

The Evolution of Phishing

By Michael Urban

Many believe that phishing is purely a tactic carried out in our current Internet and computer environment, but this is not the case. Phishing is really the use of social engineering to gain illegal access to funds or privileged information through any communication channel that is heard, read or surfed by the victim. The concept has been around for years. In fact, the term “phishing” came from “phreaking,” which means hacking or cheating a phone system to make a free long-distance call.


What is phishing?

Phishing tactics became mainstreamed when criminals adapted their techniques to the financial services industry and its associated brand attributes, tricking unsuspecting consumers into providing the information required to take over their financial lives. The goal was, and still is, to scam as many people as possible using a well-known bank or financial institution logo and an urgent message requesting that the consumer update his or her account information at a counterfeit Website that looks official.

Even though the tactic doesn't fool most consumers, fraudsters rely on what's called “spam economics” – send out millions of email messages for a one or two percent response rate. This is, ironically, a better return than most direct-mail marketing campaigns used by credit-card issuers.

PIN phishing and cross-scripting

In 2003 PIN phishing was discovered. It uses the same premise to compromise consumers' PIN and cardholder information; the scammers create cards and steal money through ATMs. PIN phishing attacks initially used a method of spamming email messages to consumers with the brands and logos of well-known Internet companies. In a move similar to the phishing tactics used against



The phishing techniques in use in cyberspace today were created in the early- to mid-1990s. Hackers began sending out emails to unsuspecting AOL members, requesting their identification and password information. Back when we were charged by the minute, a hacker could get some good use out of a free Internet session. Hackers would collect these AOL user identifications and passwords to use as currency – one user identification and password equaled one “phish.”

bank customers, the consumer was directed to a counterfeit Website to update his or her information.

A short time later, criminals identified a technique called cross-site scripting. It uses a link to a bank's legitimate Website, increasing the email's credibility. But then it quickly directs the consumer to the phishing Website. Criminals also began sending Website screenshots with hidden links to the phishing sites, in order to take users directly to them with one click.

More sophisticated metamorphoses

Now up against savvier consumers, criminals have moved beyond the old goal of tricking victims into giving out their information, to new techniques for secretly acquiring that same information.

Trojan horse programs

As consumers began to hear warnings about phishing emails, the criminals started to employ Trojan horse programs covertly installed onto a consumer's computer. The Trojan horse programs are similar to adware or spyware programs which track what a consumer is doing on the Internet and report the information back to an organization unknown to the consumer. Trojan programs install a keylogger and a backdoor, so the criminal can log in and take control of the consumer's computer.

Trojan horse programs are embedded and picked up at "risky" Websites – pornography and game-cracking sites in particular – and are set up to begin logging keystrokes when a consumer's browser links to an online banking Website. In some cases, the Trojan pops up a window requesting the consumer's card and PIN number. This information is then sent back to the criminal over the Internet Relay Chat (IRC) channel. Online banking consumers whose institutions use card numbers and PINs to authorize them are already socially engineered to fall for this.

Man-in-the-middle attacks and bots

The criminal can also initiate a man-in-the-middle (MITM) attack by using the consumer's active online banking session to transfer money out of his or her account or to access additional private consumer information. MITM attacks typically bypass the multi-factor authentication at an online banking site or corporate network, since the consumer has already successfully logged on. Additionally,

a MITM attack can be carried out by requesting the multi-factor changing code or next password from a list at a counterfeit Website, and then quickly logging in to the consumer's account within the time window of the password. This generally happens within 60 seconds of the compromise, as most security tokens expire within that time. If the Website uses a list of passwords, the criminal has a wider window to access the consumer's account.

Trojan horse programs and the proliferation of always-on Internet access allow criminals to turn compromised computers into "bots." Taking over thousands of computers allows the criminal to create an outlaw network of computers called a botnet. The botnet can send more phishing emails or can host phishing Websites. It can also be hired out to other criminals to execute denial-of-service (DoS) attacks that hold Websites for ransom and create general mayhem for their lawful owners.

Phishing and phone systems

The latest form of phishing leverages a spammed email with a phone number instead of a Website link. This technique penetrates an already established comfort zone with most consumers. Interactive Voice Response (IVR) systems have been commonplace for the last ten years, and consumers are accustomed to dealing with them. By posing behind a phone number, criminals can circumvent the warnings about clicking on emails and entering personal information into a Website.

VoIP

The development of Voice over Internet Protocol (VoIP) phones has inadvertently aided criminals in the capture of cardholder data. VoIP telephones utilize the Internet instead of traditional landlines to deliver communi-

phone line. The low cost of VoIP lines and the relative ease with which they are obtained have led criminals to adopt this technology. The criminals set up an IVR system on a compromised computer using off-the-shelf software. They then send out phishing emails directing consumers to dial the VoIP telephone number instead of going to a Website to update their personal information. When a consumer dials into the fraudulent phone number, he or she is directed to enter personal information: card number, PIN, CVV2 code, and so forth.

Security best practices for financial institutions

Criminals will continue to morph their techniques to phish information from consumers. The goal for security is to protect the integrity of financial delivery channels and preserve consumer confidence in them. Certainly, financial institutions that lead by implementing the best security available will reap the benefits, including reduction in fraud; protection of brand and customers; and gain in bottom line, stock valuation and industry recognition.

Management and reduction of these risks requires best practices targeting several areas, particularly corporate security controls.

1. Utilize traditional communication channels such as statement stuffers, rather than email. Using mass emails with Web links socially engineers your customers to click on links from your organization, and may result in a phishing situation in the future.
2. Use your financial institution's domain name as the entry point to your online banking service delivery. Do not use IP addresses or confusing links in the Web address bar. Care in this detail will help consumers know they are on your site.
3. Use ATM PIN numbers only for authentication of ATM and POS transactions. Never use them to authenticate identity on your online banking Website or for telephone banking. This is another example of social engineering that can be used to take advantage of consumers.
4. Verify CVV and/or CVC on PIN-based ATM and POS transactions. These codes are in the magnetic stripes of the card, and the consumer cannot reveal them in a phishing situation. In fact, it is worth verifying all of the information on the magnetic stripe during transaction authorization. Reissue the consum-

The development of Voice over Internet Protocol (VoIP) phones has inadvertently aided criminals in the capture of cardholder data.

cation services. Once a VoIP line has been established, it allows communication to flow freely from any land- or Internet-based tele-

Trojan horse programs and the proliferation of always-on Internet access allow criminals to turn compromised computers into “bots.”

er a new card (with a new number) if there is any mismatch, especially CVV/CVC mismatches, since this means a criminal has the card number and is trying to make it work.

5. Use neural network technology to identify suspicious transaction behavior for your consumers across all of your delivery channels. Include checks, debit-card transactions, online banking transactions, and line-of-credit usage. A criminal using a MITM attack will be flagged, since the transaction will be outside the consumer's normal transaction behavior.
6. Use multi-factor authentication for consumer access to online banking sites. Even though this is still susceptible to MITM attacks, it does provide a higher degree of security.
7. Profile computer information such as IP address, location information and computer fingerprinting to uniquely identify devices accessing consumers' accounts over the Internet.
8. Train customer service representatives (CSRs) on the latest compromise techniques, and have a hotline or knowledge base they can resort to when new phishing scams arise.
9. Develop communication scripts for CSRs to use when contacting consumers on the phone about compromised accounts.
10. Draft communication templates for any documentation accompanying replacement cards sent to consumers, explaining why the card is being reissued.
11. Develop procedures to expedite funds to reimburse consumers when their accounts are compromised.

12. Report losses to federal law-enforcement agencies so they can be aggregated and linked with other fraud. This linking process will help law enforcement create a bigger case with a better chance for prosecution.
13. Employ best practices at the time of application approval or of any changes to a consumer's profile, such as change of address, new credit lines, etc. Many organizations send a postcard with the new or changed address to the old home address, to alert the consumer that a change of address was made to the account.

Careful up-front analysis and ongoing monitoring of accounts go a long way to protect consumers and reduce liabilities. Criminals take the path of least resistance. The more resistance they encounter, the more likely they will look somewhere else for the easy money.

Conclusion

Phishing techniques will use any possible communication channel to socially engineer their desired illegal access to funds or privileged information. The evolution of phishing shows that its success depends on taking quick advantage of both consumers' suggestibility in the face of social engineering, and their unsure responses to new technologies. As more and more entities move into the online space, those financial institutions which follow security best practices to protect financial delivery channels will reduce fraud; protect their brands and customers; and gain in bottom line, stock valuation and industry recognition.

About the Author

Michael Urban has over 13 years experience in banking and electronic payment systems. He is an inventor and director of Fair Isaac Corporation's CardAlert Fraud Manager Service, a national risk management service specializing in counterfeit card fraud detection and control. Michael is a board member of the ATM Industry Association (ATMIA) and the Global ATM Security Alliance (GASA). He was recognized as the 2005 ATMIA Crime Fighter of the Year.