TACD

TRANS ATLANTIC CONSUMER DIALOGUE | DIALOGUE TRANSATLANTIQUE DES CONSOMMATEURS

DOC NO. INFOSOC-33-07 DATE ISSUED: FEBRUARY 2007

RESOLUTION ON IDENTITY THEFT, PHISHING AND CONSUMER CONFIDENCE

The Issue

The Transatlantic Consumer Dialogue (TACD) is concerned about the growing number of identity theft (ID theft) and phishing attacks via the Internet. These attacks pose a significant threat to consumers on both sides of the Atlantic and worldwide. Consumer confidence in e-commerce is at stake, as trust in doing business online is eroded due to the increasing risk of such attacks.

ID theft - acquiring the means of identifying of an individual in order to commit fraudulent activity - is a large and serious problem. Whereas there are concrete data on the extent of the problem in the U.S., targeted research and statistics are harder to find in the EU. The U.S. Federal Trade Commission (FTC) reports that it received 255,565 ID theft complaints from U.S. consumers in 2005[1], up from 246,847 in 2004 and 215,177 in 2003. These figures do not tell the full story, since many consumers do not realize they have been victimized or do not report it. A survey released in January 2006 by Javelin Strategy & Research indicates that from the fourth quarter of 2004 to the fourth quarter of 2005, 4% of U.S. adults were victims of ID fraud (defined as the fraudulent *use* of their personal information, representing 8.9 million people and amounting to more than $56 billion[2].

As shown in the FTC report, the objective of ID thieves is to obtain consumers' financial account numbers and other identifying information in order to take over their existing accounts, open new accounts, and impersonate them for other illegal purposes, usually for financial gain. There are many ways that ID theft can occur, from stealing people's mail to more high-tech approaches. With the advent of e-commerce and online banking, the Internet is becoming an attractive venue for ID thieves.

There are different types of attacks used to obtain and abuse confidential information or consumers' personal data via the Internet. The main types are described in the annex to this resolution.

Risks for Consumers and E-commerce

As the number of consumers using online services is growing rapidly (in Germany, for instance, the proportion of bank customers using online banking is close to 40%) the risks of criminal attacks via the Internet are growing as well. Phishing and other forms of identity theft result not only in financial losses for consumers and businesses but in a loss of confidence in the Internet as a means of communication and commerce. A Consumer Reports WebWatch survey conducted in 2005 found that 9 out of 10 U.S. adults who used the Internet had

[1] www.ftc.gov/opa/2006/01/topten.htm
[2] www.javelinstrategy.com/reports

changed their online behavior because of fear of identity theft; 30% of those had reduced their overall use of the Internet, and 25% said they had stopped shopping online entirely[3].

Recent reports show that victims of identity theft can suffer from stress and health problems while fighting to rehabilitate their identities. The FTC estimated that 36% of victims will face further inconvenience and damage from being rejected in applications for loans, insurance policies or credit. An average of 14% of the victims will even face criminal prosecution[4].

Fighting ID Theft

Private companies and public authorities in Europe and the U.S. are making efforts to inform consumers and better protect the general public against the risks of identity theft and phishing. However, these efforts are not sufficient, especially when it comes to more sophisticated or high-tech forms of attack. No firewall or antivirus software has been shown to guarantee full protection against all of these attacks although they will detect most of them. Furthermore, the burden often rests on the consumer to install and update them. Phishing filters and other technology that can prevent consumers from accessing fraudulent emails and websites are encouraging developments but need to be deployed ubiquitously.

Security on the user's side should be a default setting, not an optional extra. For example, computers should be shipped to consumers with effective anti-spyware and virus protection automatically included and in the "on" mode. Browsers should be updated automatically and include consumer-friendly features such as moving the padlock icon to the browser field and color-coding URLs to indicate the level of their security. Security should be designed to keep consumers within the "walled city" and prevent them from being vulnerable to attack.

In terms of legal measures against ID theft, consumer protection and monitoring systems are more advanced in the U.S. than in the EU. Whereas in the U.S. firms have taken additional actions to make their services more secure, either on their own initiative or prompted by government, it appears that in the EU most countries do not even have specific offences covering identity fraud[5].

The European Commission has created a Fraud Prevention Expert Group to foster cooperation of different parties involved in fraud prevention, i.e. national and EU payment schemes, banks, national public authorities, European and international law enforcement agencies (e.g. Europol, Interpol), retailers, consumer groups, network operators. This group will also function as an advisory board for further action by the European Commission[6].

In the U.S. the President has established a federal inter-agency ID Theft Task Force[7]. Since ID theft and phishing are global in nature, with criminals victimizing consumers in multiple countries and using money-laundering schemes to attempt to make tracing them more difficult, organizations such as the APWG and arrangements between governments to share information and provide mutual enforcement assistance are essential to effectively combat them. The U.S. Federal Financial Institutions Council has issued guidelines for financial

[3] www.consumerwebwatch.org/dynamic/web-credibility-reports-princeton.cfm

[4] See references in Amanda Welsh: The Identity Theft Protection Guide, New York 2004, p. 15: "The U.S. Public Interest Research Group reports that it takes an average of two to four years to explain away the thief's bad debts. The FTC estimates that 36 % of victims also experienced problems like being denied credit, a loan or insurance as a direct result of the theft. Of the people unlucky enough to have an identity thief actually impersonate them - instead of just using their credit card account for an unauthorized shopping spree - 14 % were investigated by the police or thrown in jail."

[5] It has yet to be acknowledged that criminal law within EU Member States will tackle most of the offences causing damages to consumers (e.g. fraud and computer sabotage delicts). The European Commission has initiated efforts to prevent leaks due to the different kinds of criminal law within European Union. Preparatory activity to commit these crimes, i.e. by collecting this data, is yet not fully covered although recently criminal law in Germany, for example, is being updated to reflect the new dangers.

[6] http://ec.europa.eu/internal_market/fpeg/index_en.htm

[7] www.whitehouse.gov/news/releases/2006/05/20060510-3.html

institutions to improve authentication procedures when consumers access their accounts[8]. A private-sector coalition, the IP Governance Task Force[9], has been created to encourage trademark owners to employ technical and legal measures to prevent their brands from being abused by phishers and spoofers. The National Consumers League in the U.S. hosted an experts retreat on phishing in the fall of 2005 and has formed working groups to further explore the recommendations that resulted from that exercise[10].

TACD welcomes all these initiatives and believes that it is important that consumers are represented in the relevant committees and forums. But more needs to be done to protect consumers and the integrity of the electronic marketplace. In Germany, for example, the majority of banks still rely on password systems (e.g. PIN/TAN) that are easy to abuse, leaving consumers vulnerable to all kinds of attacks. There is no legal impetus to force industry to achieve a higher standard of safety.

Recommendations

TACD resolves that the EU and U.S. governments should:

1. Enact laws to explicitly prohibit using malware and spyware as well as remote manipulation of external computers or servers for the purpose of ID theft. New laws on ID theft and phishing should be more specific and provide rigorous punishment.

2. Enact or - where applicable - update national laws to deal with ID theft holistically. This should include:

   - legal sanctions (including criminal legal sanctions) against intrusion in private computers or external computer systems
   - general duties on companies to adopt adequate security policies and procedures and to inform customers when their data has been compromised (for example, as required by the California law on security breaches[11])
   - provisions to enable individuals to place “freezes” on their credit reports to strictly control access to their sensitive personal information and thereby reduce the risk of identity theft[12]
   - requirements for businesses to provide assistance when customers’ data has been compromised as a result of security breaches.

3. Promote research and provide incentives for the development of best practices to combat phishing, ID theft and other types of high-tech fraud via the Internet.

4. Better coordinate anti-fraud prevention initiatives and measures internationally and within the EU by, for instance, implementing recommendations in the EU Fraud Prevention Action Plan.

5. Provide incentives and regulatory guidance to spur industry to further invest in the security of their systems and their brands.

6. Require Certification Authorities to ensure that the entities to which they issue certificates actually exist and meet the relevant security standards, and to provide

[8] www.fdic.gov/news/news/financial/2005/fil10305.html
[9] www.ipgovernance.com
[10] www.nclnet.org/news/2006/Final%20NCL%20Phishing%20Report.pdf
[11] www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.25-1798.29
[12] Consumers Union: “A security freeze lets consumers stop thieves from getting credit in their names. A security freeze locks, or freezes, access to the consumer credit report and credit score. Without this information, a business will not issue new credit to a thief. When the consumer wants to get new credit, he or she uses a PIN to unlock access to the credit file”.

clear information in the certificates about the identities and locations of the certified entities. Certification Authorities should also be required to be independently monitored on a regular basis to ensure that they are fulfilling those obligations.

7. Require financial institutions to implement effective procedures for authenticating online access to accounts and closely monitor the effectiveness of the procedures they use.

8. Assign the liability for financial damages caused by ID theft or phishing to the respective companies or service providers involved and not to consumers unless they are proven to have acted negligently.

9. Mandate the deployment of Internet provider-based spam filters.

10. Support the development (with consumer participation) of common standards on web authentication.

TACD resolves that businesses should:

1. Develop and implement best practices for email communications to customers.

2. Create mechanisms to help innocent victims of ID theft or phishing fraud, including dedicated helplines and international hotlines.

3. Take appropriate measures to automatically ensure a fast rehabilitation of victims whose scoring value has been influenced in a negative way as a consequence of identity theft.

4. Compensate victims for loss of time and money in cases where a business or a credit reporting agency bears responsibility for a case of ID Theft or other failures with a harmful result to consumers.

5. Improve the security of their services and network systems following the principle of “security by design” and making security a default setting rather than an optional extra.

6. Introduce secure mutual identification procedures for communications between users and websites.

7. Use only third-party data storage, aggregation and warehouse providers that have contractually agreed to maintain the highest levels of data security and employee security, and stop doing business with those that do not.

8. Inform consumers quickly and reliably when a breach of their data has occurred. The same should apply on all major credit reporting agencies in the EU which should give free credit reports to consumers (as it is already the case in the U.S.).

9. Monitor the use of their brands and take appropriate actions against fraudsters who abuse them.

10. Help educate consumers about ID theft, phishing and other forms of Internet fraud, and enable consumers to forward questions and report suspected fraud.

ANNEX

Identity theft[13]

Identity theft is generally defined as the misappropriation of the identity (such as the name, date of birth, current address or previous addresses) of another person, without their knowledge or consent. These identity details are then used to obtain goods and services in that person's name (source: CIFAS, the UK Fraud Prevention Service). Identity fraud is sometimes used as a synonym, although the concept of identity fraud also encompasses the use of a false, not necessarily real, identity.

Spoofing

"Spoofing" is a term used to describe fraudulent email activity in which the IP address of the original sender is changed to appear as if it originated from a different IP address. Another form of spoofing is the man-in-the-middle attack. In this form of network attack, a hacker will intercept communications between two parties and alter it to convince the recipient to disclose confidential information.

Phishing

Phishing is a specific form of identity theft that employs social engineering and technical subterfuge to obtain consumers' personal information. Typically ID thieves, masquerading as legitimate companies, organizations, or agencies, use emails to lead consumers to counterfeit websites designed to trick them into divulging account numbers, passwords, and other data.

According to the Activity Trends Report of the Anti Phishing Working Group (APWG)[14] - an international industry association focused on eliminating the identity theft and fraud resulting from phishing and email spoofing - 26,150 phishing mail reports were received in August 2006 alone. A May 2005 survey by First Data Corporation showed that 43% of adults in the U.S. had received a phishing contact and of those, 5% (representing 4.5 million people) provided the information requested. Nearly half of the victims reported that their information was used to make unauthorized transactions or commit other frauds[1]. The damage of phishing scams caused to British banks totaled more than £1 million between October 2002 and April 2004[15]. A recent online-survey by the Federation of German Consumer Organisations showed that 85% of the nearly 1000 respondents have already received phishing emails. 55% were endangered as they actually held accounts with the companies that the phishers were impersonating. More than 75% of the respondents said they consider phishing a "risk" or even a "high risk". 8.3% of the respondents stated that they have decided to refrain from any online banking and ecommerce due to these risks. 1.4% of the respondents were actually tricked into providing their personal information and faced financial losses[16].

Pharming and Trojan Attacks

New forms of obtaining access to confidential information or consumers' personal data are even more worrying. For instance, malware can be automatically installed and infect consumers' computers when they click on links to falsified websites from fraudulent emails or on manipulated banner ads displayed on unsuspecting websites.

[13] http://ec.europa.eu/internal_market/fpeg/identity-theft_en.htm
[14] www.antiphishing.org/reports/apwg_report_aug_06.pdf
[15] www.firstdata.com/media/ReleaseDetail.cfm?ReleaseID=163659
[16] www.theregister.co.uk/2004/04/26/phishing_scams/

Malware-dropping websites and new Trojans (malicious programs that are disguised as or embedded within legitimate software) aiming to steal passwords grew to 2,003 in August 2006, compared to 958 in August 2005[17]. Such attacks on consumers' computers may be used to either key-log their access to online accounts when they enter passwords, or to redirect them to fake websites even if they type in the correct Internet addresses of their banks or other online services. The latter attacks are known as "pharming". These attacks are more difficult to avert and detect due to their more sophisticated approach. Although industry has started to react to these threats - by adding anti-phishing functionality to browsers for example - protective measures must be improved and constantly updated to keep up with the evolving nature of this criminal activity.

[17] www.verbraucher-gegen-spam.de