



Hook, Line and Sinker

Phishing Attacks Going "Professional"

A Special Report by Trend Micro

Phishing is slowly becoming a household term, with a new scam arriving in users' inboxes as frequently as once per week. Phishing has become so widespread, in fact, that even many *consumers* know what it is!

But what makes phishing different from viruses and other threats – and why has it become so popular? The biggest differentiator between phishing and other threats such as viruses is the *intent* behind the attack. Many writers of viruses, worms, and other malware seek to inflict damage on users' computers or files, while others want the notoriety that can come with a successful attack that spreads far and wide.

Phishers, on the other hand, could care less about inflicting damage on users' hardware and software – and they have no interest in getting themselves into the headlines. On the contrary, phishing scams are designed specifically to operate under the radar, with their writers choosing fortune over fame.

The Spam-Phishing connection

E-mail spoofing techniques bind these two profit-driven attacks.

E-mail spoofing is based on fundamental flaws in SMTP and Internet protocols. Because of these flaws, the origin of spoofed E-mail is very difficult, if not impossible, to determine.

Also, any mail client or server, no matter how well-built it is, can still be hacked via port 25. Hackers can use these mail clients and servers for a variety of malicious purposes, including sending unsolicited E-mail by bulk or propagating E-mail-borne malware.

Repairing these flaws in existing computing protocols would require a substantial overhaul of the entire computing world!

Instead of competing with other malware writers for notoriety, the people behind online profit-driven attacks are spending their time developing and improving techniques to increase their chances of stealing more valuable information – anonymously and more efficiently.

As with other profit-driven attacks, phishing utilizes the power of the Internet – the same medium that drives myriad businesses and services throughout the world.

Phishing is actually two online identity thefts used together. In phishing scams, the identity of the target company is stolen first in order to steal even more identities—those of unsuspecting customers of the target company.

A typical phishing attack is made up of two components: an authentic-looking e-mail and a fraudulent Web page. The content of the phishing e-mail is usually designed to confuse, upset or even excite the recipient. Typical e-mail topics include account problems, account verifications, security updates/upgrades, and new product/service offerings. Recipients of the e-mail are prompted to react immediately. They then click on the link provided in the e-mail body, which actually directs them to the phishing Web page.

Like the phishing e-mail, the phishing Web page almost always possesses the look and feel of the original—often containing the same company logos, graphics, writing style, fonts, layout, etc. This spoofed Web page may also include a graphical user interface (GUI) intended to lure the user into entering his/her bank account information, credit card number, Social Security number, passwords or other sensitive information. All types of stolen information may then be used either by the phisher or sent to anonymous, remote users.

The Evolution of Phishing

Phishing can be considered as the natural derivative of spamming. Both spamming and phishing mainly employ e-mail-spoofing techniques, which are actually possible because of fundamental and critical flaws in SMTP and standard Internet protocols.

Phishing, however, goes a step beyond spamming by making extensive use of spam distribution tricks and techniques, while adding its own unique identity theft routines.

Like many hacking pseudonyms, we can trace phishing's roots back to the now infamous *phreaking* hacks of the 1970s, which involved the illegal accessing of telephone systems using a simple child's toy. Phishing follows the tradition of *phone phreaking* by also making ill use of technical knowledge in order to obtain unauthorized practical benefits.



HACKER PROFILE: John “Cap’n Crunch” Draper

John Draper used a plastic toy whistle from a Cap’n Crunch cereal box with his own “bluebox”, which allowed him to make free phone calls. The said whistle produced the 2600 Hz tone necessary to authorize calls.¹

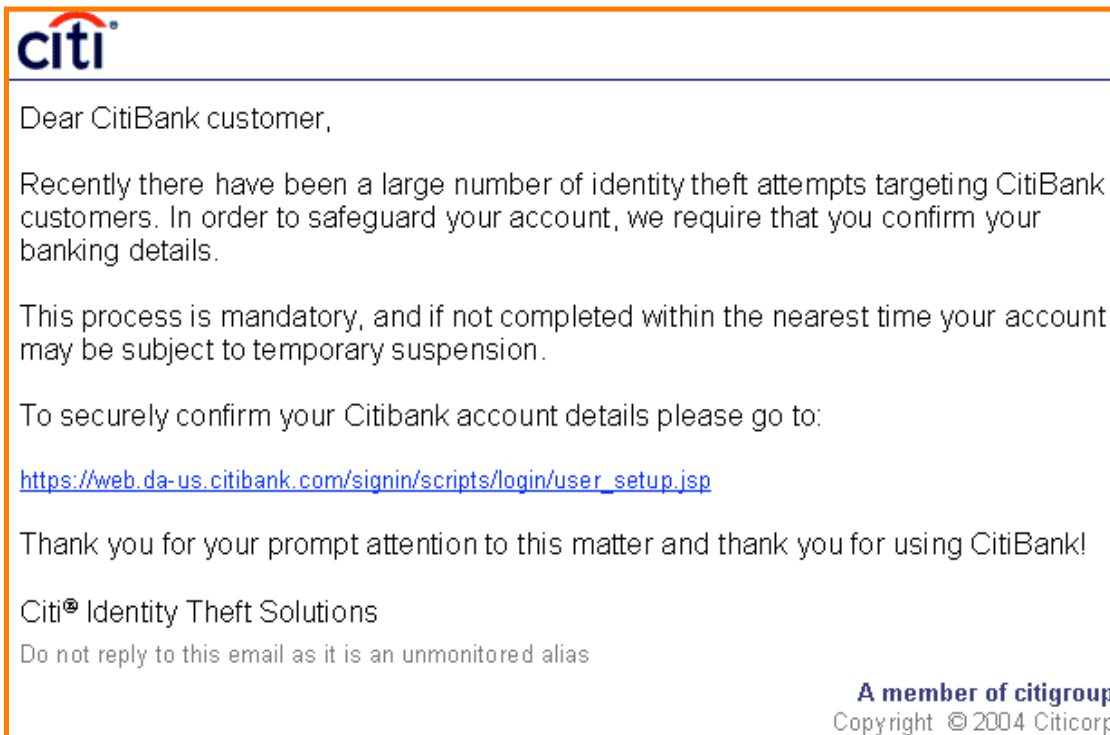
He went to prison for his phone phreaking activities.


Early phishing scams were little more than an e-mail, written in plain ASCII text, requesting that the user divulge personal information. The text was poorly written, with numerous grammatical and spelling errors throughout. Users soon caught on to these scams.

Over the years, however, phishing has evolved into a far more professional-appearing, complex scam. The plain ASCII e-mails have largely been replaced by professional-looking, HTML-based e-mails that include font styles, colors, graphics, and other elements to successfully spoof the supposed sender. Most also contain a link to a Website, where the information is actually collected. The site is nearly always an exact replica of the spoofed site, thereby luring users into parting with their personal information. In many present-day phishing scams, the grammatical and spelling errors have ceased, now replaced with a polished, professional look and feel one would expect from a bank or other target of phishing attacks.

The harvesting of the information on the back-end has also become far more complex. Gone are the script kiddies who obtained a credit card number for their personal use. Current phishing scams utilize an organized and systematic means of gathering, collating and exploiting stolen information so as to maximize profit – lending credence to the belief of some industry experts that present-day phishing scams may be run by organized crime groups.

Examples of the Components of a Modern Phishing Attack





Dear CitiBank customer,

Recently there have been a large number of identity theft attempts targeting CitiBank customers. In order to safeguard your account, we require that you confirm your banking details.

This process is mandatory, and if not completed within the nearest time your account may be subject to temporary suspension.

To securely confirm your Citibank account details please go to:

https://web.da-us.citibank.com/signin/scripts/login/user_setup.jsp

Thank you for your prompt attention to this matter and thank you for using CitiBank!

Citi® Identity Theft Solutions

Do not reply to this email as it is an unmonitored alias

A member of citigroup
Copyright © 2004 Citicorp

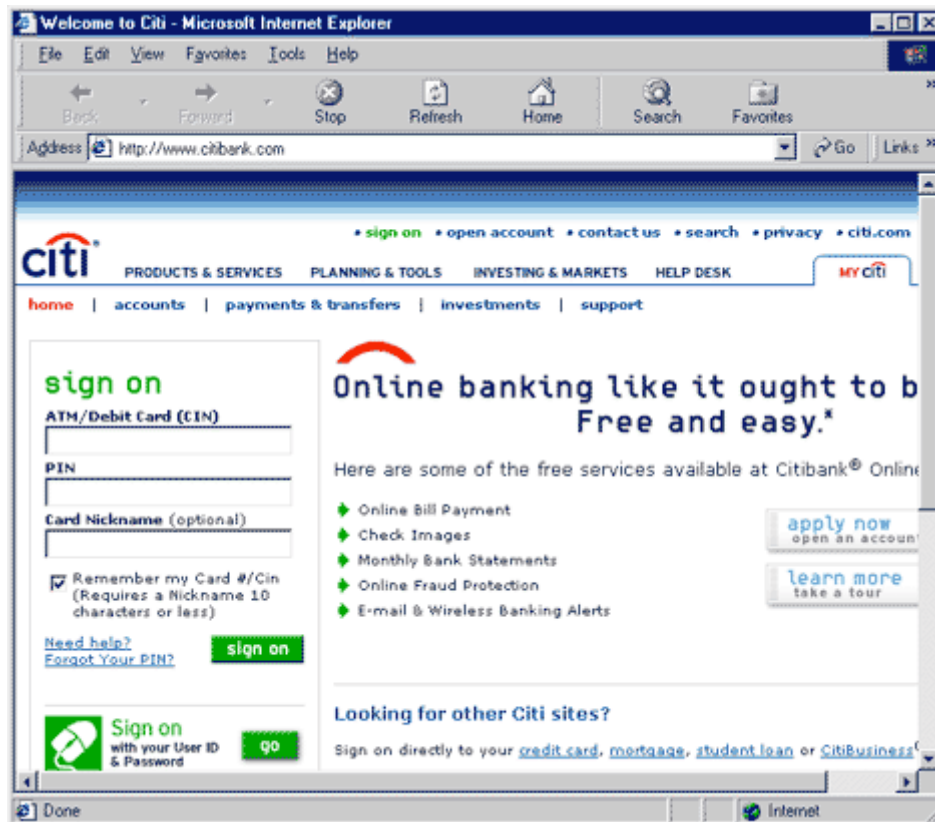
Source: Trend Micro Phishing Encyclopedia
<http://www.trendmicro.com/en/security/phishing/overview.htm>

This e-mail is designed to alarm the recipient into thinking that his/her account may not be secure. Adopting a business style of writing, it then tries to convince the recipient that the account verification process is mandatory and that he/she must act *immediately* to avoid the temporary suspension of the account. The e-mail then proceeds to provide the link to the fraudulent Web site. Although the indicated URL may look legit, phishers have devised ways to mask the actual URL.

This phishing e-mail tries to convince recipients that it is indeed authentic by making use of the Citibank logo and trade names, as well as the copyright and “registered” symbols. Some recent phishing e-mails have even included the bank’s warnings about phishing attacks!

Most importantly, phishers are getting better at their writing style. This, coupled with better spoofing techniques, the extensive use of graphics and other elements to make it look genuine, and better targeting techniques to ensure the phishing e-mail only goes to the actual customers of the bank, help increase the odds that the phishing attack will be successful.

Any user fooled by the e-mail would be sent to the Web site shown below. As mentioned previously, the fraudulent Web page is an *exact replica* of the genuine one, thereby making it even more convincing than the e-mail.



Source: Trend Micro Phishing Encyclopedia
<http://www.trendmicro.com/en/security/phishing/overview.htm>

Phishing Techniques

Here are the five major Phishing techniques – in a general order of technical complexity – that are all, to some degree, in use today:

Explicit Display of Phishing URL – This is arguably the easiest technique to identify. In this case, phishers make no effort in hiding the actual phishing URL, and so the phishing URL is explicitly displayed on the address bar. In some cases, it involves the use of domain names that resemble legitimate domains.

Address Bar Spoofing – This involves the alteration of the browser's address bar to display a legitimate address. The overall effect is that a text object with a white background hovers over the phishing URL to display a legitimate bank address. However, checking the properties window of the Web page reveals the real address of the spoofed site.

Using Pop-up Windows - This technique uses a script that opens a legitimate Web site in the background. The spoofed pop-up window is usually identical to the legitimate Web site and is opened in the foreground. It misleads the user into thinking that the pop-up window is directly related to the official page. In some cases, the pop-up window only covers a portion of the legitimate Web site.

Using Forms within the Phishing E-mail – In this case, the Phishing e-mail arrives in HTML format. It already contains the embedded form that is used to gather personal/account

information from users. Stolen details are usually sent to a specified e-mail address or are being posted to a particular Web site.

Web site spoofing – This involves the laborious creation of exact replicas of legitimate, trusted sites. The spoofed Web site looks entirely like the real one, down to the last detail. All links visible in the spoofed site are under one phishing domain.

Phishing scams usually exploit a certain Microsoft Windows vulnerability concerning URL redirections on unpatched machines. More information on this vulnerability can be found at <http://www.microsoft.com/technet/security/bulletin/MS04-004.msp>.

The Impact of Phishing Attacks

Stolen bank account information can be exploited in a variety of ways. After illegally accessing the victim's account, phishers can change account passwords, effectively locking the legitimate user out of his or her own account. They can then transfer available funds electronically to a temporary account and withdraw them before the victim becomes aware of it. Phishers may also write bogus checks on the account of the victim.

Harvested credit card credentials are used to make unauthorized online subscriptions or purchases. Victims would only know about it when they see their outrageous monthly bills or if they discover that their credit cards have been maxed out.

Stolen ATM account information, such as card numbers, PINs, and expiration dates may be used by phishers to create duplicate ATM cards. Phishers may then proceed to empty the corresponding ATM accounts.

Generally, all stolen information may be kept for future use and may also be traded or sold in online underground communities.

However, the overall impact of phishing attacks does not necessarily end with individual victims having their accounts emptied. One has to consider the fact that successful phishing attacks also result in a violation of privacy of the individual consumer, and an unauthorized use of the network identity of an enterprise.

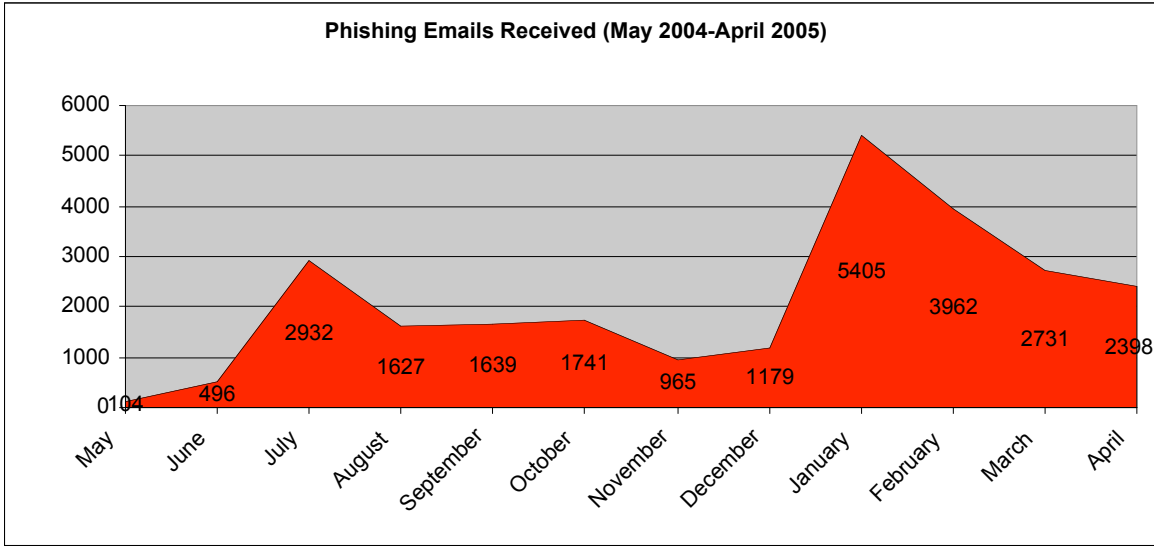
Phishing may invariably taint the reputation and diminish the credibility of the companies that were used in phishing attacks. In business, the trade name is an important asset of each company, and it takes years of hard work to build a name that customers actually trust. Victims of phishing attacks may find it hard to transact business with companies that seemingly could not protect their assets and privacy. Customer trust is an asset that is difficult to measure, but losing it could certainly spell bad news for any business.

In the long run, the success of phishing attacks could influence more and more people to lose trust in the Internet as a means of doing business. This could impede the further growth and development of the Internet as a technological innovation that actually contributes to the improvement of life in general.

Phishing Incidence

The first isolated phishing scams were publicized around March 1997. However, the attention given to phishing was initially very minimal. Through better sample collection and growing public awareness, phishing incidence became more pronounced in the second quarter of 2004.

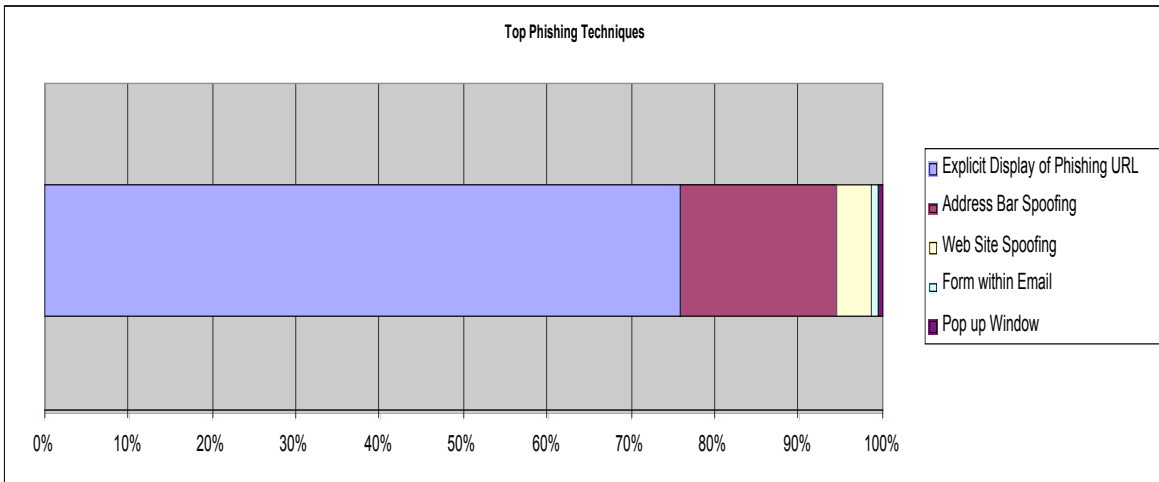
>> TREND MICRO: PHISHING ATTACKS GOING PROFESSIONAL



Source: Trend Micro

The graph above shows that phishing incidence peaked during the month of January 2005, with a total of 5,405 received samples. Since then, reported phishing incidence has been on a seemingly steady decline. This may be due to the changing nature of phishing scams. For one thing, attacks are believed to have become more organized and professional than ever, and instead of a one-to-one phishing e-mail to victim relationship, one attack can lure multiple victims. So, while the quantity of e-mails may be going down, the quality – and therefore the *effectiveness* – of the attacks are on the rise.

The most alarming part of this statistic, though, is when it's coupled with the statistics of the incidence of attacks by type. As the graph below illustrates, 76% of phishing scams involved the explicit display of phishing URLs. This figure is quite daunting since this technique is arguably the easiest to detect. This data suggests that with the increasing quality in appearance of phishing attacks, users are not actually scrutinizing the actual *messages!*



Source: Trend Micro

Here is a summary of the other techniques:

- 19% use address bar spoofing.
- 4% use full-fledged spoofed Web sites.
- 1% arrives as HTML e-mail using fake forms.
- The rest use pop-up windows.

User Education – The Best Defense

Perhaps one of the most important things to consider regarding phishing is that the extent of its success is mainly dependent on the people who actually receive the e-mail. Clearly, the human factor is the only vulnerability that is virtually unpatchable, and no security product, service or update can protect people from their own choices. Users must never let their growing dependency on technology lead to complacency and irresponsibility. Users can contribute significantly to the security of the Internet by just following certain guidelines and performing simple, logical practices, such as those outlined below.

Phishing-related Best Practices

The Internet community is not completely helpless against phishing attacks. This section outlines several logical guidelines and phishing-related best practices that could help prevent users of all types from being victimized by phishing scams.

Personal and Home Networks

1. Practice prudence when receiving e-mail messages that ask for account credentials. Remember, phishing e-mails are designed to upset, confuse, or excite recipients, to entice them to react immediately.
2. Ensure that any Web site visited is secure when submitting sensitive information such as credit card numbers. One indication that a Web address is secure is if it starts with *https://* rather than *http://*. Another indication is a padlock icon at the bottom of the screen, which when clicked, displays a security certificate.
3. Do not click any link inside an e-mail that is suspected to be spoofed. Instead, go directly to the legitimate company's site by directly typing in the legitimate company URL in the address bar of the browser, then log on from there. One can also call the company directly. Many previously-targeted companies have disclosed contact information for phishing-related incidents.
4. Avoid opening any file attachments of suspected phishing e-mail messages as they might execute a malware program that can steal personal information.
5. Make a habit of scouring the Internet for the latest news and information regarding phishing. Trend Micro regularly maintains this Phishing-specific Web page:
<http://www.trendmicro.com/en/security/phishing/overview.htm>
6. Ensure that your browser is up-to-date and security patches are always promptly applied. For Internet Explorer, a special patch relating to certain phishing schemes can be downloaded at:

<http://support.microsoft.com/?id=833786>

7. Phishing attacks may also be linked to various malware and spyware programs for distribution and execution purposes. Therefore, consider installing personal security software that protects not only against malware and hacker intrusion, but also against phishing attacks.
8. Always update installed security software.
9. Report suspected phishing attacks to any of the following Web sites and e-mail addresses:
Internet Crime Complaint Center (a joint project of the FBI and the National Collar Crime Center):

<http://www.ic3.gov>

Federal Trade Commission's identity theft Web site:

<http://www.consumer.gov/idtheft>

Federal Trade Commission's e-mail address:

uce@ftc.gov

Anti-Phishing Working Group:

reportphishing@antiphishing.org

Trend Micro Anti-Fraud Unit:

antifraud@support.trendmicro.com

Trend Micro encourages people to report phishing incidents to facilitate better sample gathering.

Small and Medium Businesses (SMB) to Enterprise Networks

Aside from those previously mentioned, here are some more guidelines for company networks:

1. Establish and enforce corporate e-mail policies.
2. Regularly conduct highly visible anti-phishing information campaigns.
3. Support consumer education regarding phishing.
4. Consider acquiring anti-phishing products and services from your trusted security software vendor. The main concern for the enterprise network is to prevent phishing e-mail from ever reaching the inboxes of employees. Typical anti-phishing products are integrated with a regularly maintained database of malicious URLs. They also usually

employ both heuristics and signature-based methods in scanning e-mail for possible malicious characteristics.

Trend Micro also provides a safe computing guide that can serve as a starting point for all computer users in protecting their systems and networks. The safe computing guide is outlined at:

<http://www.trendmicro.com/en/security/general/guide/overview.htm>

Conclusion

Identity has always been a valuable commodity. In the old days, people would “steal” identities through skillful imitation or mimicry. Centuries later, people would rummage through another person’s mailbox, drawers, and even garbage bins in search for misplaced information. In this day and age, identity has already been translated to a series of alphanumeric strings, and ultimately, discrete bits of data. People can now transact all sorts of business and perform a host of services without their physical presence. The convenience and efficiency brought about by this technology has unfortunately provided another avenue for some people to perform reprehensible acts that can actually generate profit at the victim’s expense.

About Trend Micro

Trend Micro Inc. provides centrally controlled server-based virus protection and content filtering products and services. By protecting information that flows through Internet gateways, email servers, and file servers, Trend Micro allows companies worldwide to stop viruses and other malicious codes at a central access point before they reach the desktop.