Europol's new iOCTA* report examines how EU citizens are risking their personal identities, privacy and computer data through the use of social media tools which are increasingly a target for cybercriminal activity.

In recent years the transition of the world wide web from a collection of websites to a platform for linked services such as social networking sites and real–time communication tools (‘Web 2.0’), has provided the technical means for the expansion of social engineering.

Users of social networking sites, such as FaceBook, can easily place content from photo or video sharing sites on their profiles pages and install small applications, tools and games which they use to interact with friends. However, cybercriminals exploit the trust of users – who consider themselves to be in a ‘safe’ network of people they know – by injecting malicious software into posted items and sharing links to websites that are bogus and designed to extract personal information.

The majority of organisations have come to accept the use of social networking sites in the workplace. But under the right circumstances, access to social media at work has the potential to infect corporate networks with spyware and other means to harvest large amounts of personal, corporate and financial data for profit. 33% of small and medium businesses in the US say that they have been infected with malicious software distributed through social networking sites. 35% of those infected suffered financial loss, and more than a third of these lost more than $5000 as a result of the infection (source: PandaLabs). Organisations can reduce these risks by drawing up social media guidelines for employees to follow.

Social engineering – the act of manipulating people into performing actions or divulging confidential information – is a key feature of hacker culture and cybercriminal methods. Criminals involved in phishing, for example, aim to persuade email recipients that they represent organisations which require verification of customers’ personal data, while spoof websites are fake versions of legitimate online services designed to dupe customers into revealing their account details. Internet users can even be manipulated into paying for anti–virus software which is useless, or worst case scenario, contains crimeware and security risks.
‘Advanced fee fraud’ is another example of social engineering that has undergone wholesale transformation in the internet age, due to the low cost and ease of contacting people. Advanced fee fraudsters entice victims with the promise of reward and, through this crime, internet users continue to pay ‘release fees’ for non-existent legacies and lottery winnings. The effects of the ongoing economic crisis may well make people more susceptible to scams. Raising awareness amongst internet users is therefore crucial to successfully preventing and combating cybercrime.

Online location–based services have also developed which allow users to locate their friends more easily offline, and to add information to their social networking profiles (‘geotagging’), informing where the user has been but, more crucially, their current location. Statistics show that 69% of teenagers have included their physical location in updates on social networking sites (source: McAfee). Concerns are being expressed over the willingness of internet users to divulge their offline locations, as there is an obvious security risk run by those who clearly state that they have left their personal property unattended.

Europol’s iOCTA: Selected findings and recommended actions

- EU Member States already rank amongst the most highly infected countries in the world when it comes to computer viruses and malware. As internet connectivity continues to spread, EU citizens and organisations will be subjected to more cyber attacks, and to attacks from previously underconnected areas of the world. Combating cybercrime will therefore require new international strategic and operational partnerships.

- **Active partnership with the private sector** is essential, not only to share intelligence and evidence, but also in the development of technical tools and measures for law enforcement to prevent online criminality. The academic community also has an important part to play in the research and development of such measures.

- Because of the global reach and scale of internet facilitated organised crime, its disparate nature, and the unprecedented volumes of data involved, **centralised coordination of intelligence** gathering, analysis, training, and partnership management is required at an EU level, to ensure that Member States and EU agencies make the most effective use of resources. The establishment of a **European Cybercrime Centre**, as outlined in the recent Council conclusions on cybercrime and in the EU’s Internal Security Strategy, will be an important and timely step forward.

- Awareness raising on individual and corporate user responsibility are key to combating cybercrime. **EU–wide awareness raising and points of contact** are required for a range of issues, including illegal downloading, social engineering, payment card security, securing wireless internet connections, and the risks to children. The use of crowdsourcing to gather intelligence on cybercrime from internet users should also be considered.

Europol’s role in the fight against cybercrime
Europol is the European Union law enforcement agency. It plays a key role in the **European Cybercrime Task Force** – an expert group made up of representatives from Europol, Eurojust and the European Commission, working together with the Heads of EU Cybercrime Units to facilitate the crossborder fight against cybercrime.

By means of its **cybercrime database**, Europol provides EU Member States with investigative and analytical support on cybercrime, and facilitates crossborder cooperation and information exchange.

**Strategic analysis of Internet Facilitated Organised Crime** (iOCTA) assesses current and future trends in cybercrime, and informs both operational activity and EU policy.

The **Internet Crime Reporting Online System (ICROS)** and **Internet & Forensic Expert Forum (IFOREX)** are currently in development. These will provide centralised coordination of reports of cybercrime from EU Member State authorities, and host technical data and training for law enforcement.

*The full iOCTA will be made available on Friday, 7 January 2011 via Europol’s website.*

### CRIME AREAS
- Cybercrime

### TARGET GROUPS
- General Public
- Law Enforcement
- Academia
- Professor
- Students
- Researcher
- Other

### ENTITIES
- European Cybercrime Center (EC3)

**Source URL:** https://www.europol.europa.eu/newsroom/news/hidden-risks-of-social-media