

newsletter

Phishing

Security threat in the Internet

Enticing users to surrender confidential information via fraudulent e-mails and bogus websites has become a significant Internet risk.

Introduction

The number of people using the Internet to purchase goods (online shopping) or conduct banking transactions (online banking) is increasing all the time. According to the latest figures supplied by the Federal Association of German Banks (BdB), around 40% of German banking clients now perform standard transactions online.

But as the Internet increasingly pervades our everyday lives, so do the criminal activities of fraudsters. For a good few years, Internet users have been accustomed to cyber attacks by viruses, Trojan horses, worms and other forms of computer crime. A relatively recent phenomenon, however, is what is known as phishing – now the biggest security threat to the e-commerce and e-banking environment.

Indeed, in the wake of a series of massive phishing attacks, a Swedish bank felt obliged to shut down its online banking service at short notice. In Germany, criminal authorities are currently investigating over 1,000 cases of phishing.

Definition

The term phishing is a variation on "fishing" (hackers invariably replace "f" with "ph" in their communication), the idea being that bait is thrown out in the hope that, while most will ignore, some will be tempted to bite. Phishing is a modern form of Internet fraud. It refers to the act of sending an e-mail to a user while falsely claiming to be a legitimate enterprise in an attempt to scam the user into surrendering private information such as passwords and credit card, social security, and bank account numbers that will be used for identity theft.

Phishing mails are very similar in appearance to the bona fide e-mails issued by legitimate online providers such as banks. As a rule, a scam e-mail will contain a clickable link which will route the user to a bogus website that is virtually identical to the site of the legitimate provider. Often, the address names on a phishing site will vary only slightly from the original URL (eg www.ebay-ag.de instead of www.ebay.de). This authentic appearance together with a perfectly justifiable request to verify, for technical reasons, a banking ID or password aim to get the user to disclose confidential information. As the persons responsible for such scams are highly adept at concealing their identity, investigating such crimes is no easy task.

How a phishing attack is launched

As a rule, phishing e-mails do not target a specific individual but are issued en-masse using state-of-the-art, electronic mass-mailing techniques (spam). In the course of a single phishing attack, hundreds of thousands of e-mails may be dispatched. The mailing campaign adopts a scatter-shot approach, under the assumption that at least some of the recipients will be clients of the organisation.

Typically, a phishing attack will comprise the following phases:

- The attacker obtains the e-mail addresses of his potential targets;
- The attacker designs an e-mail that looks as though it has been produced by a trustworthy institution (eg an online bank, eBay); the content of the mail requests the recipient to verify confidential access data;
- Using a bogus sender address (eg userservice@volksbank.de), the perpetrator then mass-mails the spam to potential victims;
- The e-mail may prompt the victim to complete an electronic form, visit a bogus website, or open attached malware;
- Having obtained confidential banking data (passwords, PINs, TANs, etc), the fraudster can set about profiting from the scam by withdrawing cash from online bank accounts, making purchases from online stores, etc).

Current figures

In August 2005, the Anti-Phishing Working Group (APWG) registered around 13,700 phishing mail campaigns worldwide. In the same month, the number of phishing websites reached a new high of around 5,200 (see graph). According to the APWG, the average lifespan of a phishing website was 5.5 days, a slight drop compared with previous months.

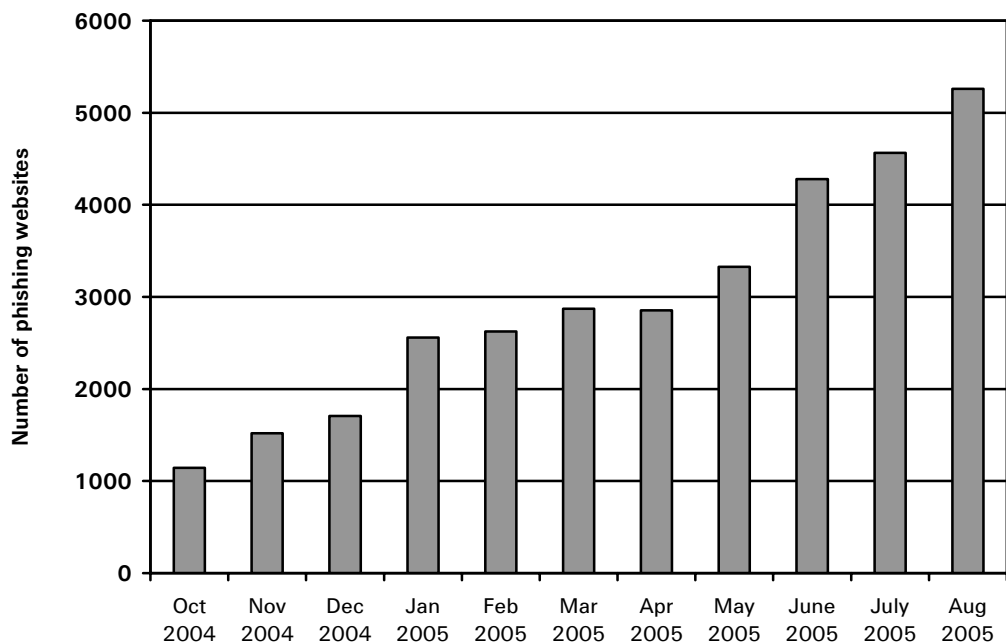


Fig.: Number of new phishing websites (Oct 2004 - Aug 2005). Source: APWG

According to the APWG, 75-100 million phishing mails are sent out each day. It is estimated that, of these, around 20% are opened, while in 3-5% of cases, the recipients comply with the request to divulge sensitive data.

Targets

An analysis of phishing websites and attacked organisations shows that financial service providers are hardest hit. A break-down of phishing attacks by industry sector produced the following picture (source: APWG):

Financial service providers	85.9%
Internet service providers	5.6%
Retail companies	2.8%
Others	5.7%

One of the first European banks to be afflicted by the phishing syndrome was Germany's Postbank. But savings banks, other financial institutions and online stores are equally highly exposed to this form of computer crime. Indeed, clients of the online auction house eBay are frequently the target of phishing attacks. In two spectacular cases, scam artists used data obtained by phishing to purchase goods worth almost a million euros from the eBay site. The spoofed companies suffer not only financially, their professional image is impaired, too. What is more, phishing erodes customer confidence in e-commerce and online banking.

Information for the underwriter

Phishing attacks represent a serious loss potential for electronic commerce and banking, and identity theft can leave a big hole in the pockets of Internet users. The Gartner Group (USA) estimated that the direct cost to US credit-card companies and banks was more than USD 1.2 billion in 2004. Other estimates put a much bigger figure on the loss.

A more selective variant of phishing is "spear fishing", where specific individuals in a company are enticed to divulge passwords and access codes to corporate computer networks for the purpose of industrial espionage.

As phishing attacks become more varied and sophisticated (they sometimes employ backdoor software and other malware/spyware), the risk of corporate and client data being manipulated increases. This can lead to a corresponding increase in exposure of IT insurance covers (first/third-party damage) eg computer crime insurance.

Generally, inadequate IT security, eg obsolete access control systems, can, in the event of a loss, lead to liability suits being brought against the operators of those systems.

Contact

AssTech GmbH
Postfach 1211
85766 Unterföhring bei München
Telephone + 49 89 3844-1585
Telefax + 49 89 3844-1586
info@asstech.com
www.asstech.com