International Working Group
on Data Protection
in Telecommunications

675.29.6

19 November 2004

Working Paper
on
Means and Procedures to Combat Cyber-Fraud in a Privacy-Friendly Way

- adopted at the 36th meeting on 18-19 November 2004 in Berlin -

Just like in the offline world, the bulk of online crime is crime against property. The most common forms appear to be fraud and copyright piracy.

The Internet Fraud Complaint Center (IFCC) lists internet fraud as a growing problem in its 2002 report[1]. Auction fraud was the most reported offence.

The OECD Council adopted the "OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders"on 11 June 2003[2].

Many remedies have been suggested to combat cyber-fraud. Most of these involve improved forms of prosecution and better cooperation between governments. Whilst these remedies are no doubt useful, they may also involve data collection and data transfers that raise privacy concerns.

It appears that remedies which emphasize prevention have so far received considerably less attention. The International Working Group on Data Protection in Telecommunications stresses the positive effects that preventive techniques may have on the reduction of the crime rate in general and the safeguarding of privacy aspects concerned with prosecution. The International Working Group on Data Protection in Telecommunications has addressed this subject before[3].

The following methods and techniques may be used to combat cyber-fraud in a privacy-friendly way:

- **Digital signatures** can help to identify business partners;
- **Escrow systems** can make the exchange of goods and money safer for both parties through the use of a trustworthy third party;
- **Audits and quality** seals can help customers to recognize trustworthy online stores;
- **Improved payment** systems are less vulnerable to fraud;

[1] www.ic3.gov/media/annualreport/2002_IFCCReport.pdf
[2] http://www.oecd.org/dataoecd/24/33/2956464.pdf
[3] Common Position on the detection of fraud in telecommunications adopted at the 27th Meeting of the Working Group on 4-5 May 2000 in Rethymnon / Crete, available online http://www.datenschutz-berlin.de/attachments/232/fr_en.pdf

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.datenschutz-berlin.de

The Working Group has been initiated
by Data Protection Commissioners
from different countries in order
to improve privacy and data protection
in telecommunications and media

- **Better Informed customers** are less likely to become victims of fraud;
- **Better informed businesses** are more likely to employ systems that are better protected against fraud;
- **Enhanced security** can reduce many forms of fraud that target computer systems or exploit their weaknesses to deceive humans.

The explanatory paper to this document contains examples.

Conclusions

The International Working Group on Data Protection in Telecommunications recommends that authorities should

- Promote privacy-friendly means to prevent cyber-fraud before looking at other measures to combat cyber-fraud
- Collect information and examples on privacy-friendly means of combating cyber-fraud; and
- Exchange such information;
- Promote the adoption of privacy-friendly codes of practice by the business community, especially intermediaries
- Inform the public and the business community.

Explanatory Paper

(To the paper ”Means and Procedures to Combat Cyber-Fraud in a Privacy-Friendly Way”)

This explanatory paper lists some of the techniques that can be used to combat cyber-fraud in without infringing civil rights in more detail. Throughout this paper, examples for existing services and products have been provided. These are not to be understood as an endorsement by the International Working Group on Data Protection in Telecommunications. They merely serve as a guideline for what is already available. All information and hyperlinks were last checked in November 2004.

Digital Signatures

Digital signatures can help identify business partners. A digital signature is one of the few ways one can be certain of the business partner’s identity.

Digital signatures are not available everywhere and not perfect. There will always be means to obtain genuine but misleading certificates[4], or to trick people into doing business without a signature, but it does help.

Companies may issue sales certificates that are signed, thereby giving the buyer proof of the sale as well.

Escrow Systems

Systems where the money is not immediately paid to the seller, but kept by a trustworthy third party (“escrow service”) may prevent delivery fraud where a dishonest seller demands advance payment and never delivers. This kind of fraud is especially common in online auctions. The IFCC 2002 Internet Fraud Report lists the case of “United States v. Teresa Smith”, in which Mrs. Smith sold computers on internet auction sites but did not deliver. She defrauded more than 300 victims for over $800.000.

With an escrow system, the buyer gives the money to the escrow service. The seller receives information from the escrow service that the money is ready for him and cannot be withdrawn, while the buyer releases the money only when he receives the goods. In case of dispute, the money remains blocked until a proper decision can be reached. A properly used escrow service can make delivery fraud very impractical. The swindler must deceive the buyer or the escrow service into releasing the money (e.g. by delivering goods that appear legitimate, but are of lower quality, or faking a release order). However, all of these countermeasures appear risky and expensive for the swindler.

The drawback of escrow services is that they must be available and accepted by both parties, and that they cost money. Persons involved in deals with legitimate but embarrassing goods (e.g. pornography) may refuse to use an escrow service for privacy reasons. Highly professional swindlers can offer their own fraudulent escrow service. Other criminals may talk gullible people into not using an escrow service.

As an additional privacy benefit, the seller receives information from the escrow service that the promised money is available. The seller does not need to check the buyers creditworthiness. He merely has to trust the escrow service.

Ebay, a popular online auction house, recommends escrow services:
http://pages.ebay.com/help/community/escrow.html

[4] E.g. it is possible to pay an accomplice with no criminal records to “lend” his signature for the purpose of fraud.

Sellers should be encouraged to cooperate with good escrow services and recommend them to their customers.

Audits and Quality Seals

How can one know that a seller is trustworthy? To address this question, various programs for audits and quality controls have sprung up.

These programs may not be perfect, but they do make a difference between a web shop customers know nothing about and one that has been examined by a trusted organisation.

Improved Payment Systems

Much of the potential for abuse and fraud lies in technical and organisational weaknesses of payment systems. Credit cards, in particular, have proven to be too easy to abuse. Many forms of fraud involve credit card payments.

The authorities should examine what can be done to improve payment systems so that swindlers have less opportunity to exploit weaknesses.

Customer Information

The best weapon against fraud is information. Many countries already have good consumer information services in place, others should follow suit. In some counties, the police agencies offer information as well.

There is enough information available (though often in English). Creating and spreading such information in a language and form appropriate for the citizens can help a lot.

Information for Businesses

The adoption by business of more secure systems that are less susceptible to compromise should reduce the incidence of fraud.

Enhanced Security

Frauds that attack computer systems frequently profit from inadequate security measures and insecure software.

Fraud targeting computer systems is a completely new form of crime. In computer fraud, the main target of the swindler is the computer system of the victim. The criminal aims to obtain funds, access rights or resources that are either unavailable to him or would cost him money by manipulating a computer. Some swindlers copy personal data to deceive credit card companies or banks[5]. This kind of fraud may involve the user, but only to a limited degree, such as tricking somebody into downloading a program that permits an attacker access to his computer (a “Trojan Horse”).

Other criminals forge e-mails from banks to make the recipients enter confidential access information for their bank accounts (this is called “phishing”). Phishers abuse security leaks in web browsers and e-mail software to aid in the deception, e.g. to create the impression that somebody is visiting the web site of his bank while he is actually on a fake page with a different address.

A type of attack that has become common is computer hijacking to send out spam. This is not “fraud” in the classic sense, but it still involves deception to commit illegal actions. Moreover, many spammers sell fraudulent products or services. Less spam means less fraud.

[5] This is often called “identity theft”.

The best way to combat such crimes is to improve computer security. The authorities can propose better security measures, quicker responses to leaks and threats as well as legal remedies against damage by insecure systems. It is possible to encourage the use of more secure technology by citizens.

Suppliers can help by promoting the advantages of more secure hardware and software solutions, especially the use of firewalls in conjunction with broadband connections. These can reduce the opportunities for attack by blocking unrecognised inward connection attempts.

Sometimes, even simple things like a good e-mail-program and a well-made web browser can help.