



# INFORMANT

EDUCATIONAL INFORMATION ABOUT SAFE USE OF THE INTERNET

## ~GONE PHISHING~ Internet Identity Theft

**phishing** (FISH.ing) *pp.* Creating a replica of an existing Web page to fool a user into submitting personal, financial, or password data. —*adj.* —**phisher** *n.*

FBI called **phishing** the “hottest, and most troubling, scam on the Internet.”

### What is Phishing and Pharming?

Phishing attacks steal consumers’ personal identity data and financial account credentials by using ‘spoofed’ e-mails 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. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince up to 5% of recipients to respond. Crimeware is implanted onto PCs to steal credentials directly, often using Trojan keylogger spyware. Pharming crimeware misdirects users to fraudulent sites or proxy servers, typically through DNS (domain name server) hijacking or poisoning.

### How to Avoid Phishing Scams

While online banking and e-commerce is very safe, be careful giving out your personal financial information over the Internet.

- Be suspicious of any email with urgent requests to provide personal financial information or to fill out forms.
- Don’t use the links in an email to get to any web page, call the company on the telephone, or log onto the website directly by typing the web address in your browser.
- Ensure that you’re using a secure website when submitting credit card or other sensitive information via your web browser, URL should be https:// rather than “http://”.
- Routinely log into your online accounts, including bank, credit and debit card statements to ensure that all transactions are legitimate.
- Keep your web browser up to date, Microsoft Internet Explorer users should go to <http://www.microsoft.com/security/> to download a special patch relating to certain phishing schemes.

- Always report “phishing” or “spoofed” e-mails:
  - forward the email to [reportphishing@antiphishing.com](mailto:reportphishing@antiphishing.com)
  - forward the email to the Federal Trade Commission at [spam@ftc.gov](mailto:spam@ftc.gov)
  - forward the email to the “abuse” email address at the company that is being spoofed (e.g. “[spoofof@ebay.com](mailto:spoofof@ebay.com)”)
  - when forwarding spoofed messages, always include the entire original email with its original header information intact.

**Identity Theft Help Sites:**  
[www.antiphishing.org](http://www.antiphishing.org)

**Identity Theft Quiz For Consumers:**  
[www.usdoj.gov/criminal/fraud/websites/idquiz.html](http://www.usdoj.gov/criminal/fraud/websites/idquiz.html)

**Interactive e-Card:**  
[www.ftc.gov/bcp/edu/multimedia/ecards/phishing](http://www.ftc.gov/bcp/edu/multimedia/ecards/phishing)

### Just Say “NO”

- In general - no one should respond/reply to an unsolicited email message, or forward an email message to a friend, family member, or co-workers - when the email message encourages you to do so. For example: Chain e-mails encourage the recipient to forward to as many people as possible, warning them not to break the chain (see definitions at the bottom of the page on how viruses work).
- If you respond to a request to be “removed” (from the “send to” list) from an “unsolicited” message sent to you, you are notifying the sender that you have a working email account. Just delete the message.
- Never open an email attachment, unless you knew it was expected, or you speak with the sender to verify its contents. If you are unsure it is OK, delete the entire message.

*Source: Anti-Phishing Working Group (APWG) - Committed to Wiping Out Internet Scams and Fraud at [www.antiphishing.org](http://www.antiphishing.org).*

### WHAT DOES THAT MEAN?

**Viruses** - A virus is a small piece of software that piggybacks on real programs. Each time the program runs, the virus runs, too.

**E-mail viruses** - An e-mail virus moves around in e-mail messages and usually replicates itself by automatically mailing itself to all the people in the victim’s e-mail address book.

**Worms** - A worm is a small piece of software that uses computer networks and security holes to replicate itself.

**Trojan horses** - A Trojan horse is a computer program, that claims to do one thing (it may claim to be a game) but instead does damage when you run it (it may erase your computer hard disk). Trojan horses have no way to replicate automatically.