

Phishing & Pharming Scam

This Internet scam has already claimed one million victims.

Phishers send fraudulent or spoofed e-mails containing authentic looking logos and graphics of banks, e-retailers and credit card companies to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. Since the e-mail looks authentic to the untrained eye phishers are often able to convince the recipients of their e-mails to respond.

By clicking on the link, crimeware is planted onto the users PC to steal credentials directly, often using Trojan keylogger spyware.

Pharming crimeware misdirects the user to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning.

The newest scam is activated when you simply open an e-mail, no clicking required.

2 Examples of Phishing E-mails:

Example 1:

E-mail Subject Line: LaSalle Bank - 'IMPORTANT: Account Verification'



We are glad to inform you, that our bank has a new security system. The new updated technology will ensure the security of your payments through our bank.

Hoping you understand that we are doing this for your own safety we suggest you to update your account , this update will maintain the safety of your account . All you have to do is to complete our online secured form . Thank You.

[Continue](#)

Example 2:

E-mail Subject Line: eBay- 'Update Your Account'

03-May-2005

Dear eBay User,

During our regular update and verification of the accounts, we couldn't verify your current information.

Either your information has changed or it is incomplete.

If the account information is not updated to current information

within 5 days then, your access to bid or buy on eBay will be suspended.

go to the link below,

and re-enter your account information.

[Click here to update your account.](#)

*****Please Do Not Reply To This E-Mail As You Will Not Receive A Response*****

To see over 100 examples of actual phish e-mails go to http://www.antiphishing.org/phishing_archive.html

Tips to Prevent Phishing & Pharming

Tip 1: Change your online banking and shopping account passwords every three to six months.

Tip 2: To avoid being led to fraudulent Web sites, retype Web addresses in your browser rather than click through e-mail links.

Tip 3: When the phish site opens up, it looks almost exactly like the legitimate login page. However, a few important clues that this is a fraudulent website can be noticed:

- The suspicious URL in the address bar - it is not hidden with any tech tricks
- The absence of a 'lock' icon in the status bar which indicates you are on an unsecured site.
- No **"s"** after http in the address bar which again indicates you are on an unsecured site.