for 128-bit SSL certification.[181] EV1Services offered starter SSL certificates for as low as USD 4.95, for a 128-bit service, at the same date.[182] The large range of prices found in the SSL certification market reflects providers willing to offer loss leaders to attract customers and the recognition some brands have in the market. Different pricing has also emerged depending on whether the Web site owner wants a domain-validated SSL certificate or an organisation-validated certificate.

Organisation-validated certificates offer a lengthier and more thorough vetting of the certificate purchaser, which is attractive to site operators who want to offer the highest level of assurance to users about the safety of using their site.[183] According to Netcraft, a private company that runs the largest online survey of secure servers, the "…key question going forward will be whether SSL certificate buyers continue to opt for lower priced domain certificates, or whether concerns about phishing and other security threats prompt site operators to pay a little more to upgrade to organization-assurance certificates. At present, most certificate buyers believe that customers aren't differentiating between the two validation methods."[184] This may change, however, as the makers of browsers, such as Firefox and Opera, highlight SSL features more in their navigational frames as an additional security enhancement.

Data on SSL certification market share and type of certification are available from Netcraft. They also make the data available to their clients by country. This allows analysts not only to see the largest global players but also a breakout of data on market share by country. In Germany, for example, TC Trust Center for Security in Data Networks GmbH and Deutsche Telekom are also significant players in addition to the largest global players which operate in that market.

To date, most use of SSL has been associated with fixed network access to the Internet. Cellular mobile networks are also increasing their capabilities to offer e-commerce services. In Japan, NTT DoCoMo has launched FeliCa smart-card service and FeliCa-enabled handsets can be used for a variety of applications, previously only possible with smart-cards, including ticket purchasing, debit and credit card transactions, personal identification, and building access.[185] Certificate Authorities, with a view to supporting that market, have begun to offer SSL services aimed at wireless devices. In July 2004, GeoTrust began offering SSL certification aimed at providing Web-based information to the mobile wireless market (*e.g.* handheld computers and smartphones).[186]

Netcraft's SSL survey also provides, on a monthly basis, the actual number of secure servers by country and, among a range of other indicators, the level of encryption used by each secure server. In July 2004 there were 305 000 secure servers in the OECD area (Annex 3: Table 15). Just under two-thirds of these secure servers are located in the United States. These data can be weighted by population to

facilitate a comparison of the relative take-up of SSL throughout member countries. In July 2004, Iceland, the United States and Canada recorded the leading deployment of SSL per 100 000 inhabitants. One factor to remember when interpreting the take up of secure servers is that there is a higher degree of centralised use of secure servers in some countries than others. In the Nordic countries, for example, merchants may not have their own secure server but instead payment will be made through the secure server of the consumer's bank.[187] In the United States, and many other countries, merchants use PayPal to conduct e-commerce. By using PayPal merchants do not need to install their own secure server. Instead PayPal automatically encrypts communication between themselves and users with PayPal's own secure servers.

Netcraft's secure server survey has the following methodology. Each of the sites from which Netcraft receives a successful response in the Netcraft Web Server Survey, together with a number of sites that Netcraft thinks might be offering purely SSL-encrypted services, are queried with an SSL request to retrieve the site certificate and server signature using an SSL client offering a full set of ciphers. This information is then automatically interrogated to provide information such as geographical location, operating system, certificate authority, level of encryption and so forth. It should be noted that a change in methodology, in October 2001, introduced a stricter definition for authenticated sites. Data from prior surveys have not been adjusted, such that comparing surveys over the period 1998 to 2004 may slightly understate growth.

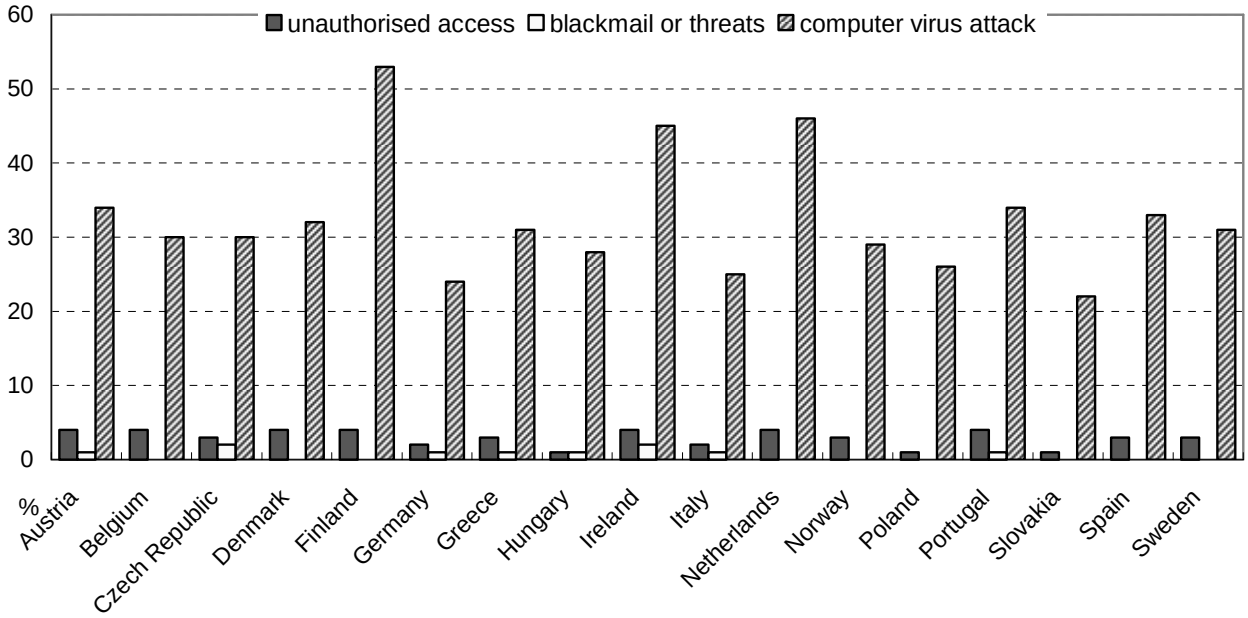
ANNEX 1: SELECTED OFFICIAL STATISTICS ON TRUST (IN THE ONLINE ENVIRONMENT)

Eurostat

Some examples of Eurostat data are provided below (Figures 1, 2, 3 and 4). Eurostat has other information on this topic which is publicly available on its New Cronos Web site.[188]

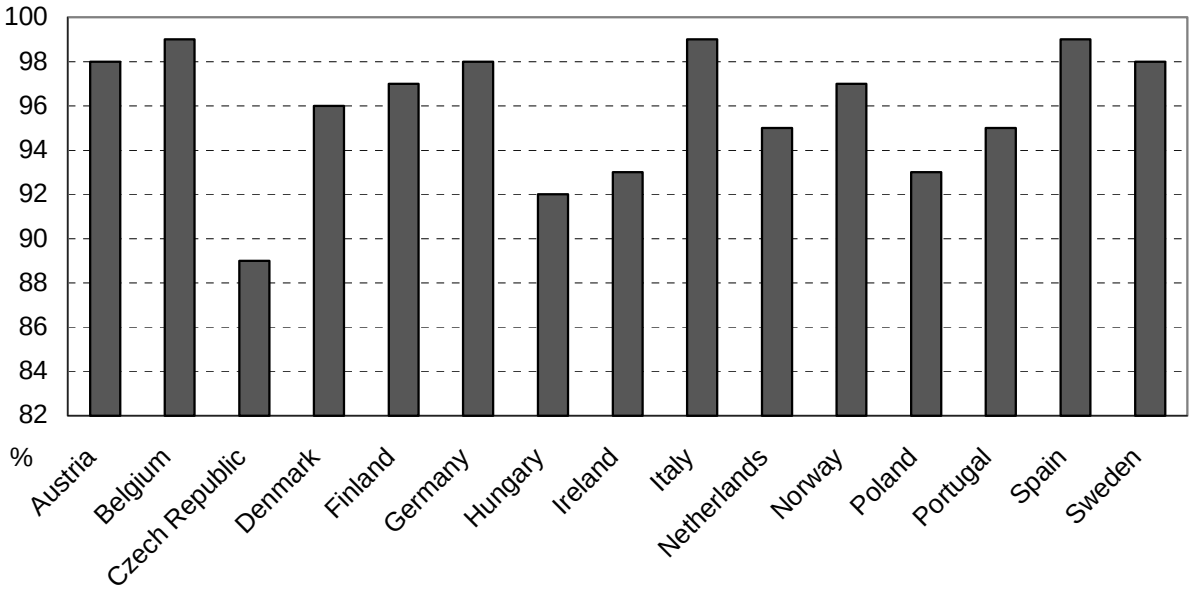
Enterprise data on IT security

Figure 1. **Percentage of enterprises with Internet access having encountered security problems in 2004**
Percentage of enterprises with ten or more employees and with Internet access



Source: Eurostat, Community Survey on ICT Usage in Enterprises, 2003, February 2005.

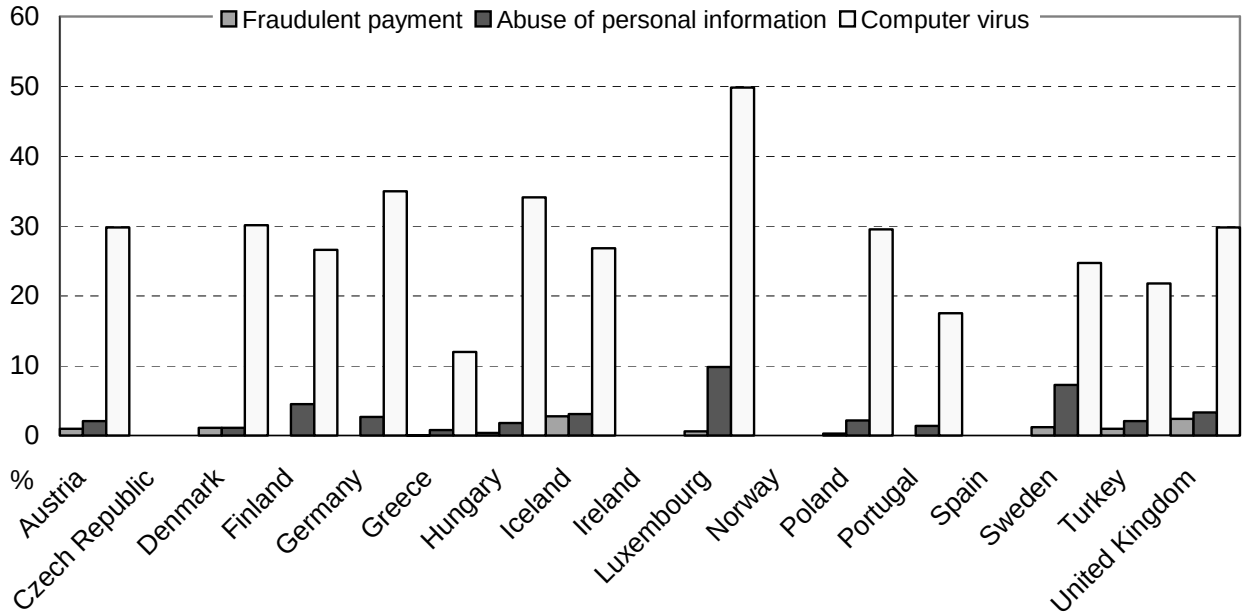
Figure 2. **Percentage of enterprises with Internet access taking security precautions in 2004**
Percentage of enterprises with ten or more employees and with Internet access



Source: Eurostat, Community Survey on ICT Usage in Enterprises, 2004, February 2005.

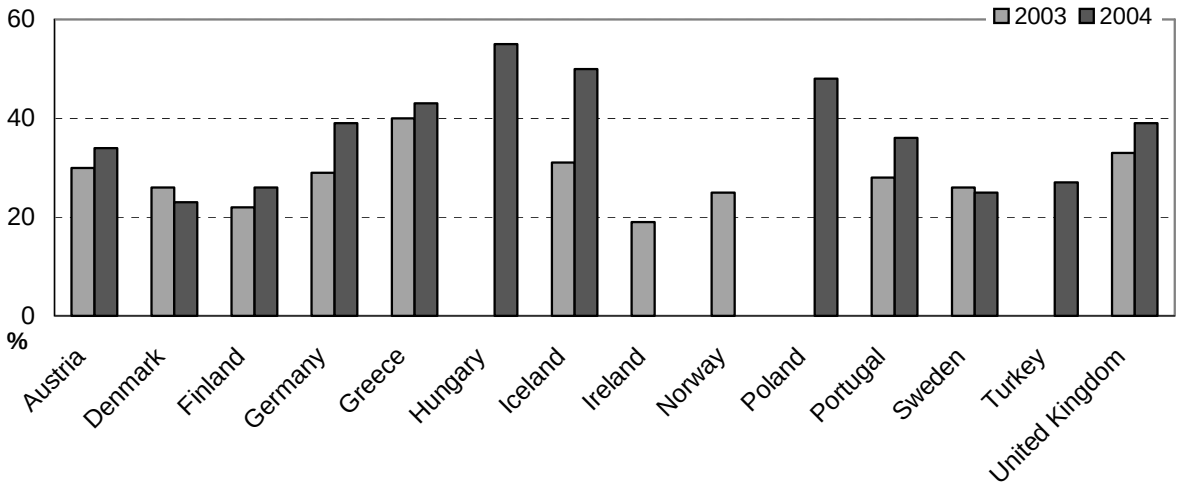
Household data on IT security

Figure 3. **Percentage of individual Internet users having encountered security problems in 2004**
Percentage of individuals who used the Internet within the last year



Source: Eurostat, Community Survey on ICT Usage in Households and by Individuals, 2004, February 2005.

Figure 4. **Percentage of individuals who have, in the previous three months, installed a virus-checking programme**
Percentage of individuals who used Internet in the last three months

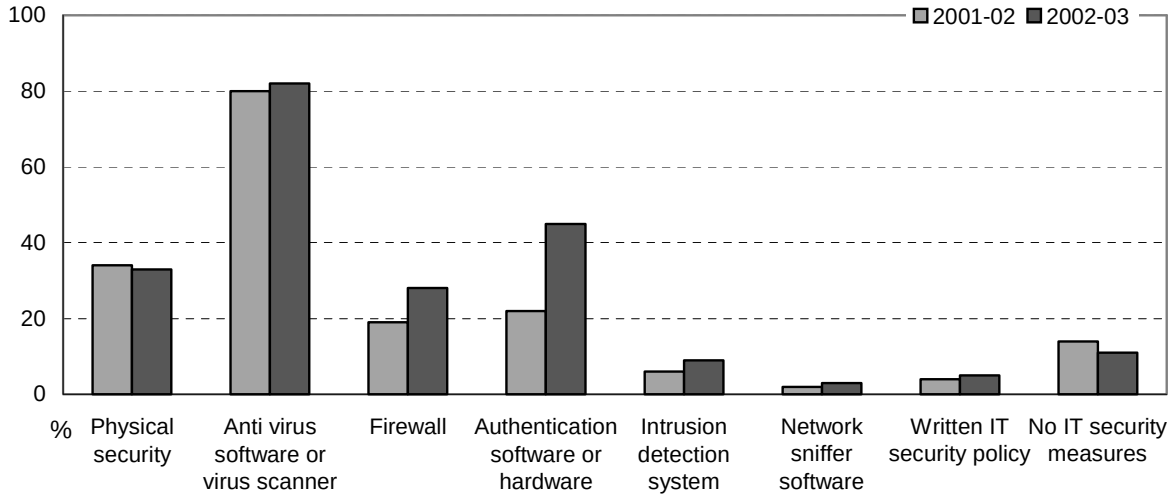


Source: Eurostat, Community Survey on ICT Usage in Households and by Individuals, 2003 and 2004, February 2005.

Australia

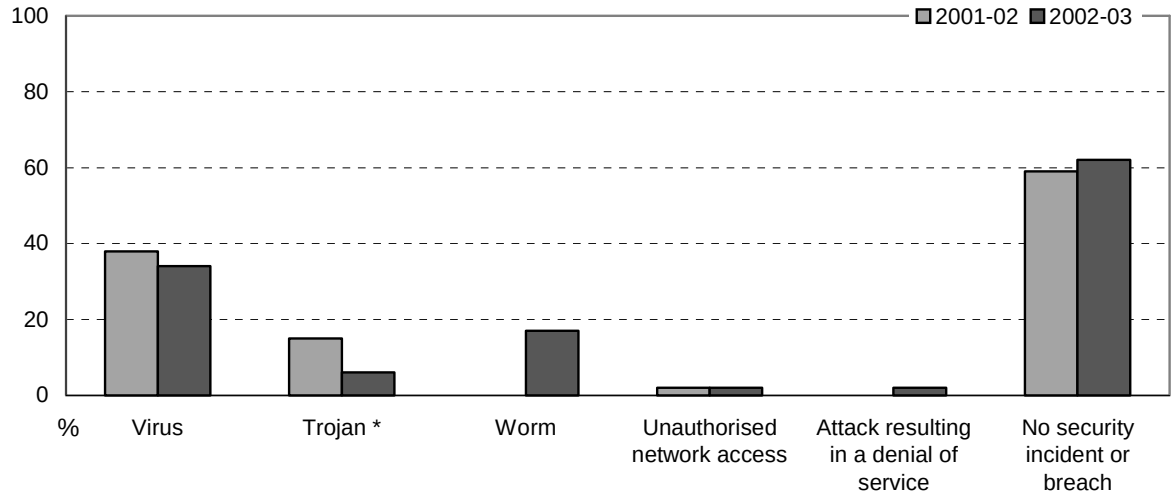
The Australian Bureau of Statistics collected IT security data from business in respect of 2001-02 and 2002-03 in its annual *Business Use of Information Technology Survey* for those years. Selected results are shown below (Figures 5 and 6). The complete publications are available from the ABS Web site.[189]

Figure 5. **Businesses' security measures in 2001-02 and 2002-03**
Percentage of businesses with a computer reporting on security measures in place



Source: Australian Bureau of Statistics, *Business Use of Information Technology*, 2000-01 and 2002-03, Cat. no. 8129.0.

Figure 6. **Businesses reporting IT Security Incidents or Breaches in 2001-02 and 2002-03**
Percentage of businesses with a computer reporting security incidents or breaches



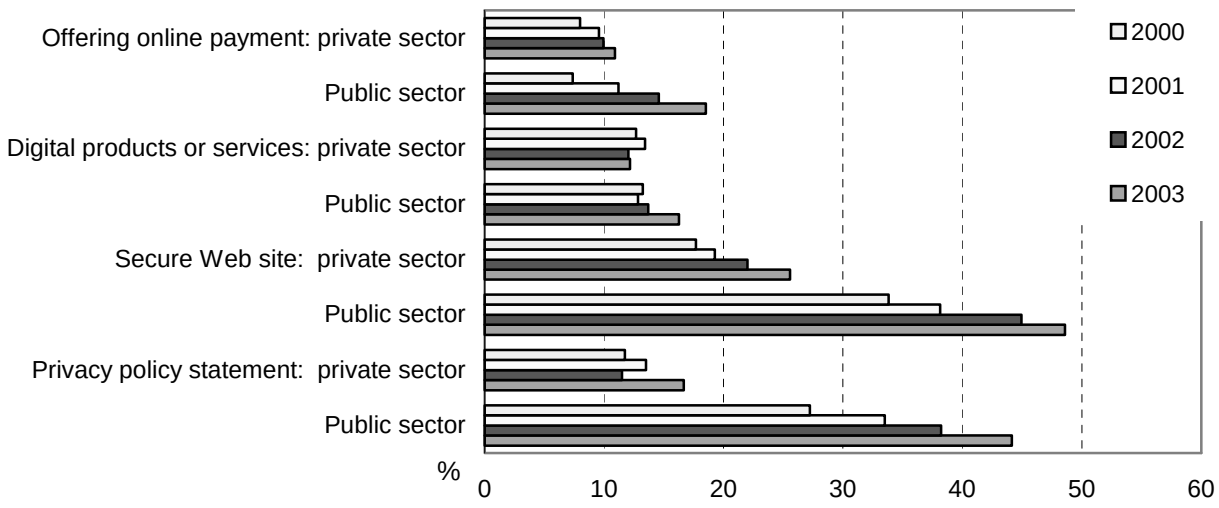
* In 2001-02 Trojan includes Worm.

Source: Australian Bureau of Statistics, *Business Use of Information Technology*, 2000-01 and 2002-03, Cat. no. 8129.0.

Canada

Statistics Canada conducts an annual *Electronic Commerce and Technology Survey*, in which it collects ICT use data from both private- and public-sector organisations (excluding local government). Included are questions on: whether the organisation's Web site has a privacy policy statement and whether that Web site is secure, that is, whether there are policies and technologies (*e.g.* SSL, PKI) to secure transactions and/or information. Selected results are shown below (Figure 7).

Figure 7. **Characteristics of Web sites in the Public and Private Sector, 2000 to 2003**
Percentage of enterprises with different Web characteristics



Source: Statistics Canada, *Survey of Electronic Commerce and Technology*, 2000 to 2003.

Japan

Japan's Communications Usage Trend Survey (2003) for both households and businesses has a number of questions relating to trust. 2003 data are publicly available.[190] Refer to Figures 6-11 (covering both households and businesses). Questionnaires for these surveys are also available.[191]

United States

The United States Census Bureau Current Population Survey, Computer and Internet Supplement, October 2003, took a different approach from other surveys and asked about perceptions of concern about providing personal information (comparing Internet and telephone) and material children are exposed to on the Internet (compared with TV). Other results from the survey are available from the 2004 report *A Nation On-line: Entering the Broadband Age.*[192] The results are shown below (Tables 1 and 2).

Table 1. **Concerns about providing personal information over the telephone compared with the Internet, October 2003, United States**

Compared to providing personal information over the telephone, how concerned are you about providing personal information over the Internet?

							Total	
	16-24	25-44	45-64	65-74	Males*	Female*	All*	Internet users*
More concerned	46.1	45.8	52.3	57.2	48.1	49.8	49.0	47.4
Less concerned	8.2	8.7	7.7	6.5	8.5	7.8	8.1	7.7
About the same	45.7	45.5	40.0	36.3	43.4	42.4	42.9	44.8

*Aged 16-74.

Source: US Department of Commerce, Economic and Statistics Administration, Computer and Internet Supplement to the Current Population Survey, October 2003, unpublished information.

Table 2. **Concerns about children's exposure to material on television compared with the Internet, October 2003, United States**

Compared to the material on television, how concerned are you about the kind of material children may be exposed to on the Internet? (only asked of respondents with children under the age of 18 in the household)

							Total	
	16-24	25-44	45-64	65-74	Males*	Female*	All*	Internet users*
More concerned	68.8	69.1	73.4	75.0	69.5	70.5	70.0	72.3
Less concerned	6.1	5.8	4.5	1.0	5.5	5.6	5.5	5.3
About the same	25.1	25.1	22.1	24.0	25.0	24.0	24.5	22.4

*Aged 16-74.

Source: US Department of Commerce, Economic and Statistics Administration, Computer and Internet Supplement to the Current Population Survey, October 2003, unpublished information.

ANNEX 2: OECD DRAFT MODEL QUESTIONS ON TRUST

The OECD model surveys on ICT use by businesses and households/individuals are currently being revised. At time of writing, the drafts included a number of questions relating to trust in the online environment. In addition, the proposals included discussion points on measurement of other issues relating to trust. Details are provided below.

OECD draft model questionnaire for ICT use by businesses (at April 2005)

A revised model questionnaire on ICT use by businesses was presented to the April 2005 meeting of the Working Party on Indicators for the Information Society (WPIIS) in [DSTI/ICCP/IIS(2005)2, internal working document]. The questionnaire will be further revised based on the discussion during the April 2005 meeting and written comments following the meeting.

The relevant questions from the April draft are copied below. A short report on feedback from delegates, including the likely impact on the draft questions, is presented beneath the questions.

Section A: General information about your business' use of ICT

Question 8 in Section A is asked of enterprises with a Web presence (defined as Web site/home page or presence on a third party's site (including a related entity) where the enterprise has substantial control over the content of the site/page).

As at <reference date> did your business' Web presence have?

Tick all which apply

A security policy statement	☐	A security policy statement explains security measures taken and can refer to security of customer information (in transmission and/or storage) or financial transactions.
A security seal or certification	☐	Refers to third party security certification. May also be called a trustmark.
A privacy policy statement	☐	May be called privacy guidelines, a privacy notice or a privacy guarantee. It explains the privacy practices of the business with regard to handling and using personal information.
A privacy seal or certification	☐	Refers to third party privacy certification. May also be called a trustmark.

Section B: IT security

Questions 9 and 10 deal with IT security. Draft questions are as follows:

Did your business have any of the following IT security measures in place at <reference date>?

Tick all which apply

Virus checking or protection software which is regularly updated	☐	Software which detects and responds to malicious programs such as viruses, trojan horses and worms. Regular update refers to automatic or manual downloading of virus definitions.
Anti-spyware software	☐	Software which detects and removes spyware from a computer system (spyware gathers user information through an Internet connection without the user's knowledge).
Firewall	☐	Software or hardware that controls access in and out of a network or computer.
Secured communication between clients and servers (*e.g.* via SSL, SHTTP)	☐	SSL is an encryption protocol which creates a secure connection between a client and a server. SHTTP supports the secure transmission of individual messages over the WWW.
Authentication software or hardware for internal users	☐	Authentication software or hardware which verifies the identity of an internal or external user, user device, or other entity. Forms of credentials include passwords, tokens and digital signatures.
Authentication software or hardware for external users (*e.g.* by customers)	☐	
Intrusion detection system	☐	Any system which attempts to detect intrusion into a computer or network by observation of actions, security logs or audit data.
Regular back up of data critical to your business operations	☐	
Offsite data backup	☐	Backup copies of computer files stored at a different site to your main data store.
Employee training programs in IT security	☐	
Other (please specify)……	☐	
No IT security measures in place	☐	

Did your business experience any of the following IT security problems during <period>?

Excluding: *attacks which were* *<u>successfully prevented</u>* *by security measures in place*

Tick all which apply

An attack by a virus, trojan horse or worm	☐	Resulting in loss of data or time, or damage to software or hardware.
Unauthorised external access to your data or computer systems	☐	Possibly resulting in fraud, extortion or theft of information.
An attack resulting in denial of service	☐	A denial-of-service attack deliberately restricts access to an information system, for example, by flooding it with traffic, so that it becomes unavailable for its intended purpose.
Other (please specify)…….……	☐	
No IT security problems experienced	☐	

Section C: How your business uses ICT in its operations

Question 29 in Section C is a barriers question directed to all respondents which use computer networks. Relevant response categories are: *Security concerns*, *Privacy concerns* and *Uncertainty concerning legal/regulatory framework for sales over computer networks.*

Which of the following factors, if any, limited or prevented selling via the Internet or other computer networks by your business during <period>?
Tick all which apply

Products of your business are not well suited to sale by computer networks	☐	
Security concerns	☐	Includes concerns your business has and the perceived concerns of customers (*e.g.* on providing credit card details over the Internet).
Privacy concerns	☐	Includes concerns your business has and the perceived concerns of customers (*e.g.* about providing personal information over the Internet).
Prefer to maintain current business model *e.g.* face to face interaction	☐	
Customers' systems incompatible with your business' systems	☐	Refers to interoperability issues which could also be described as technical difficulties with interaction between internal and external systems.
Insufficient level of customer demand for online ordering over computer networks	☐	
Uncertainty concerning legal/regulatory framework for sales over computer networks	☐	
Cost of development/maintenance is too high	☐	
Lack of skills or appropriate training	☐	
No limitations to sales over computer networks	☐	
Not relevant – as selling over computer networks is currently under development or planned for the near future	☐	
Other (please specify)……	☐	

Feasibility of IT security questions in the model questionnaire

Delegates to the 2005 WPIIS meeting were asked for their views on the statistical feasibility of the draft questions presented above and on the following topics for possible inclusion.

- Whether the business has conducted a risk assessment on the security of its computer system and, if so, what type of assessment that was (for instance, internal, by an external party, by a certifying organisation/authority etc).
- Whether businesses which use anti-virus software download virus definitions and, if so, whether automatically, daily, weekly etc.
- Whether the business applies patches to, or updates, software which is critical to the security of its computer systems, and if so, whether automatically, daily, weekly etc.

Feedback from the Working Party

The main area of feedback was on the feasibility of question 10 shown above. Several countries, as well as Eurostat, mentioned that businesses tend to under-report security incidents they have experienced. For this reason, that question will be included in the next draft – but as a **non-core** question. There was little specific comment on questions 8, 9 and 29, so these are likely to be retained in a similar form in the next draft. Very little feedback was received on the new topics raised for discussion, however, questions on risk assessment and updating of anti-virus software are currently included on a limited form testing exercise being undertaken by Statistics Canada. Results are expected by the end of August.

OECD revised model questionnaire for ICT use by households and individuals (at August 2005)

A revised model questionnaire on ICT use by households and individuals was presented to the WPIIS meeting of April 2005 [DSTI/ICCP/IIS(2005)3]. The questionnaire was subsequently revised following discussion during the meeting and written comment following the meeting. Delegates were particularly asked to comment on draft IT security questions and the feasibility of including new topics. A short report on the latter is presented below.

The relevant questions from the draft which incorporates delegates' views are copied below.

Section A: Household access to information and communication technologies

Question 5 in Section A is a barriers question directed to households without Internet access (at home). The relevant response categories are *Privacy concerns, Security concerns* and *Concern that content is harmful*. The question is as follows:

What are ALL the reasons for members of this household not having access to the Internet at home?[10] *Population: in-scope households without access to the Internet at home (whether or not they have a computer)* Multiple responses allowed		Note that not having a computer is not a valid response.
Not interested	☐	
Costs are too high	☐	Includes equipment and access costs.
Lack of confidence, knowledge or skills	☐	
Concern that content is harmful	☐	For instance, concern that children will access inappropriate sites.
Have access to Internet elsewhere	☐	For example, household members use the Internet at work.
Security concerns, for example, concerns about viruses	☐	
Privacy concerns, for example, concerns about abuse of personal information	☐	
Other (please specify)…….……..	☐	

Section B: Individual (adult) use of information and communication technologies

Questions 8, 15 and 16 in Section B are IT security questions directed to an individual. Question 8 concerns backing up of files on computers used at home and questions 15 and 16 deal with security in relation to home Internet. The questions are as follows:

Question 8

When using a computer at home in the last 12 months, have you backed up files (such as documents, spreadsheets or digital photographs) which you created and kept on the computer?
Population: all in-scope individuals who used a computer at home in the last 12 months

For example, by putting them onto a CD, memory stick or external hard drive, or storing them on Web sites (such as those offering online storage of photographs or other files). Includes files created elsewhere (for instance, a handheld computer or digital camera) and transferred to a computer used at home.

- Always or almost always ☐
- Sometimes ☐
- Never or hardly ever ☐
- Not applicable - I have not created files which I kept on a computer used at home ☐

That is, all or most files created by the individual are backed up – either individually or via a periodic backup of new (or all) files.

Question 15

When using a computer to access the Internet at home in the last 12 months, have you experienced an attack by a virus or similar (for example, a trojan horse or worm) which has resulted in loss of data or time, or damage to software or hardware?[19]
Population: all in-scope individuals who used a computer to access the Internet at home in the last 12 months

No **Yes** **Don't know**

Excluding attacks which were successfully prevented by security measures in place.

Question 16

Was the computer you used to access the Internet at home protected by:

Population: all in-scope individuals who used a computer to access the Internet at home in the last 12 months

	No	Yes	Don't know	
Virus checking or protection software?				Software which detects and responds to malicious programs such as viruses, trojans and worms.
A firewall?				Software or hardware that controls access into and out of a network or a computer.
Anti-spyware software?				Software which detects and removes spyware from a computer system (spyware is tracking software which gathers user information without the user's knowledge).

Question 23 in Section B is a question on barriers to Internet purchasing and is directed to individuals who are Internet users but have not purchased over the Internet (in the last 12 months). Relevant response categories are:

- Security concerns (for example, worried about giving debit or credit card details over the Internet).
- Privacy concerns (worried about giving personal details over the Internet).
- Trust concerns (worried about warranties, receiving goods or services, or returning goods).

What were ALL the reasons for not buying or ordering goods or services for private use over the Internet in the last 12 months?

Population: all in-scope individuals who used the Internet in the last 12 months, but who did not buy or order goods or services for private use over the Internet during that period

Multiple responses allowed

Not interested	☐
Prefer to shop in person or deal personally with a service provider	☐
Security concerns, for example, worried about giving debit or credit card details over the Internet	☐
Privacy concerns, for example, worried about giving personal details over the Internet	☐
Trust concerns, for example, worried about warranties, receiving goods or services, or returning goods	☐
Lack of confidence, knowledge or skills	☐
Speed of connection is too slow	☐
Other (please specify)……..……	☐

Feasibility of additional trust material for the model questionnaire

Delegates to the 2005 WPIIS meeting were asked for their views on the statistical feasibility of the following types of questions and to offer any experience in testing or asking such questions.

- Whether households which use anti-virus software download virus definitions and, if so, whether this is done automatically, daily, weekly etc. (such a question could be at the household or individual level).

- Whether households which use the Internet apply patches or software updates which are critical to the security of their computer, and if so, whether this is done automatically, daily, weekly etc (such a question could be at the household or individual level).

- Whether individuals regularly back up their important files, *e.g.* documents, spreadsheets, e-mails, digital photos.

- Which sources individuals use to find information about IT security issues (*e.g.* newspapers, TV, Vendor Web sites, government Web sites etc).

Feedback from the Working Party

General feedback from Eurostat and others is that it is problematic asking individuals about IT security in terms of: the incidents they have encountered, what action they take to protect themselves and whether the computer they use at home is protected. Feedback on the inclusion of the new topics outlined above was couched in similar terms, that is, respondents are unlikely to be able to respond to such technical questions. The only exception appears to be whether individuals regularly back up important files. This is a question successfully asked by Finland and a new non-core question (Q8) on this topic has been added to the model questionnaire. While the general feedback on IT security questions was sceptical, they are of such policy importance that they have been retained as **non-core** questions in the revised model questionnaire. One change made as a result of feedback is to limit questions 8 (on data backup) and 15 (on incidents experienced) to **home use** as this is the environment about which users are likely to know most and over which they have most control (for instance, they may have no role in backing up material at work, nor knowledge about attacks on the computer they use at school).

ANNEX 3: SELECTED STATISTICS ON TRUST FROM PRIVATE AND SEMI-OFFICIAL SOURCES

Table 1. **Reasons for not buying over the Internet in EU countries, 2003 (%)**

	You do not have access to Internet	**You do not trust Internet**	Using Internet is too expensive	You are not interested in buying anything on the Net	Buying anything over Internet is too complicated	Internet is too complicated	You have no credit cards	You do not understand the language well enough	Other reasons	Don't know
Austria	58	**20**	7	34	8	7	10	4	9	0
Belgium	55	**31**	4	35	5	6	8	2	7	1
Denmark	46	**31**	4	34	9	8	9	3	7	1
Finland	46	**22**	3	41	10	6	12	7	8	3
France	66	**31**	8	22	8	7	5	2	5	2
Germany	64	**20**	9	36	10	9	7	3	3	2
Greece	56	**27**	3	29	4	4	5	5	6	3
Ireland	50	**16**	4	24	6	5	14	2	5	8
Italy	47	**26**	3	23	3	4	8	1	5	1
Luxembourg	42	**34**	3	28	5	7	7	1	8	2
Netherlands	36	**32**	7	33	7	6	16	4	11	1
Portugal	57	**20**	7	29	6	9	3	3	11	2
Spain	56	**24**	3	21	5	5	3	3	4	1
Sweden	33	**37**	4	45	13	6	6	5	7	4
UK	58	**22**	2	25	5	7	8	2	9	2
EU15	**57**	**25**	**5**	**28**	**7**	**7**	**7**	**2**	**6**	**2**

Note: This question was asked of the 83% of EU citizens responding to the survey who had not used Internet to make purchases.

Source: European Commission, Special Eurobarometer survey on *European Union public opinion on issues relating to business to consumer e-commerce* (Reference: 201 EB60.0), March 2004.

Table 2. **Concerns about buying over the Internet in EU countries, 2003 (%)**

	Security of payment	Credibility of information on Internet	Delivery (damaged goods, delay, non-delivery, etc.)	Your rights as a consumer being respected	Ability to get a refund	Anonymity of sellers	I am not worried	Other	Don't know
Austria	35	22	26	13	25	19	34	2	0
Belgium	53	20	35	14	32	8	25	1	2
Denmark	41	19	33	18	33	8	31	0	0
Finland	36	24	34	18	38	28	25	0	2
France	51	20	44	25	36	16	21	0	0
Germany	38	32	40	21	42	20	23	0	1
Greece	50	23	36	8	27	10	25	3	0
Ireland	45	24	21	18	21	8	31	1	2
Italy	61	26	32	19	43	11	21	2	0
Luxembourg	61	31	42	19	34	15	16	2	2
Netherlands	39	23	35	18	37	15	30	2	1
Portugal	54	30	46	29	24	18	13	0	0
Spain	61	32	29	31	41	8	9	0	2
Sweden	47	17	38	17	40	11	26	0	1
UK	58	29	34	24	37	19	24	1	1
EU15	48	27	36	23	38	16	23	1	1

Note: This question was asked of the 16% of EU citizens who have used Internet to make purchases.

Source: European Commission, Special Eurobarometer survey on *European Union public opinion on issues relating to business to consumer e-commerce* (Reference: 201 EB60.0), March 2004.

Table 3. **Internet trust marks awareness in EU countries, 2003 (%)**

	Yes	No	Don't know
Austria	19	76	5
Belgium	9	86	5
Denmark	16	83	1
Finland	11	82	7
France	9	89	3
Germany	15	77	9
Greece	7	85	9
Ireland	10	86	4
Italy	6	90	4
Luxembourg	13	84	2
Netherlands	14	80	6
Portugal	6	92	2
Spain	7	85	9
Sweden	8	86	6
UK	8	88	4
EU15	**10**	**85**	**6**

Note: In the context of the Internet, have you ever heard of Internet trust marks? This question was asked to all respondents.

Source: European Commission, Special Eurobarometer survey on *European Union public opinion on issues relating to business to consumer e-commerce* (Reference: 201 EB60.0), March 2004.

Table 4. **Security of payment data awareness in EU countries, 2003 (%)**

	Yes	No	Don't know
Austria	17	74	9
Belgium	13	81	6
Denmark	30	68	2
Finland	22	70	8
France	24	73	3
Germany	21	69	9
Greece	6	86	9
Ireland	18	77	5
Italy	18	76	6
Luxembourg	22	75	4
Netherlands	33	59	8
Portugal	10	88	2
Spain	11	80	8
Sweden	32	61	8
UK	27	70	4
EU15	**21**	**73**	**6**

Note: In the context of the Internet, have you ever heard of statements about the security of payment data? This question was asked to all respondents.

Source: European Commission, Special Eurobarometer survey on *European Union public opinion on issues relating to business to consumer e-commerce* (Reference: 201 EB60.0), March 2004.

Table 5. **Protection of personal data awareness in EU countries, 2003 (%)**

	Yes	No	Don't know
Austria	25	68	7
Belgium	14	80	6
Denmark	32	66	2
Finland	24	68	8
France	20	77	4
Germany	25	66	9
Greece	9	82	9
Ireland	21	75	4
Italy	29	67	4
Luxembourg	26	72	3
Netherlands	38	56	6
Portugal	12	86	2
Spain	16	76	8
Sweden	33	59	8
UK	28	68	4
EU15	**24**	**70**	**6**

Note: In the context of the Internet, have you heard of statements about protecting personal data? This question was asked to all respondents.

Source: European Commission, Special Eurobarometer survey on *European Union public opinion on issues relating to business to consumer e-commerce* (Reference: 201 EB60.0), March 2004.

Table 6. **Internet users' fears in US, 2000 (%)**

	Concerned	Not concerned
Businesses and people you don't know getting personal information about you and your family	84	15
Computer hackers getting your credit card number online	68	30
Having unqualified people give you medical information online	54	43
That you'll get a computer virus when you download information	54	45
Seeing false or inaccurate news reports online	49	49
People spreading false rumors online to affect stock prices	47	50
People you meet online lying about who they really are	39	48
Someone might know what Web sites you've visited	31	68
Your email will be read by someone besides the person you sent it to	27	72

Source: Pew Internet & American Life Project May-June 2000 Poll.

Table 7. **Internet users' fears in US, 1998 and 2000 (%)**

	1998	2000
Your email will be read by someone besides the person you sent it to	20	27
Someone might know what Web sites you've visited	21	31
That you'll get a computer virus when you download information	42	54

Sources: Pew Internet & American Life Project May-June 2000 Poll and The Pew Research Center for the People and the Press 1998.

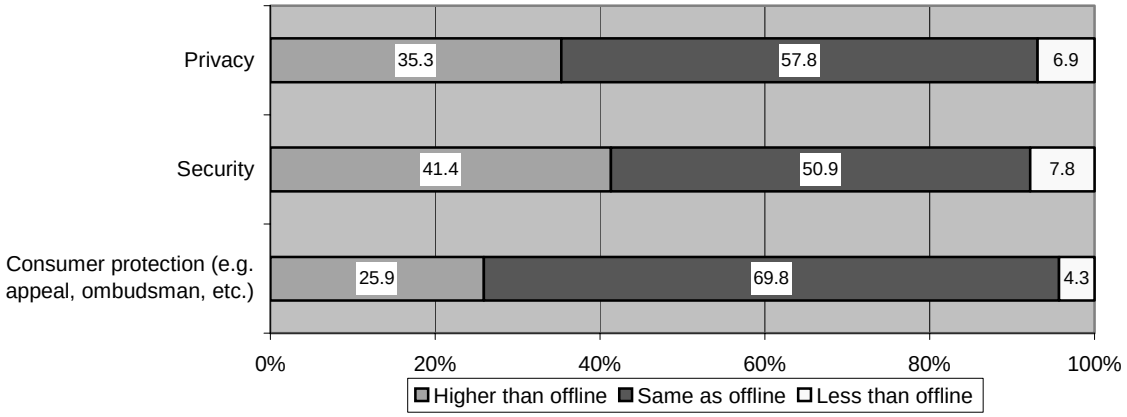
Table 8. **Awareness of being tracked in US, 2000 (%)**

	Know what a "cookie" is	Refuse "cookies"
All Internet users	43	10
Internet users who had clicked on an ad	51	12
Internet users who had bought a product online	56	11

Source: Pew Internet & American Life Project May-June 2000 Poll.

Figure 1. **Results of OECD e-government survey, Denmark**

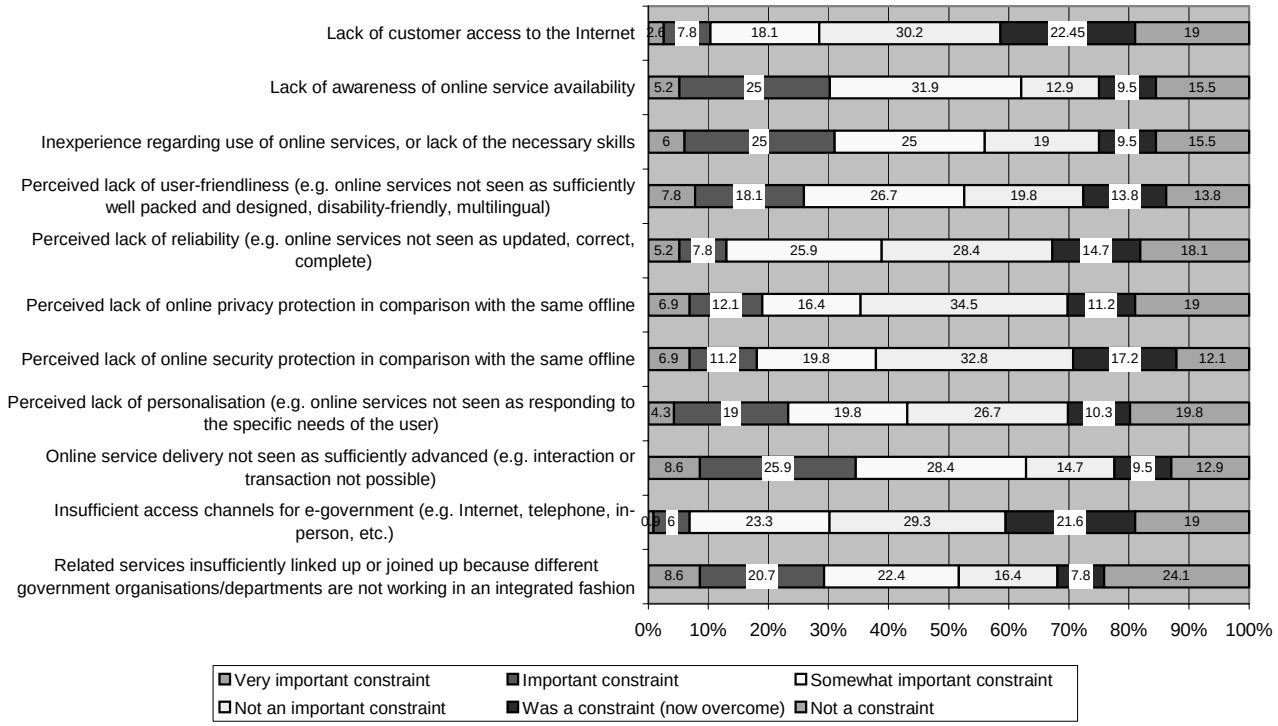
Q.3.5 Do you think that online processes in your organisation have the same equivalent level of protection as the same processes offline, with regard to:



Source: OECD GOV E-Government Survey.

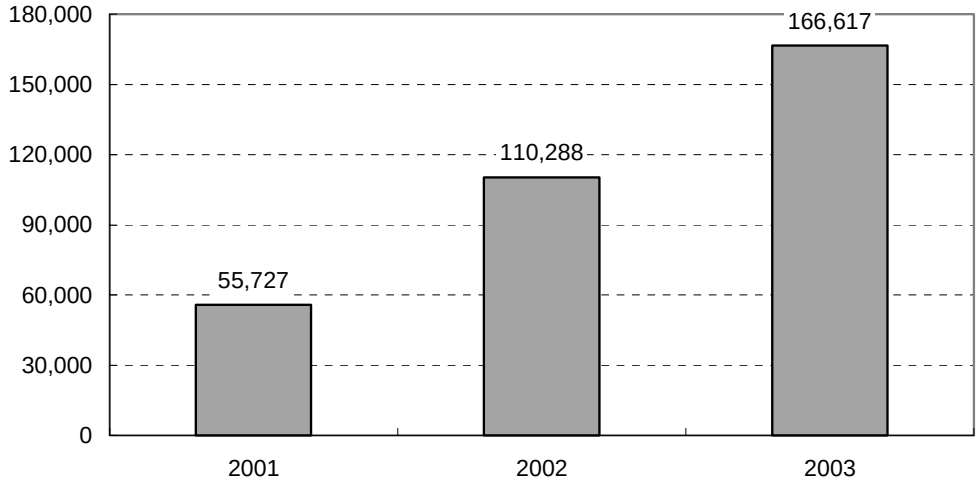
Figure 2. **Results of OECD e-government survey, Denmark**

Q. 7.4 Do the following constrain consumer demand for the online services provided by your organisation and, if so, how important are they?



Source: OECD GOV E-Government Survey.

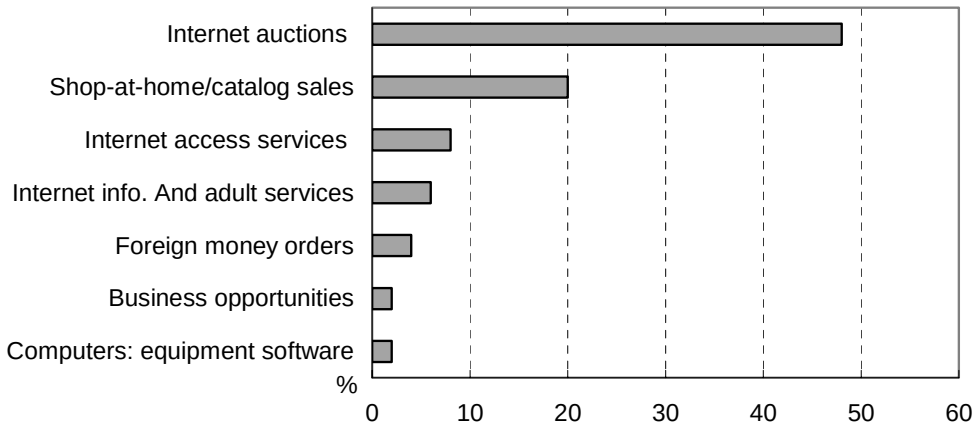
Figure 3. **Consumer Sentinel, Internet-related fraud complaints, 2001-2003**



1. Consumer Sentinel data cover total internationally reported fraud complaints.

Source: FTC, http://www.consumer.gov/sentinel/states03/3year_trends.pdf, September 13, 2004.

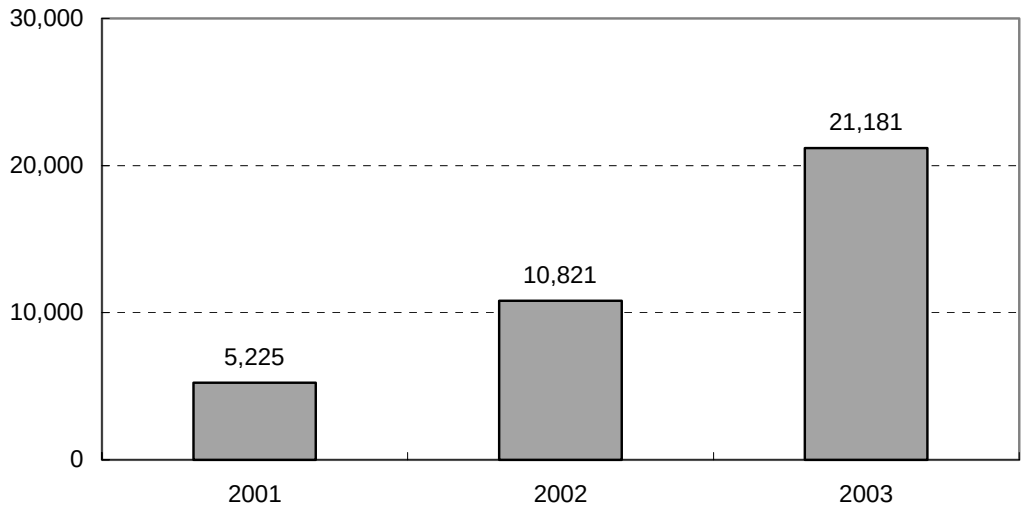
Figure 4. **Consumer Sentinel, top products/services for Internet-related fraud complaints**[1]
January 1 – December 31, 2003



1. Percentages are based on the total number of Internet-related complaints (166 617) received between January 1 and December 31, 2003.

Source: FTC, http://www.consumer.gov/sentinel/states03/internet_related_trends.pdf, September 13, 2004.

Figure 5. **Consumer Sentinel, cross-border Internet-related fraud complaints, 2001-2003**



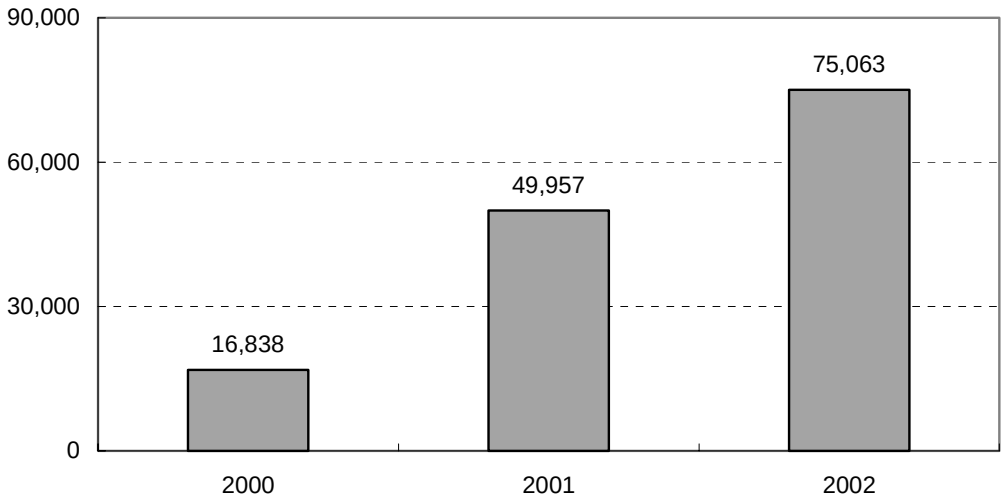
Source: FTC, http://www.ftc.gov/opa/2004/03/cbcy2003.pdf, September 15, 2004.

Table 9. **Consumer Sentinel, top consumer and company locations, January 1-June 30 2004**

Top consumer locations complaints		**Top company locations complaints**	
United States	2 774	United States	791
United Kingdom	138	United Kingdom	449
Canada	109	Netherlands	184
Australia	105	Canada	174
France	27	Spain	147
New Zealand	22	Nigeria	130
India	21	South Africa	75
Sweden	17	Australia	72
Belgium	15	Italy	64
Germany	15	Germany	63

Source: FTC, http://www.econsumer.gov/english/contentfiles/pdfs/PU15%20-%20Jan-Jun%202004.pdf, September 15, 2004.

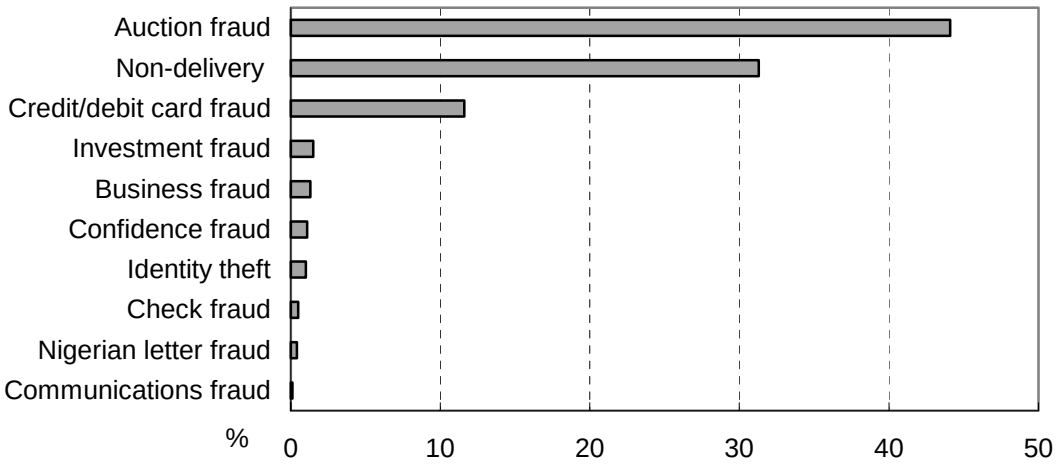
Figure 6. **IFCC, Internet-related fraud complaints, 2000-2002**



1. IFCC data are for the United States.

Source: http://www.ifccfbi.gov/strategy/2002_IFCCReport.pdf, September 15, 2004.

Figure 7. **IFCC, top ten Internet-related fraud complaints**[1]
January 1 – December 31, 2002



1. Percentages are based on the total number of Internet-related complaints (75 063) received between January 1 and December 31, 2002.

Source: IFCC, http://www.consumer.gov/sentinel/states03/internet_related_trends.pdf, September 13, 2004.

Table 10. **Countries hosting phishing sites**

	Total phishing sites (%), June 2004	Total phishing sites (%), December 2004
United States	27	32
Korea (South)	20	11
China	16	12
Chinese Taipei	7	
Netherlands	3	
Mexico	2	
Uruguay	2	
Turkey	2	
Brazil	1	2.7
Croatia	1	
United Kingdom	1	
Thailand	1	
Portugal	1	
Poland	1	
Sweden	1	
Madagascar	1	
Russia	1	
Spain	1	
Unable to Trace	10	
Japan		2.8
Germany		2.7
France		2.7
Romania		2.2
Canada		2.1
India		2.1

Source: Anti Phishing Working Group.

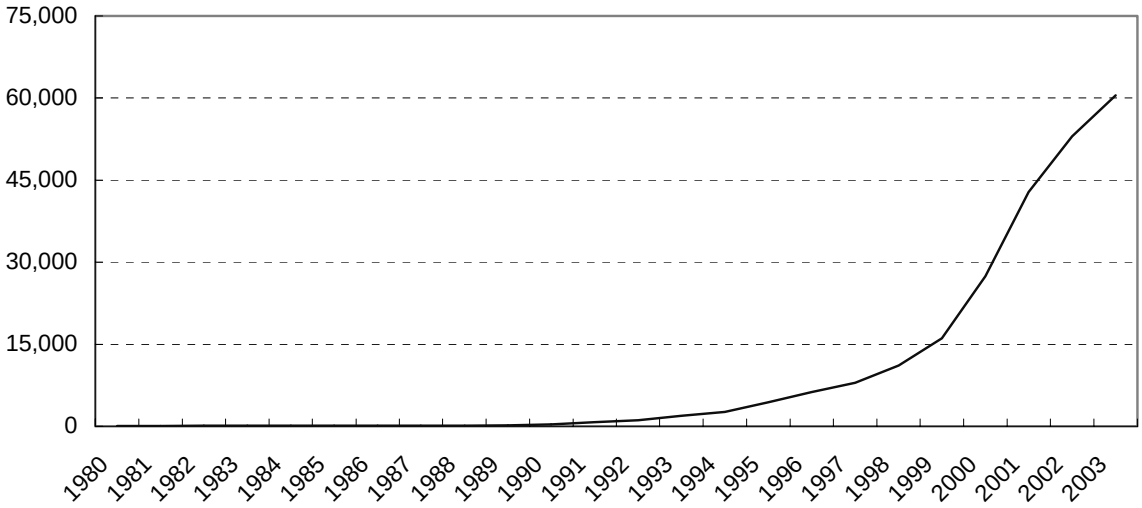
Table 11. **Phishing sites by country as recorded by Netcraft's toolbar**

Country	Country TLD Code	Total sites	Phishing sites	% of known phishing sites	Probability of phishing site (1)
Syria	SY	58	4	0.1	1 in 14
Cameroon	CM	49	1	0.0	1 in 49
Northern Mariana Islands	MP	153	1	0.0	1 in 153
Brunei Darussalam	BN	302	1	0.0	1 in 302
Jamaica	JM	328	1	0.0	1 in 328
Pakistan	PK	4 035	10	0.2	1 in 403
Chinese Taipei	TW	79 823	188	4.2	1 in 424
Philippines	PH	8 250	18	0.4	1 in 458
Armenia	AM	541	1	0.0	1 in 541
Viet Nam	VN	2 481	4	0.1	1 in 620
Honduras	HN	639	1	0.0	1 in 639
Romania	RO	41 772	65	1.5	1 in 642
Belarus	BY	1 944	3	0.1	1 in 648
Namibia	NA	696	1	0.0	1 in 696
Iran	IR	4 338	6	0.1	1 in 723
Bolivia	BO	1 820	2	0.0	1 in 910
Mongolia	MN	952	1	0.0	1 in 952
Nicaragua	NI	962	1	0.0	1 in 962
Palestine Territory	PS	977	1	0.0	1 in 977
Ecuador	EC	2 957	3	0.1	1 in 985
Paraguay	PY	1 988	2	0.0	1 in 994
Colombia	CO	10 864	10	0.2	1 in 1 086
Bahamas	BS	1 164	1	0.0	1 in 1 164
Egypt	EG	8 705	7	0.2	1 in 1 243
Russian Federation	RU	299 078	168	3.7	1 in 1 780
Lithuania	LT	12 558	7	0.2	1 in 1 794
India	IN	102 659	54	1.2	1 in 1 901
Sri Lanka	LK	1 941	1	0.0	1 in 1 941
Morocco	MA	7 931	4	0.1	1 in 1 982
Guatemala	GT	2 078	1	0.0	1 in 2 078
Malaysia	MY	48 384	23	0.5	1 in 2 103
Korea	KR	1 026 567	486	10.8	1 in 2 112
Costa Rica	CR	6 525	3	0.1	1 in 2 175
Kenya	KE	2 207	1	0.0	1 in 2 207
Brazil	BR	219 287	98	2.2	1 in 2 237
Puerto Rico	PR	2 290	1	0.0	1 in 2 290
Indonesia	ID	24 220	10	0.2	1 in 2 422
Peru	PE	4 877	2	0.0	1 in 2 438
Thailand	TH	64 264	26	0.6	1 in 2 471
Argentina	AR	161 173	59	1.3	1 in 2 731
Hong Kong, China	HK	146 847	53	1.2	1 in 2 770
Chile	CL	70 499	23	0.5	1 in 3 065
China	CN	1 159 391	350	7.8	1 in 3 312
Panama	PA	3 371	1	0.0	1 in 3 371
Mexico	MX	59 926	14	0.3	1 in 4 280
Bulgaria	BG	39 542	7	0.2	1 in 5 648
Iceland	IS	12 486	2	0.0	1 in 6 243
Uruguay	UY	19 385	3	0.1	1 in 6 461
Turkey	TR	160 215	24	0.5	1 in 6 675
Poland	PL	248 603	34	0.8	1 in 7 311

1. As ranked by Netcraft.

Source: Netcraft (5 April 2005).

Figure 8. **Spyware in figures**
All pests counts by year, 1980–2003[1]



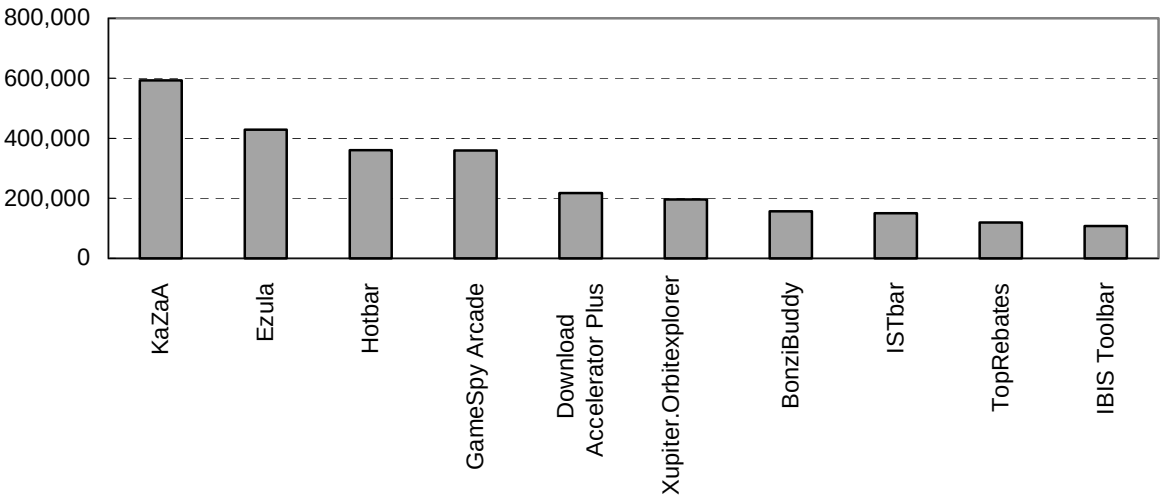
1. Last revised Saturday, December 13, 2003.

This graph shows the cumulative number of pests categorized as "All pests". The value for each year represents the approximate number of such pests in existence in that year. Note that such figures are likely to be underestimated, with the greatest underestimation likely of new pests for recent years, since these are sometimes less likely to be prevalent or found in collections.

Values are cumulated from year-to-year because trojans and other pests never become "extinct." Their probability of being encountered may change, of course.

Source: http://research.pestpatrol.com/Trends/All_Pests_Counts_by_Year.asp, October 5, 2004.

Figure 9. **Top ten pests in the past 28 days**[1]

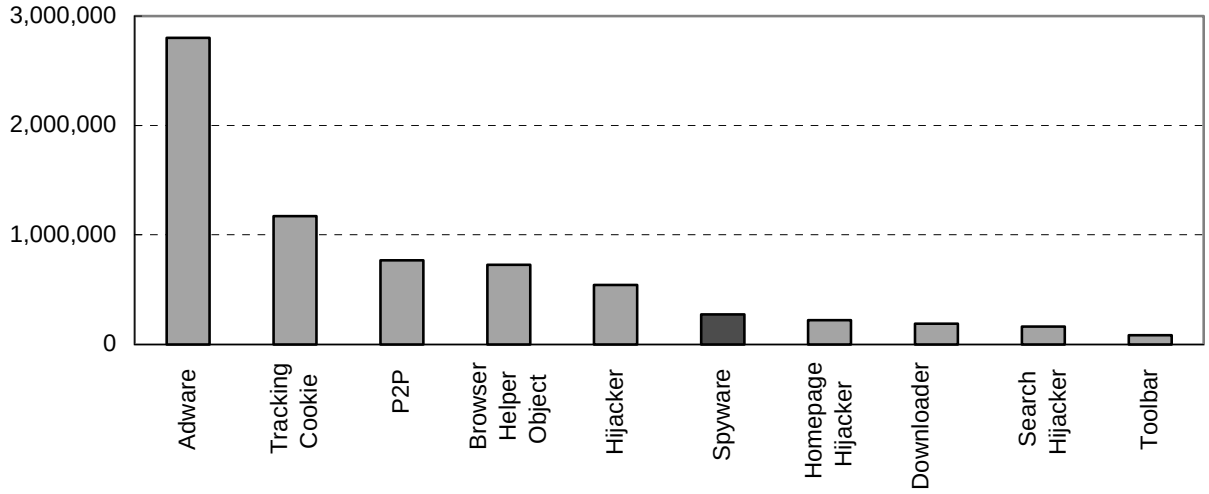


1. Last updated Tuesday, October 5, 2004.

This graph summarizes the top ten pests totalling 2 688 751 of a total of 6 618 454 pest reports from PestPatrol users for the past 28 days. In these tabulations, each report is of a single "object", such as a registry entry, file, or directory. A total of 1 996 unique pests were reported.

Source: http://research.pestpatrol.com/Lists/MostPrevalentPests.asp, October 5, 2004.

Figure 10. **Top ten types of pests in the past 28 days**[1]

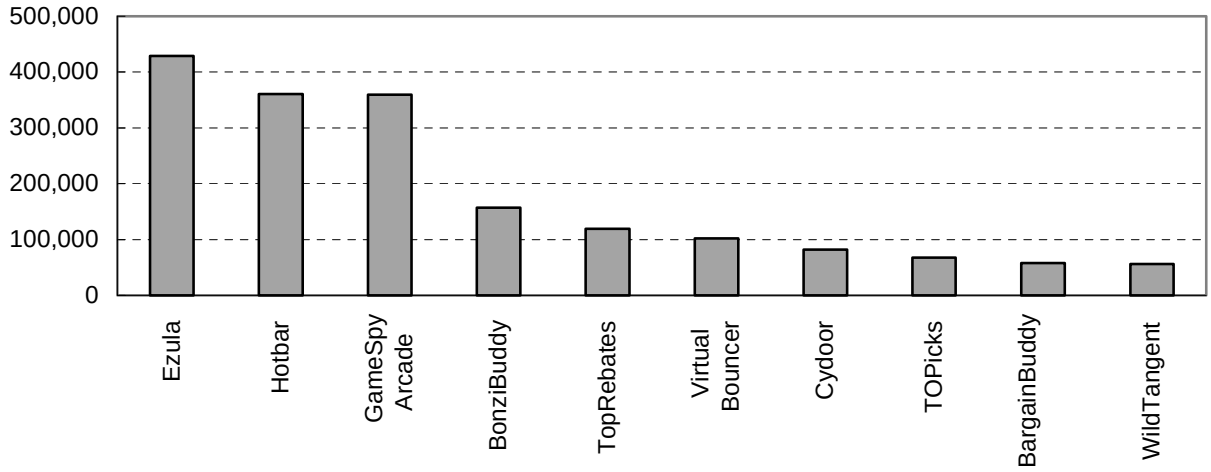


1. Last Updated Tuesday, October 5, 2004.

The graph summarizes by category 6 937 456 of a total of 7 153 591 pest reports from PestPatrol users for the 28 days. In these tabulations, each report is of a single "object", such as a registry entry, file, or directory. A total of 2 253 unique pests were reported.

Source: http://research.pestpatrol.com/Lists/MostPrevalentPests.asp, October 5, 2004.

Figure 11. **Top 10 spyware programmes eliminated in the past 28 days**[1]



1. Last Updated Tuesday, October 5, 2004.

Table 12 below is drawn from a total of 6 546 623 pest reports from PestPatrol users for the past month. This graph shows the most common pests in the category "All Spyware (includes Trackware and Adware. Spyware Cookies are excluded)."

Source: http://research.pestpatrol.com/Lists/TopTenPestsByType.asp, October 5, 2004.

Table 12. **Bot-infected computers by country (July-December 2004)**

Country	Bot-infected computers (% of total)
United Kingdom	25.2
United States	24.6
China	7.8
Canada	4.9
Spain	3.8
France	3.6
Germany	3.5
Chinese Taipei	3.1
Korea	3.0
Japan	2.6
Rest of World	17.9

Source: Symantec Internet Security Threat Report (Published March 2005).

Table 13. **Bot-infected computers by country (July-December 2004)**

Country	Bot-infected computers (July 2004-December 2004)	Bot-infected computers per 10 000 inhabitants	Bot-infected computers per 100 broadband subscribers (1)	Share of OECD broadband subscribers September 2004) (%)	Share of OECD bot-Infected computers (%)
Australia	9 650	4.8	0.74	1.23	1.29
Austria	4 235	5.2	0.57	0.70	0.57
Belgium	3 469	3.3	0.22	1.46	0.47
Canada	43 609	13.8	0.81	5.03	5.85
Czech Republic	884	0.9	0.65	0.13	0.12
Denmark	6 855	12.7	0.72	0.90	0.92
Finland	4 091	7.8	0.64	0.60	0.55
France	31 874	5.2	0.58	5.16	4.28
Germany	31 035	3.8	0.53	5.54	4.16
Greece	574	0.5	1.77	0.03	0.08
Hungary	1 682	1.7	0.57	0.28	0.23
Iceland	337	11.6	0.72	0.04	0.05
Ireland	466	1.2	0.48	0.09	0.06
Italy	19 092	3.3	0.49	3.66	2.56
Japan	22 712	1.8	0.13	16.21	3.05
Korea	26 660	5.6	0.23	11.07	3.58
Luxembourg	186	4.1	0.54	0.03	0.02
Mexico	2 578	0.3	0.40	0.61	0.35
Netherlands	7 635	4.7	0.26	2.70	1.02
New Zealand	647	1.6	0.40	0.15	0.09
Norway	3 696	8.1	0.66	0.53	0.50
Poland	7 411	1.9	1.01	0.69	0.99
Portugal	17 205	16.5	2.30	0.70	2.31
Slovak Republic	224	0.4	0.52	0.04	0.03
Spain	34 076	8.4	1.18	2.71	4.57
Sweden	13 172	14.7	1.11	1.11	1.77
Switzerland	6 724	9.1	0.58	1.09	0.90
Turkey	1 691	0.2	0.69	0.23	0.23
United Kingdom	223 836	37.7	4.25	4.95	30.04
United States	218 911	7.5	0.64	32.32	29.38
OECD	745 217	6.5	0.70	100.00	100.00

1. In practice some computers using dial-up would also be infected. This indicator does not try to take this into account and is merely the ratio of total bot-infected computers (which would include dial-up) to broadband subscribers.

Source: Symantec, OECD.

Table 14. **SSL certification market share (July 2004)**

Company	Market share (%)
Verisign (including Thawte)	39
RSA data security (including Verisign certificates)	22
Geotrust	19
Comodo	11
Other	9
Total	100

Source: OECD based on Netcraft surveys (www.netcraft.com).

Table 15. **Secure servers in the OECD area**

	Secure servers July 1998	Secure servers July 1999	Secure servers July 2000	Secure servers July 2001	Secure servers July 2002	Secure servers July 2003	Secure servers July 2004	Per 100 000 inhabitants (July 1998)	Per 100 000 inhabitants (July 1999)	Per 100 000 inhabitants (July 2000)	Per 100 000 inhabitants (July 2001)	Per 100 000 inhabitants (July 2002)	Per 100 000 inhabitants (July 2003)	Per 100 000 inhabitants (July 2004)
Australia	632	1 305	2 828	3 704	4 693	4 830	8 079	3.4	6.9	14.7	19.0	23.8	24.5	40.9
Austria	98	241	447	881	949	1 073	1 590	1.2	3.0	5.6	11.0	11.8	13.3	19.7
Belgium	52	159	268	431	439	512	912	0.5	1.6	2.6	4.2	4.2	5.0	8.8
Canada	929	1 789	3 896	6 050	7 768	9 378	15 166	3.1	5.9	12.7	19.4	24.7	29.9	48.3
Czech Republic	19	88	194	383	185	213	315	0.2	0.9	1.9	3.7	1.8	2.1	3.1
Denmark	44	112	289	523	660	890	1 681	0.8	2.1	5.4	9.8	12.3	16.5	31.2
Finland	68	180	343	660	744	870	1 255	1.3	3.5	6.6	12.7	14.3	16.7	24.1
France	222	632	1 297	1 969	2 511	2 646	3 799	0.4	1.0	2.1	3.2	4.1	4.3	6.2
Germany	492	1 630	3 761	6 442	7 987	7 912	13 163	0.6	2.0	4.6	7.8	9.7	9.6	16.0
Greece	8	48	87	176	170	181	270	0.1	0.4	0.8	1.6	1.6	1.7	2.5
Hungary	18	26	90	165	86	122	199	0.2	0.3	0.9	1.6	0.8	1.2	2.0
Iceland	13	29	67	91	136	170	249	4.7	10.5	23.8	31.9	47.3	59.1	86.6
Ireland	56	97	245	467	579	701	1 201	1.5	2.6	6.4	12.1	14.8	17.9	30.7
Italy	167	432	795	1 264	1 167	1 327	1 977	0.3	0.7	1.4	2.2	2.0	2.3	3.4
Japan	429	1 170	2 900	7 952	7 179	10 513	19 610	0.3	0.9	2.3	6.2	5.6	8.2	15.4
Korea	38	106	243	397	562	623	878	0.1	0.2	0.5	0.8	1.2	1.3	1.8
Luxembourg	11	26	44	68	97	104	184	2.6	6.0	10.0	15.4	21.7	23.3	41.2
Mexico	26	58	176	310	324	379	605	0.0	0.1	0.2	0.3	0.3	0.4	0.6
Netherlands	127	306	541	1 064	1 332	1 723	3 595	0.8	1.9	3.4	6.6	8.2	10.7	22.3
New Zealand	90	227	482	778	983	1 124	1 668	2.4	5.9	12.4	19.9	24.7	28.3	42.0
Norway	55	130	273	491	528	666	1 122	1.2	2.9	6.1	10.9	11.6	14.7	24.7
Poland	23	61	188	467	373	382	557	0.1	0.2	0.5	1.2	1.0	1.0	1.5
Portugal	27	59	116	192	214	286	443	0.3	0.6	1.1	1.9	2.1	2.8	4.3
Slovak Republic	15	..	45	110	38	47	61	0.3	..	0.8	2.0	0.7	0.9	1.1
Spain	239	432	759	1 194	1 315	1 764	2 745	0.6	1.1	1.9	3.0	3.2	4.4	6.8
Sweden	145	406	811	1 261	1 246	1 437	2 826	1.6	4.6	9.1	14.2	14.0	16.1	31.7
Switzerland	152	401	854	1 370	1 555	1 769	2 826	2.1	5.6	11.8	18.9	21.2	24.1	38.5
Turkey	7	50	116	285	400	432	855	0.0	0.1	0.2	0.4	0.6	0.6	1.2
United Kingdom	714	1 735	4 404	7 916	10 288	11 714	20 339	1.2	3.0	7.5	13.4	17.4	19.8	34.4
United States	14 674	32 053	65 565	86 025	106 884	120 661	197 769	5.3	11.5	23.2	30.2	37.2	42.0	68.8
OECD	19 590	43 988	92 124	133 086	161 392	184 449	305 939	1.8	3.9	8.2	11.7	14.1	16.1	26.7

Source: OECD based on Netcraft surveys (www.netcraft.com).

NOTES

1. The OECD Working Party on Information Security and Privacy (WPISP) promotes an internationally co-ordinated approach to policy making in security and protection of privacy and personal data in order to help build trust. A note on terminology: this report uses the term "trust in the online environment" to cover a number of aspects of trust, including security of the IT environment and information placed in that environment, privacy protection and other trust issues such as consumer protection and concerns on aspects of the online environment such as Web sites which are perceived to be harmful (*e.g.* to children).

2. OECD, "Key ICT Indicators", http://www.oecd.org/document/23/0,2340,en_2649_34225_33987543_1_1_1_1,00.html.

3. Refer to http://www.whitehouse.gov/omb/memoranda/m03-19.pdf.

4. Refer to http://www.gao.gov/highlights/d04483thigh.pdf.

5. Refer for example to Jonathan Cave, "The Economics of Trust Between Cyber Partners", http://www.foresight.gov.uk/previous_projects/cyber_trust_and_crime_prevention/reports_and_publications/index.html and the papers from the Fourth Workshop on the Economics of Information Security, Kennedy School of Government, Harvard University, 2-3 June 2005 http://infosecon.net/workshop/schedule.php.

6. For questionnaires and background to the survey, see http://www.census.gov/eos/www/css/css.html.

7. http://europa.eu.int/comm/public_opinion/index_en.htm.

8. http://europa.eu.int/comm/consumers/topics/btoc_ecomm.pdf. The study involved face-to-face interviews with 16 207 EU15 citizens.

9. European Commission, "Data Protection", Special Eurobarometer, December 2003 http://europa.eu.int/comm/public_opinion/archives/ebs/ebs_196_highlights.pdf.

10. Verisign, "Enhanced VeriSign Secured™ Seal Enables Consumers to Verify E-Commerce Site Security Prior to Transacting Business Online", News Release, 2 November 2004. http://www.verisign.com/verisign-inc/news-and-events/news-archive/us-news-2004/page_017440.html.

11. The online sample consisted of 2 237 adults nationwide and was comprised of 1 073 men and 1 164 women – 18 years of age or older. The online sample of those who have made a purchase online at some point in their lives consisted of 2 027 adults nationwide and was comprised of 987 men and 1 040 women – 18 years of age or older.

12. Susan Kuchinskas, "VeriSign Strengthens Secured Seal", 17 November 2004. http://www.ecommerce-guide.com/essentials/paypal/article.php/3436811.

13. Verisign, "Enhanced VeriSign Secured™ Seal Enables Consumers to Verify E-Commerce Site Security Prior to Transacting Business Online", Opcit.

14 AOL/NCSA Online Saftey Study, October 2004. http://www.staysafeonline.info/news/safety_study_v04.pdf.

15. Dr. Malte Krueger and Kay Leibold, "Internet Payment Systems: The Consumers' View", Karlsruhe, November 2004.

16. George Danezis, Stephen Lewis and Ross Anderson, "How much is privacy location worth", Paper dated February 2005 to be presented at the Fourth Workshop on the Economics of Information Security, Kennedy School of Government, Harvard University, 2-3 June 2005, http://infosecon.net/workshop/pdf/38.pdf.

17. For example: Nielsen//NetRatings, "Over 18 million Europeans bank online, but they trust traditional banking brands on the Internet", Press Release, 20 November 2002.

18. Rob O'Neill, "Banks wary of online monitoring", *The Age*, 22 March 2005. http://www.theage.com.au/articles/2005/03/21/1111253920118.html.

19. http://www.pewinternet.org/pdfs/PIP_Trust_Privacy_Report.pdf. Between May to June 2000, the Pew Internet & American Life Project surveyed 2 117 adult (over 18 years old) Americans, 1 017 of whom were Internet users. The interviews were conducted by telephone.

20. Consumer Reports "Net Threat Rising", (Dated September 2005), http://www.consumerreports.org

21. http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf.

22. http://www.csoonline.com/releases/ecrimewatch04.pdf.

23. AusCERT, "Computer Crime and Security Survey", 2004. http://www.auscert.org.au/render.html?it=2001.

24. Refer for example to the 2002 survey at: http://www.btglobalservices.com/en/products/trustservices/docs/security_breaches_2002.pdf.

25. Refer NHTCU, "High Tech Crime: The Impact on UK Business", 2004. http://www.nhtcu.org/NOP%20Survey.pdf.

26. Bill Goodwin, "E-crime is costing UK business £2.4bn a year, says police report", Computerweekly.com, 5 April 2005. http://www.computerweekly.com/articles/article.asp?liArticleID=137740&liArticleTypeID=1&liCategoryID=6&liChannelID=22&liFlavourID=1&sSearch=&nPage=1.

27. Refer to: www.vm.fi/tiedostot/pdf/fi/95054.pdf

28. www.asimelec.es The study is at: http://www.asimelec.es/pdf/seguridad/asimelec%20estudio%20mercado%20ISO17799-021024.pdf.

29. "Survey Reveals that Consumers and Tech Professionals Share Concern About Cybercrime, But Only 19.5 Percent of Consumers And 48.9 Percent of Tech Professionals Currently Use a Personal Firewall", News Release, 29 June 2004, http://www.symantec.com/press/2000/n000629a.html. A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Refer: http://www.webopedia.com/TERM/f/firewall.html.

30. Sarah Gordon, "Privacy: A Study of Attitudes and Behaviours in the US, UK and EU Information Security Professionals", Symantec White Paper, 2004. http://securityresponse.symantec.com/avcenter/reference/privacy.attitudes.behaviors.pdf.

31. Deloitte, "2004 Global Security Survey", 2004, http://www.deloitte.com/dtt/cda/doc/content/GFSISE.pdf.

32. PLS RAMBOLL, "E-business Nordic.com 2003", Aarhus, November 2003.

33. http://www.consumer.gov/sentinel/. and http://www.ftc.gov/.

34. http://www.ifccfbi.gov/.

35. http://www.ifccfbi.gov/strategy/statistics.asp.

36. http://www.fraud.org/internet/intinfo.htm.

37. http://www.fraud.org/2004-internet%20scams.pdf.

38. http://www.fraud.org/2003internetscams.pdf.

39. http://www.econsumer.gov/english/index.html.

40. http://www.icpen.org.

41. http://www.econsumer.gov/english/contentfiles/pdfs/PU15%20-%20Jan-Jun%202004.pdf.

42. Symantec, "Internet Security Threat Report", Trends for 1 January–30 June 2004, September 2004. http://www.symantec.com/region/se/seresc/download/istr_sept_2004.pdf.

43. http://www.census.gov/mrts/www/current.html.

44. Visa, "VISA EU 2003 Annual Results", Press Pelease, April 2004, http://www.visaeu.com/pressandmedia/press188_pressreleases.html.

45. APACS, "10 per cent of all credit card payments now made on-line", Press Release, 5 August 2004, http://www.apacs.org.uk.

46. Visa Quarterly Report, April-June 2004, http://usa.visa.com/media/global/Q22004.pdf.

47. Overall fraud rates are available at: http://usa.visa.com/personal/newsroom/fraud_security.html?it=il_/personal/site_map/visa_analyst_center.html.

48. http://www.mastercardintl.com/newsroom/programs_faqs.html#fraud.

49. Susanne Schnorr-Bäcker, Federal Statistics Office, Germany, "Towards the knowledge society: ICT regarding households and individuals in Germany", paper presented to the WSIS Thematic Meeting on Measuring the Information Society, Geneva, 7-9 February 2005. These data refer only to the former territory of the Federal Republic including the whole of Berlin.

50. There are other offences that may be related to the use of ICT not included under this grouping.

51. Schnorr-Bäcker, Op.cit.

52. Refer to http://www.usdoj.gov/opa/pr/2004/August/04_crm_583.htm consulted October 6, 2004.

53. ACPR, Standardisation of Definitions of Identity Crime Terms, Discussion Paper, May 2004, http://www.acpr.gov.au/pdf/Standdefinit.pdf.

54. Australian Bureau of Statistics, "Development of e-crime statistics", National Crime Statistics Unit, Unpublished, 21 September 2004.

55. http://www.austrac.gov.au/policy/DEFINITIONSjoint.pdf.

56. Federal Deposit Insurance Corporation (FDIC), "Putting an End to Account-Hijacking Identity Theft", 14 December 2004, http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

57. Home Office Identity Fraud Steering Committee, Website, 28 February 2005, http://www.identity-theft.org.uk/.

58. Australian centre for Policing Research, "Identity Crime Research and Coordination", February 2005. http://www.acpr.gov.au/research_idcrime.asp and Susan Cuganesan and David Lacey, *Identity Fraud in Australia: An Evaluation of its Nature, Cost and Extent*, cIRCA, September 2003. http://www.austrac.gov.au/publications/identity_fraud/identity_fraud_extract.pdf.

59. FDIC, op.cit.

60. Refer to http://www.enisa.eu.int/ (October 2004).

61. http://www.enisa.eu.int/about/activities/index_en.htm.

62. http://www.enisa.eu.int/.

63. http://www.waarschuwingsdienst.nl/render.html?cid=106.

64. http://www.itsafe.gov.uk/links/international.html.

65. http://www.ahtcc.gov.au/.

66 http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase.

67. The definition of "Pharming" comes from the Ant-Phishing Working Group Web site at: http://www.antiphishing.org/. Netcraft reported an incident of cache poisoning in March 2005: http://news.netcraft.com/archives/2005/03/07/dns_poisoning_scam_raises_wariness_of_pharming.html.

68. Andy Sullivan, "Con artists dial for dollars on Net Phones", Reuters, 20 March 2005. http://msnbc.msn.com/id/7235764/.

69. Brightmail, "Brightmail to Provide Data to EarthLink to Power Anti-Phishing Toolbar", Press Release, 19 April, 2004.

70. Refer for example to APACS, "New Trojan Email Attack targets On-line Banking Customers", Press Release, 13 August 2004. http://www.apacs.org.uk/. An example of a phishing attack can be viewed at http://news.netcraft.com/archives/2005/03/07/phishers_use_wildcard_dns_to_build_convincing_bait_urls.html.

71. http://www.antiphishing.org.

72. APWG, "Commentary to FDIC "Putting an End to Account-Hijacking Identity Theft", 4 February 2005.

73. http://www.trustwatch.com/.

74. http://pages.ebay.com/ebay_toolbar/.

75. Dennis Fisher, "IE 7: No Phishing Allowed", 21 February 2005, http://www.eweek.com/article2/0,1759,1766250,00.asp.

76. http://www.aa419.org/fake-banks/fakebankslist.php?start=1.

77. APACS, "UK card fraud losses reach £504.8m", 8 March 2005 http://www.apacs.org.uk/about_apacs/htm_files/pressreleases.htm.

78. "U.S. Consumer Loss of phishing Fraud to Reach $500 Millon", 29 September 2004, http://www.truste.org/about/press_release/09_29_04.php.

79. Gartner, "Gartner Study Finds Significant Increase in E-Mail Phishing Attacks", 6 May 2004. http://www3.gartner.com/5_about/press_releases/asset_71087_11.jsp.

80. TowerGroup, "Fraud Losses from email phishing attacks to total USD 137 million globally in 2004, Lower than other estimates", 1 December 2004. http://www.towergroup.com/public/presscenter/default_press.asp.

81. Out-Law.com, October 2004, reporting release of APACS statistics. http://www.out-law.com/php/page.php?page_id=apacslaunchesanti1096883491&area=news.

82. Gartner, Op.cit. http://www3.gartner.com/5_about/press_releases/asset_71087_11.jsp.

83. "U.S. Consumer Loss of phishing Fraud to Reach $500 Millon", Op.cit.

84. Duane Wessels, "Searching for DNS Cache Poisoners" DNS-OARC Workshop, Santa Clara, 25-26 July 2005. http://www.caida.org/projects/oarc/200507/slides/oarc0507-Wessels-poisoning.pdf

85. Ibid and http://www.measurement-factory.com/ and https://oarc.isc.org/

86. Refer to http://www.ftc.gov/opa/2004/04/spywaretest.htm.

87. FTC, "Spyware Workshop: Monitoring Software on your PC: Spyware, Adware, and Other Software", Staff Report March 2005. http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf.

88. http://www.antispywarecoalition.org/

89. http://www.antispywarecoalition.org/definitions.pdf

90. PTS, "Spyware and closely related phenomena", 8 April 2005. http://www.pts.se/Archive/Documents/EN/Spyware_eng.pdf

91. John Leyden, "Spyware 'calling home' volumes soar", *The Register*, 25 July 2005. http://www.theregister.co.uk/2005/07/25/spyware_screening/

92. One question that might be raised is how is spyware different from cookies, which have beneficial aspects for users (*e.g.* for recording preferences), but which can record some aspects of Internet use. Some of the main differences are that cookies do not act maliciously, are identifiable, can be deleted at any time and can not spread viruses or access a user's hard drive. Some spyware has, however, been reported to tamper with cookies with the aim of extracting information to open new accounts or to gain access to the user's existing accounts. Refer to http://www.webopedia.com/DidYouKnow/Internet/2002/Cookies.asp and http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci861584,00.html and http://www.w3.org/Security/Faq/wwwsf2.html#CLT-Q10.

93. Refer to http://www.ftc.gov/bcp/workshops/spyware/transcript.pdf, page 12, consulted 5 October, 2004.

94. Refer to http://spywarewarrior.com/asw-test-guide.htm (October 2004).

95. http://research.pestpatrol.com/WhitePapers/Glossary.asp.

96. http://research.pestpatrol.com/.

97. Bryson Gordon, McAfee Security http://www.ftc.gov/bcp/workshops/spyware/transcript.pdf and http://www.ftc.gov/bcp/workshops/spyware/gordon.pdf.

98. Declan McCullagh, "Few solutions pop up at FTC adware workshop", 19 April 2004, http://news.com.com/Few+solutions+pop+up+at+FTC+adware+workshop/2100-1028_3-5195222.html.

99. http://www.earthlink.net/spyaudit/press/.

100. Symantec, "Internet Security Threat Report Highlights Rise In Threats To Confidential Information", Media Release, 21 March 2005. http://www.symantec.com/press/2005/n050321.html.

101. Matthew Fordahl, "Microsoft to make antispyware software free", *Associated Press*, 15 February, 2005.

102. Andrew Birmingham, "The spy in your machine", 7 September 2004. http://australianit.news.com.au/articles/0,7204,10665570%5E15382%5E%5Enbv%5E,00.html refer also to the FDIC report, Op.cit.

103. Dell, "Dell Launches Campaign to Build Awareness of PC Security Issues", Press Release, Round Rock, Texas, 20 July 2004 http://www1.us.dell.com/content/topics/global.aspx/corp/pressoffice/en/2004/2004_07_20_rr_000?c=us&l=en&s=gen&cs=#tn1.

104. FTC, Staff report of Spyware Workshop, Op.cit.

105. Matt Hines, "Microsoft launches anti-spyware beta", CNET, 6 January 2005. http://news.com.com/Microsoft+launches+anti-spyware+beta/2100-1029_3-5514899.html.

106. BBC, "UK police foil massive bank theft", 17 March 2005. http://news.bbc.co.uk/2/hi/uk_news/4356661.stm.

107. ISC, Handlers Diary, 27 February 2005. http://isc.sans.org/index.php?off=worldmap.

108. Gregg Keizer, "CoolWebSearch tops spyware threat list", *Techweb*, 31 March 2005. http://www.itnews.com.au/newsstory.aspx?CIaNCID=35&CIaNID=18386.

109. Marco Cremonini and Patrizia Martini, Evaluating Information Security Investments from the Attacker's Perspective", presented at the Fourth Workshop on the Economics of Information Security, Kennedy School of Government, Harvard University, 2-3 June 2005. http://infosecon.net/workshop/pdf/23.pdf and at the same conference: Paul Judge, Dmitri Alperovitch and Weilai Yang, "Understanding and Reversing the Profit Model of Spam", http://infosecon.net/workshop/pdf/49.pdf.

110. The map can be found at: http://us.mcafee.com/virusInfo/default.asp?cid=10371.

111. http://securityresponse.symantec.com/avcenter/vinfodb.html.

112. John Leyden, "Internet neighbourhood watch set up", 7 December 2000. http://www.theregister.co.uk/2000/12/07/internet_neighbourhood_watch_set_up/.

113. http://www.dshield.org/.

114. http://isc.sans.org/.

115. http://isc.sans.org/survivalhistory.php.

116. http://www.nist.gov/public_affairs/general2.htm.

117. http://icat.nist.gov/icat.cfm?function=statistics.

118. https://cassandra.cerias.purdue.edu/main/index.html.

119. http://www.us-cert.gov/aboutus.html.

120. http://www.auscert.org.au/render.html?it=4125, http://www.cancert.ca/Home/Default.php, http://www.certcc.or.kr/, http://www.cert-ist.com, http://www.jpcert.or.jp/english/, http://www.apcert.org/ and http://www.first.org/about/organization/teams/.

121. http://www.us-cert.gov/federal/statistics/.

122. http://www.jpcert.or.jp/isdas/readme-en.html#graph.

123. Refer for example to: http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.14.pdf.

124. "IBM report: Surge in viruses and worms targeting mobile devices, satellite communications anticipated in 2005", 9 February 2005, http://www-1.ibm.com/services/us/index.wss/rs/imc/a1008866.

125. http://www.f-secure.com/v-descs/cabir.shtml.

126. http://www.f-secure.com/weblog/.

127. John Markoff and Laura M Holsen, "At the Oscars, stars'phones were open book", *The New York Times* (reprinted in the International Herald Tribune 3 March 2005).

128. http://www.f-secure.com/v-descs/commwarrior.shtml.

129. http://www.caida.org

130. Bradley Huffaker, "Overview of CAIDA Data Collection, Analysis and Visualization", 9 June 2005. http://www.caida.org/outreach/presentations/2005/iij/

131. Michael Delio, "Find the Cost of (Virus) Freedom", *Wired*, 14 January 2002. http://www.wired.com/news/infostructure/0,1377,49681,00.html.

132. The SANS Institute, "The Top 20 Internet Security Vulnerabilities and How to Eliminate Them", 2003, http://www.sans.org/top20/cdipresentation.pdf.

133. Reuters, "Virus damage estimated at $55 billion in 2003", 16 January 2004, http://msnbc.msn.com/id/3979687/.

134. Prevx, "Prevx names top ten Internet attacks of the year", 28 December 2004. http://www.prevx.com/newspress.asp.

135. The Honeynet Project & Research Alliance, "Know your Enemy:Tracking Botnets", 13 March 2005 http://project.honeynet.org/papers/bots/.

136. Micah Hoffman, "BOTS – The creation of a Botnet Tracking Web Application", DNS-OARC Workshop, Santa Clara, 25-26 July 2005. http://public.oarci.net/oarc/workshop-2005/minutes/hoffman-BOTS

137. http://www.ciphertrust.com/resources/statistics/zombie.php

138. Symantec, "Symantec Internet Security Threat Report Identifies More Attacks Now Targeting e-Commerce, Web Applications", 20 September 2004. http://www.symantec.com/press/2004/n040920b.html.

139. "IRC Botnet Found and Shutdown", 10 September 2004. http://isc.sans.org/diary.php?date=2004-09-07.

140. "Botnets: hidden menace makes PCs an instrument of extortion", 16 December 2004. http://www.nzherald.co.nz/index.cfm?c_id=688&ObjectID=9003405.

141. Symantec, "Internet Security Threat Report", Trends for July 04 – December 04", Volume VII, March 2005.

142. Netcraft, "E-commerce Firm 2Checkout Reports DDoS Extortion Attack", 17 April 2004, http://news.netcraft.com/archives/2004/04/17/ecommerce_firm_2checkout_reports_ddos_extortion_attack.html.

143. "Hackers Almost Break Bookmaker", *Kommersant Daily*, 4 April 2005 http://www.kommersant.com/page.asp?id=560203 and Bill Goodwin, "Crime gangs unite to launch online attacks", 5 April 2005. http://www.computerweekly.com/articles/article.asp?liArticleID=137723&liArticleTypeID=1&liCategoryID=6&liChannelID=13&liFlavourID=1&sSearch=&nPage=1.

144. Avi Goldfarb, "Why do denial of service attacks reduce future visits?: Switching costs versus changing preferences", paper dated February 2005 for Fourth Workshop on the Economics of Information Security, Kennedy School of Government, Harvard University, 2-3 June 2005 http://infosecon.net/workshop/pdf/6.pdf.

145. Netcraft, "Akamai Attack Highlights Threat From Bot Networks", 16 June 2004, http://news.netcraft.com/archives/2004/06/16/akamai_attack_highlights_threat_from_bot_networks.html and "DDoS Attack on DoubleClick Slows Many Sites", 28 July 2004, http://news.netcraft.com/archives/2004/07/28/ddos_attack_on_doubleclick_slows_many_sites.html.

146. http://www.fbi.gov/mostwant/fugitive/jan2005/janechouafni.htm and Netcraft, "Botnet with 10,000 Machines Shut Down", 8 September 2004. http://news.netcraft.com/archives/2004/09/08/botnet_with_10000_machines_shut_down.html.

147. Elizabeth Biddlecombe, "Criminal use of spam increasing – experts", Total Telecom, 31 January 2005, http://www.totaltele.com/view.asp?ArticleID=115625&pub=tt&categoryid=0.

148. John Leyden, "Botnets strangle Google Adwords", *The Register*, 3 February 2005. campaignshttp://www.theregister.co.uk/2005/02/03/google_adwords_attack/.

149. Dan Ilet, "Organised crime's grip on the Net 'is tightening'", 9 December 2004, http://news.zdnet.co.uk/0,39020330,39180206,00.htm and Netcraft "Fraud Hosting Services widely promoted", 1 March 2004, http://news.netcraft.com/archives/2004/03/01/fraud_hosting_services_widely_promoted.html.

150. Ilet, “Organised crime's grip on the Net 'is tightening'”, op.cit.

151. Elizabeth Biddlecombe, “Criminal use of spam increasing – experts”, Op.cit; Reuters, “Scotland Yard and the case of the rent-a-zombies”, 7 July 2004, http://news.zdnet.com/2100-1009_22-5260154.html; James Robertson, “Zombies join the attack”, 8 January 2005, http://www.smh.com.au/news/Icon/Zombies-join-the-attack/2005/01/04/1104601351920.html.

152. Bill Goodwin, “Crime gangs unite to launch online attacks”, 5 April 2005. http://www.computerweekly.com/articles/article.asp?liArticleID=137723&liArticleTypeID=1&liCategoryID=6&liChannelID=13&liFlavourID=1&sSearch=&nPage=1.

153. Netcraft, “Euro 2004 Gambling Sites Hit By Denial Of Service Attacks”, 10 June 2004. http://news.netcraft.com/archives/2004/06/10/euro_2004_gambling_sites_hit_by_denial_of_service_attacks.html and “Botnets: hidden menace makes PCs an instrument of extortion”, 16 December 2004. http://www.nzherald.co.nz/index.cfm?c_id=688&ObjectID=9003405.

154. Telus, “Modem Hijacking”, http://about.telus.com/publicpolicy/scams_modemhijacking.html.

155. McAfee, “Virus Watch”, *eSeurity news*, Summary 2004. http://dispatch.mcafee.com/us/esecuritynews/summer2004/viruswatch.asp?cid=10984.

156. McAfee, “Virus Watch”, *eSeurity news*, Summary 2004. http://dispatch.mcafee.com/us/esecuritynews/summer2004/viruswatch.asp?cid=10984. Refer also to McAfee testimony at http://www.ftc.gov/bcp/workshops/spyware/transcript.pdf, p 74.

157. Robin Langford, “BT blocks 1000 rogue diallers”, 5 October 2004. http://www.netimperative.com/2004/10/5/BT_blocks_diallers.

158. The eFinland Weblog, “The Consumer Should Not Have to Pay for Modem Hijacking – That an Internet-Based Test Is Charged for Has Come as a Surprise to Many”, 2 August 2004. http://e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=26518.

159. http://isc.sans.org/diary.php?date=2005-02-19.

160. http://www.phonebusters.com/english/statistics.html.

161. http://www.content.overture.com/d/USm/ac/index.jhtml.

162. http://isp.webopedia.com/TERM/C/click_fraud.html.

163. Zoltan Gyongyi and Hector Garcia-Molina, “Link Spam Alliances”, Stanford University, 2 March 2005. http://blog.searchenginewatch.com/blog/pdf/linkalliance.pdf

164. Rob McGann , “Impression Spam Worries Google Advertisers”, *ClickZ News*, 24 february 2005. http://www.clickz.com/news/article.php/3485386.

165. For example, Associated press, “Click Fraud Threat Looms”, 15 February 2005 http://edition.cnn.com/2005/TECH/internet/02/15/click.fraud.ap/ and Brad Stone, “When Mice Attack”, *Newsweek*, 24 January 2005 http://msnbc.msn.com/id/6830802/site/newsweek/.

166. Brad Stone, Op.cit.

167. For a discussion see: http://news.netcraft.com/archives/2005/02/02/google_domain_strategy_could_impact_domain_resale_values.html and http://news.netcraft.com/archives/2005/02/22/searchoptimized_domain_portfolio_sells_for_164_million.html.

168. "Report Details New Threats to Data Security", 8 March 2005, http://www.govtech.net/magazine/channel_story.php?channel=4&id=93314.

169. http://www.iab.net/standards/measurement.asp.

170. Brad Stone, Op.cit.

171. SEMPO, "The State of Search Engine Marketing – 2004", January 2005. http://www.sempo.org/research/sem-trends-2004.php and "Click Fraud, an Industry Crisis, or Blip on the Search Engine Marketing Landscape?", 23 February 2005. http://www.sempo.org/press/click-fraud.php.

172. http://www.pewinternet.org/PPF/p/1052/pipcomments.asp.

173. The results come from a monthly tracking survey by the Pew Internet & American Life Project. In all, 2 201 adults 18 and over took part in the telephone survey.

174. http://www.mobilespam.org/.

175. Netscape provides an introduction to SSL at: http://developer.netscape.com/docs/manuals/security/sslin/contents.htm and http://wp.netscape.com/security/techbriefs/ssl.html.

176. http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm.

177. http://www.lastminute.com/lmn/banner/security/securityg.htm.

178. http://www.lastminute.com/lmn/banner/security/securityg.htm.

179. David Johnson, "A Modest Approach to SSL Certificate Costs", http://www.workz.com/cgi-bin/gt/tpl_page.html,template=1&content=2133&nav1=1&.

180. Netcraft, "Do SSL Certificate Authorities still have a margin generating business model?", 9 September 2003 http://news.netcraft.com/archives/2003/09/09/do_ssl_certificate_authorities_still_have_a_margin_generating_business_model.html.

181. "Go Daddy Launches Low-Priced, 128-Bit Turbo SSL Certificates With Issuance in Minutes", Press Release, 15 September 2004 http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=109&STORY=/www/story/09-15-2004/0002250580&EDATE=.

182. http://www.ev1servers.net/english/starterssldetails.asp.

183. Netcraft, Secure Server Report, April 2005.

184. Ibid.

185. ACCESS Co., Ltd, "ACCESS NetFront Browser Powers First 3G Smart-Card Handset From NTT DoCoMo", Press Release, 1 September 2004. http://www.symbianone.com/index.php?option=content&task=view&id=748.

186. GeoTrust, "GeoTrust Announces Power Server ID™ SSL Certificate with Expanded Support for Mobile Computing", Press release, 20 July 2004, http://www.geotrust.com/news_events/press/pr_power_server_id_071904.htm.

187. http://www.secgo.com/ebanking/english/.

188. http://epp.eurostat.cec.eu.int/portal/page?_pageid=1996,45323734&_dad=portal&_schema=PORTAL&screen=welcomeref&open=/&product=EU_MAIN_TREE&depth=1.

189. http://www.abs.gov.au/Ausstats/abs@.nsf/Lookup/D4F295CE33FAC665CA256E59007AC471 and http://www.abs.gov.au/Ausstats/abs@.nsf/Lookup/45C825409149033FCA256889000B8132.

190. http://www.johotsusintokei.soumu.go.jp/tsusin_riyou/data/eng_tsusin_riyou02_2003.pdf.

191. http://www.johotsusintokei.soumu.go.jp/tsusin_riyou/data/eng_tsusin_riyou01_2003.pdf.

192. http://www.ntia.doc.gov/ntiahome/dn/html/anationonline2.htm.