ww&p Walder Wyss & Partners
Attorneys at Law

NewsLetter No. 67 October 2006

Phishing – an insidious form of internet-based criminal activity

Phishing is an internet-based criminal activity that is an increasing problem in Switzerland and around the world. Phishing is a form of fraud in which seemingly legitimate e-mails and websites are used by impostors to induce their victims to disclose sensitive information, such as passwords, bank account numbers and credit card information.

by Suzanne Merz, Attorney-at-Law
+41 44 265 75 56; smerz@wwp.ch

Definition and main problems

The word *phishing* derives from a combination of the words *"password harvesting"* and *"fishing"*. "Phishing" is used to gain any kind of confidential data, such as passwords for internet accounts, credit card numbers, personal identification (PIN) codes or e-banking access information, from unsuspecting internet users.

Phishing attacks exploit the trust customers have in a company's identity and the authenticity of its websites and e-mails. The perpetrators of a phishing scam often send e-mails appearing to come from a well-known company, such as a bank, an internet provider or a retailer. These e-mails have the aura of authenticity because they copy the company's trademarks and trade dress and use sender information, such as e-mail addresses and links to websites that appear to be genuine. Often phishing e-mails purport to give notice of new security measures being undertaken by the company and ask the recipient to verify or reconfirm confidential personal information, such as account numbers, PIN codes and passwords. Other phishing scams create copy a company's website, again in an effort to induce the company's customers to disclose sensitive information via the counterfeit website to the phishers.

In 2006 in the United States, a new form of phishing appeared that relies on voice-over-internet-protocol (VoIP) services, so-called *"vishing."* In this fraud, the perpetrator sent e-mails to a bank's customers asking them to call a specified local telephone number (a VoIP number) that appeared to be the bank's telephone number. Customers who called the indicated telephone number heard a recorded message directing the caller to enter his or her account number.

Whatever the form, phishing may cause serious damage to the targeted company's reputation and undermine confidence in online commerce generally. Unlike attacks on a company's electronic security systems, phishing targets a company's customers. Like breaches of website security systems, phishing attacks create a public relations dilemma for the affected company: customers may need to be informed about potential phishing attacks in order to reduce potential liability issues, on the other hand, such announcements should be carefully drafted in order to avoid the loss of confidence in the company by consumers.

Once the perpetrator is in possession of phished or vished data, the data may then be used to transfer funds from bank accounts, make credit card payments or to facilitate crimes based on the misappropriation of the victim's identity.

Treatment of phishing activities under Swiss law

E-mails and websites used in phishing attacks usually make use of trademarks, logos and other intellectual property belonging to a company. The unauthorised use of trademarks and copyrighted material is an infringement of trademark and copyright laws, which may be subject to criminal prosecution (Art. 61 Swiss Trademark Act, Art. 67 Swiss Copyright Act). The creation and distribution of phishing mails also may be a violation of the Swiss Unfair Competition Act because those engaged in phishing, by creating e-mails and websites that appear genuine, may either cause confusion with the services or business of others or make incorrect or misleading statements about a business and its products or services. Such unfair competition may also be subject to criminal prosecution (Art. 23 Swiss Unfair Competition Act).

The mere creation and distribution of phishing e-mails, under current law, is usually not a criminal offence. However, if the phisher uses phished

confidential information to commit illegal acts, such as the unauthorised transfer of funds, those acts are likely to be subject to punishment under criminal laws. The use of phished bank account information to transfer of funds through internet banking transactions may constitute the fraudulent use of a computer under Art. 147 Swiss Penal Code.

Preventive measures

Anti-phishing software provides one line of defence against phishing attacks. This software is designed to identify potential phishing content in websites and e-mails. Anti-phishing technology also may be included as a feature of some web browsers. In any event, it is advisable to install anti-virus and anti-spyware software and to keep the operating system as well as software updated and secure by installing all security updates and patches.

Special care in handling sensitive data also is crucial and businesses should adopt clear guidelines for the protection of sensitive data, including an action plan in case of potential phishing attacks.

As an additional preventive measure, it may be helpful to inform clients and customers of the potential risks in connection with phishing attacks and the ways in which they can protect themselves against the threat of phishing. Customers and clients should be reminded to call the company's customer service centre immediately if they receive any suspicious e-mail. Customers also may be encouraged to use anti-spam software as protection against phishing-related e-mails. Such information may be implemented on the company's website.

Possible first steps to stop phishing activities

Should a company nevertheless be confronted with phishing attacks, appropriate measures should be taken in order to inform customers and clients of the potential risks. This is important in limiting potential harm to customers and clients, as well in protecting the company against potential liability claims. As mentioned above, corporate guidelines on how phishing attacks should be handled may reduce the possibility that the company's response to an attack is inadequate.

Often it is not easy to identify or locate a phisher. Phishing activities may be launched from anywhere in the world and victims may be harmed worldwide. As a result, the arrest of a phisher may not only be difficult as a practical matter, it also may be made more difficult by applicable national laws.

Usually, a first step in stopping the fraudulent activities of a phisher and preventing further harm is to identify the internet service provider (ISP) providing the e-mail addresses and servers used by the phisher. If the ISP can be identified, the ISP can be given notice of the phishing activities and asked to freeze or delete the e-mail accounts and websites of the phisher, provided that such actions are permitted under applicable laws. In any event, it is crucial to secure any evidence (such as internet and e-mail protocols, copies of websites, etc.) which may be useful in connection with potential legal actions against the phisher. Under the laws of some jurisdictions, the ISP may not be allowed to identify the phisher to the victims of the phishing attack or provide them with copies of documents and other information secured from the websites or e-mail accounts that were involved; in other jurisdictions, ISPs may be required to deliver certain information to the responsible law enforcement authorities (as it is the case under telecommunications legislation in Switzerland). Consequently in Switzerland, it may be possible to obtain information on the identity of a phisher in connection with a criminal complaint. Once the information on identity and location of the phisher is available, further legal steps against phisher may be taken.

ww&p **Walder Wyss & Partners**
Attorneys at Law

Münstergasse 2
P.O. Box 2990
CH-8022 Zurich
Phone +41 44 265 75 11
Fax +41 44 265 75 50
reception@wwp.ch
www.wwp.ch

New location as of November 1st 2006:
Seefeldstrasse 123
P.O. Box 1236
CH-8034 Zurich
Switzerland
Phone +41 44 498 98 98
Fax +41 44 498 98 99