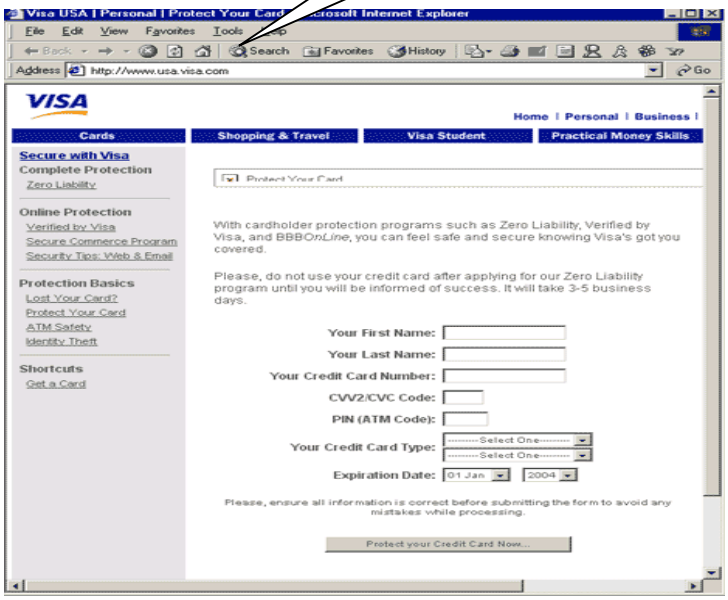
The Second Generation of Phishing: E-mails no Longer Required

Simply Entering a Bank-related Web Address Could Take You on a Phishing Trip!

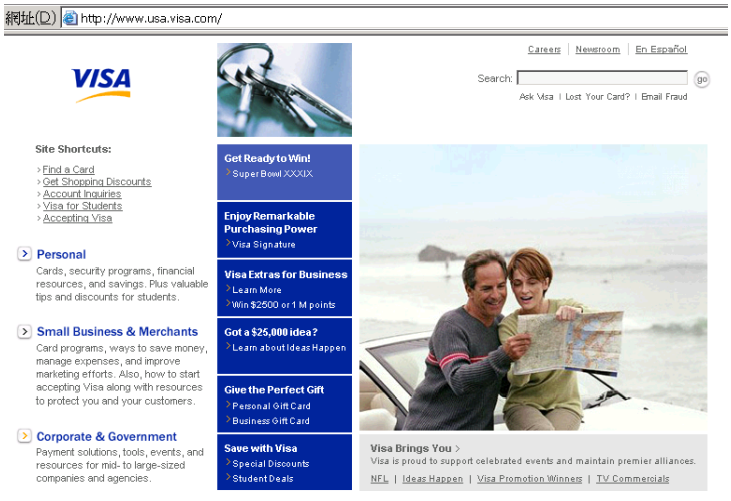
"We have discovered that someone has used your Visa card number, which could happen if you have been shopping on-line. To avoid this from happening again, we strongly recommend you fill in the forms on our company website and install the Zero Liability program, in order to quickly investigate this accident.

Visa Customer Service Centre

http://www.usa.visa.com



The fake Visa website is difficult to identify; even the website address is exactly the same as the authentic site. (The webpage above is a fake; the one below is real. The above picture is the site shown by January's HTML_VISAFRAUD.A.)



By clicking on the *Continue* in this HTML message, a webpage that looks exactly like the original appears, waiting for you to take the bait (see picture). This is HTML_VISAFRAUD.A, one example of a malware that has been using the Visa name to deceive victims since January of this year. This kind of 'Phishing' has become a common phenomenon over the last year. This form of fraud is used to steal the personal information of email users, including ID numbers, ATM codes, credit card numbers and more. These emails use the names of well-known companies to warn unsuspecting customers and urge them to visit a fake website to enter their personal information. As these fake websites often look just like the actual websites, many victims have been fooled, unwittingly entering their personal information. In addition, oftentimes the larger the bank, the more

people fooled.

In its early days, phishing was mainly conducted in English, with numerous grammatical errors, and users could avoid falling into their trap as long as they did not click on the link in the message. However, it is now much harder to recognize fraudulent emails; in fact, emails are not always used as bait anymore. What is happening now can be called the second generation of phishing. Trend Micro Trendlabs, a global antivirus research and support center of Trend Micro, has detected a new Trojan horse virus, TROJ_BANCOS.CP, which monitors the browsing actions of Internet Explorer in order to record the victim's browsing behavior. Once the title of the Internet Explorer window matches specified banking-related strings, a login page that looks genuine is produced, asking for the user's sensitive information, such as passwords. This secretly recorded information is stored in a special folder, and is then automatically sent to hackers via email. After this information is sent, the folder is automatically deleted in order to avoid leaving any tracks. It is very possible that a victim's information is stolen without the victim ever knowing.

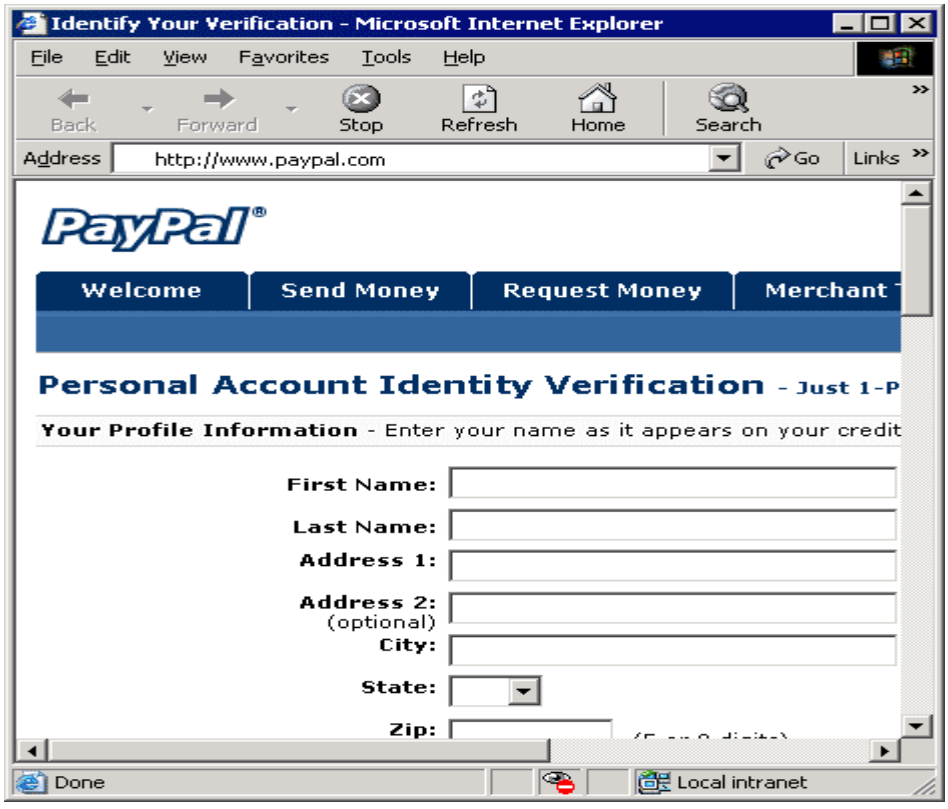
TrendLabs explains that this is very different from phishing of the past, when they simply consisted of fraudulent letters seemingly from banks. Most internet users could easily identify those fraudulent phishing emails from their grammatical errors. However, users now need only enter a bank's website address to fall victim. TrendLabs points out that there are currently eighty variants of TROJ_BANCOS, the newest of which logs keystrokes, collects data and even print screen, then it sends those stolen information to the virus author.

Once you enter a bank-related string specified by TROJ_BANCOS, a fake website will appear asking for personal information.

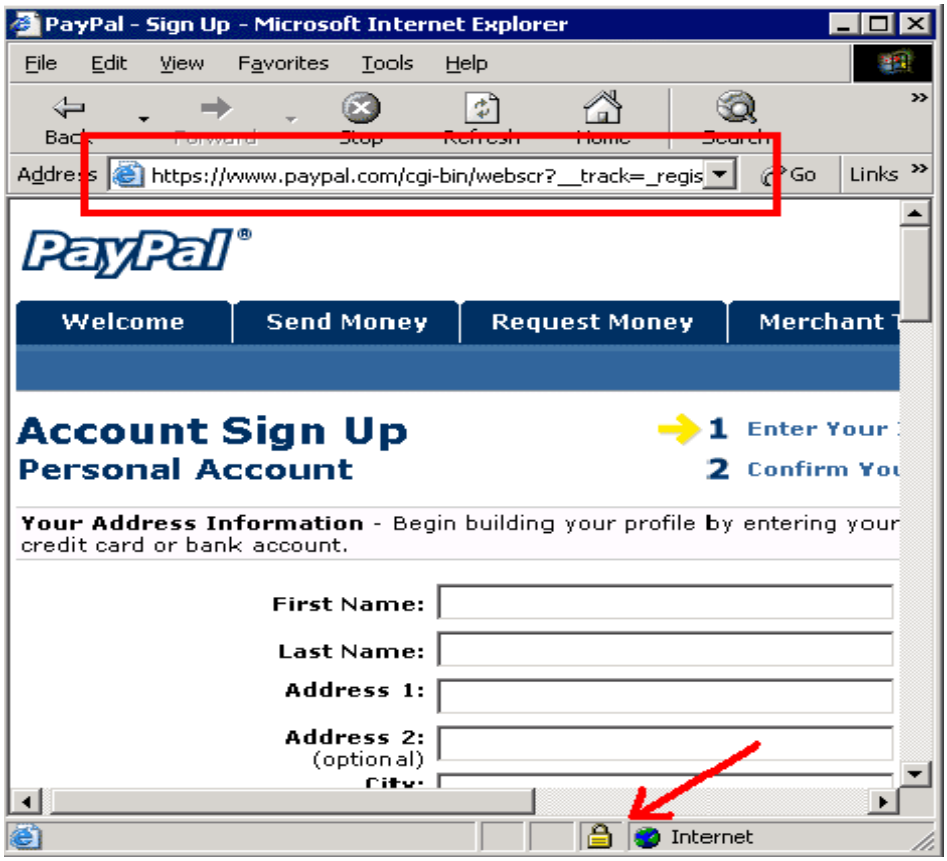
Trend Micro shows an easy way to identify such sites: legitimate HTTPS website must display the padlock icon in the status bar. When a website address begins with HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer), it signifies that a Secure Socket Layer is added to the HTTP address, making it difficult for HTTP documents to be intercepted during transmission over the internet. Therefore, the address for most websites asking for personal information will begin with HTTPS. However, this address itself is not very difficult for hackers to copy, so users must also check to see if the padlock icon is displayed in the lower right corner of the window.

In the Citibank phishing case, the link takes you to what looks like a valid Citibank website, with an address that begins with Https. However, while it looks like a secure site, there is no padlock icon in the lower right corner to verify it as a safe website.

In another example, HTML_PAYPFRAUD.A impersonates Paypal, displaying a seemingly real registration page with legitimate web address of Paypal, but the login page that is actually shown is a fake. In fact, the login page used by Paypall users is not the site's homepage; in addition, the login page displays the padlock icon, which the fake website does not.



The fake login page of Paypal – displaying homepage address of Paypal in the upper status bar, no padlock icon shown in lower right corner.



The authentic login page: the link which appears is actually not the homepage address of Paybal, in addition, padlock icon is there.

Security specialists appeal to internet users to employ an antivirus program that blocks phishing websites, such as Trend Micro's PhishTrap. This program actively stops users from accessing fraudulent websites and preventing them from downloading malware, including phishing websites with complicated script programs and those that avoid HTTP filter scanners.

Report phishing mails to: antifraud@support.trendmicro.com

Internet security specialists Trend Micro: www.trendmicro.com