Public-Private Partnerships against cybercrime

Jean-Christophe Le Toquin
Director Internet Safety
Microsoft EMEA
Evidence needed by police to solve a cybercrime is often held by private industry outside of police’s jurisdiction.

Partnerships are essential to making cross-jurisdiction, cross-culture cooperation work.

In cybercrime investigations, less restrictions may apply to cross-border cooperation for industry than to national law enforcement.

Private industry are often one of the main victims of cybercrime and for this reason are interested in cooperating with law enforcement.
Examples of informal cooperation

- Cooperation between American, Moroccan, Turkish police, and Microsoft lead to the arrests of the writers and distributors of the Zotob Virus.

- Evidence obtained by Microsoft in its civil suite was used by US prosecution in the criminal procedure against the “Spam King” Robert Soloway.

- A criminal referral by Microsoft lead to the arrest of 8 Bulgarian members of the MBAM Phishing gang for the phishing of a Microsoft billing website.
Formalizing the cooperation

- **NCFTA** is an alliance between the FBI, US Postal Inspection Service and private industry.
- **Digital PhishNet**: public-private cooperation to drive enforcement against phishing websites hosted by NCFTA.
- **Signal-Spam** was initiated as a public-private organization to identify spammers for enforcement cases.
- **London Action Plan**, a cooperation between industry and Telecom and Consumer Public Authorities to fight spam.
- **European Financial Coalition** is a cooperation between law enforcement and IT and financial industry to fight child exploitation.
**Signalez vos spams d'un simple clic**

Grâce à Signal Spam, il vous suffit d'un simple clic pour signaler les spams que vous recevez, et obtenir un suivi sur votre action.

Pour commencer dès maintenant, inscrivez-vous et téléchargez le plug-in.

**S'INSCRIRE**

---

**Plate-forme nationale de signalement des spams**

Le projet de plate-forme nationale de signalement des spams est porté par une association de loi 1901.

Elle regroupe l'ensemble des acteurs de la lutte contre le spam, qu'il s'agisse d'autorités publiques, d'organisations professionnelles ou d'entreprises privées.

**EN SAVOIR PLUS**

---

**Dernières actualités**

- Nouvelle version du site internet Signal Spam
- Microsoft et Signal Spam approfondissent leur collaboration contre le spam
- Signal Spam et la CNI, partenaires dans la lutte contre le spam

**Plus d'actualités**

---

**Recommandations**

- Vous êtes un particulier
- Vous êtes un professionnel
Challenges to cooperation

- Jurisdictional variations on data retention and sharing of evidence
- Lack of communication between law enforcement and service providers with regard to how to share and obtain needed evidence most efficiently
- Tension between privacy and needs of data retention for enforcement purposes
Improving cooperation

- Improving Public-Private Partnerships is essential to reducing the risks for Internet users.
- Harmonized legislation such as the Cybercrime convention has proven very helpful.
- The Council of Europe guidelines on law enforcement & service provider cooperation is an essential framework for dialogue.
- Joint cyber forensics training through 2CENTRE will help foster ideas on cooperation.
Cooperation against cybercrime

Contact List
(2010?)

Training
2CENTRE (2009)

Guidelines for Internet Service Providers and Law Enforcement cooperation (2008)

Convention on Cybercrime (2001)
Advance Fee Fraud Coalition

What is Advance Fee Fraud

Advance Fee Fraud is a rising type of Internet crime causing Internet users to lose significant amounts of money. The expression ‘Advance Fee Fraud’ (AFF) describes fraud cases in which criminal fraudsters convince a victim that the victim has won a prize or been selected for a business deal with easy money to be gained and the only condition to obtain the gain is that the victim has to pay a small amount of money in advance. When the victim pays the fee, it will not bring him closer to receiving the gain. In fact, he only risks losing more money as the fraudster will be encouraged to recontact the victim to request the payment of additional fees for the same transaction. The explanations used by the fraudsters for demanding the additional fees are creative but still credible and may include the advance payment of bank fees for money transfers, payment of courier services to send the check, legal fees to have an attorney or notary prepare documents needed for the money transfer, or the advance payment of taxes on the prize.

To make their deception more convincing, the fraudsters are known to create fake courier companies, public notary firms, law firms, and provide them with domain names, phone numbers, email addresses to complete the deception. They will counterfeit trusted brands to convince the victim that the prize is plausible and real.

Enforcement against AFF is complicated by the fact that fraudsters commit their crime across borders and although the aggregated cases add up to very large crimes, the individual cases may not be large enough to meet the threshold for initiating an international investigation and subpoenaing evidence to identify the fraudsters.

The Advance Fee Fraud Coalition

The Advance Fee Fraud (AFF) Coalition was announced on October 28, 2008 by its founding members, Microsoft Corp, Yahoo! Inc, The Western Union Company and the
Industry working with Public Authorities

The Advance Fee Fraud Coalition is an initiative of companies to fight Internet fraud through:

- Public awareness
- Mitigation
- Enforcement

This industry initiative demonstrates an interest and need by the private sector to also work on what is primarily a consumer protection issue.
Industry’s cooperation with law enforcement has evolved and matured in stages:

1. Informal cooperation on specific cases and communications
2. Creating common entities and Public-Private Partnerships to engage in joint actions
3. Cooperation formalized through legal instruments and guidelines

Is there a need for closer cooperation between private industry and consumer protection authorities to fight online crime?