

## What is Phishing and Pharming?

Phishing attacks use both **social engineering** and **technical subterfuge** to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use '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 recipients to respond. Technical subterfuge schemes plant **crimeware** onto PCs to steal credentials directly, often using Trojan keylogger spyware. **Pharming** crimeware misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning.

- Be suspicious of any email with urgent requests for personal financial information you can't be sure it wasn't forged or 'spoofed' phishers typically include upsetting or exciting (but false) statements in their emails to get people to react immediately
  - they typically ask for information such as usernames, passwords, credit card numbers, social security numbers, etc.
  - phisher emails are typically NOT personalized, while valid messages from your bank or e-commerce company generally are
- Don't use the links in an email to get to any web page, if you suspect the message might not be authentic instead, call the company on the telephone, or log onto the website directly by typing in the Web address in your browser
- Avoid filling out forms in email messages that ask for personal financial information
  - you should only communicate information such as credit card numbers or account information via a secure website or the telephone
- Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser
  - to make sure you're on a secure Web server, check the beginning of the Web address in your browsers address bar - it should be "https://" rather than just "http://"
- Consider installing a Web browser tool bar to help protect you from known phishing fraud websites
- Regularly log into your online accounts
  - don't leave it for as long as a month before you check each account
- Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate
  - if anything is suspicious, contact your bank and all card issuers
- Ensure that your browser is up to date and security patches applied
- Always report "phishing" or "spoofed" e-mails to the following groups:
  - forward the email to [reportphishing@antiphishing.com](mailto:reportphishing@antiphishing.com)
  - forward the email to the Federal Trade Commission at [spam@uce.gov](mailto:spam@uce.gov)
  - forward the email to the "abuse" email address at the company that is being spoofed (e.g. "spoof@ebay.com")
  - when forwarding spoofed messages, always include the entire original email with its original header information intact
  - notify the Internet Fraud Complaint Center of the FBI by filing a complaint on their website: [www.ifccfbi.gov/](http://www.ifccfbi.gov/)

