

What is Phishing?

Phishing is a high-tech scam that uses spam or pop-up messages to attempt to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, and / other sensitive information.

Phishing is the term coined by hackers who imitate legitimate companies in e-mails to entice people to share passwords or credit card numbers.

What is Spoofing?

Pretending to be something it is not, on the Internet, usually an e-mail or a Web site.

How to report Phishing:

We suggest reporting phishing e-mails or spoofed Web sites to the following groups:

- Forward e-mail to reportphishing@antiphishing.org
- Forward e-mail to the Federal Trade Commission at spam@uce.gov
- Forward the e-mail to the “abuse” e-mail address at the company that is being spoofed (e.g., spoofer@ebay.com).
- When forwarding spoofed messages, always include the entire original e-mail with its original header information intact.
- Notify the Internet Crime Complaint Center of the FBI by filing a complaint on their Web site: www.ic3.gov

Recommended Actions if You’ve become a Victim of a Phishing Scam

If you have given out your credit, debit or atm card information

- Report the incident to the card issuer as quickly as possible
- Report using toll-free numbers and 24-hour services that many companies have established to deal with such emergencies.
- Request your card issuer close your compromised account number and reissue you a new card with a different number.
- Monitor your account activity and review account statements carefully after the information loss.
- If any unauthorized charges appear, call the card issuer immediately and follow up with a hard copy letter via a traditional delivery service such as the U.S. Postal Service. (keep a copy for yourself) describing each questionable charge.

Credit Card Loss or Fraudulent Charges

Your maximum liability under federal law for unauthorized use of your credit card is generally \$50. However, that \$50 potential liability probably does not apply for

unauthorized telephone and Internet transactions because there is “no means to identify the cardholder” in those cases.

ATM or Debit Card Loss or Fraudulent Charges

- Your liability under Federal law for unauthorized use of your ATM or debit card depends on how quickly you report the loss.
- You risk unlimited loss if you fail to report an unauthorized transfer within 60 days after your bank statement containing unauthorized use is mailed to you for transactions made after that 60 day period.

If you have given out your Bank Account Information

- Report the theft of this information to the bank as quickly as possible.
- Request your bank close the compromised account and re-open a like account with a different number.

If you have downloaded a Virus or “Trojan Horse”

Some phishing attacks use viruses and/ or “Trojan Horses” to install programs called “key loggers” on your computer. These programs capture and send out any information that you type to the phisher, including credit card numbers, user names, passwords, Social Security numbers, etc. If this happens, it’s likely you may not be aware of it until you notice unusual transactions on your account.

To minimize this risk, you should:

- Install and / or update anti-virus and personal firewall software
- Update all virus definitions and run a full scan
- If your system appears to have been compromised, repair it and then change your password again, since you may well have transmitted the new one to the hacker
- Check your other accounts! The fraudsters may have helped themselves to many different accounts: ebay account, Paypal, your e-mail ISP, online bank accounts, online trading accounts and other e-commerce accounts, and everything else for which you use online passwords.

If you have given out your Personal Identification information

If you believe you have given out personal information such as your name, address, and Social Security number to someone who may use it for fraud:

Contact the three major credit reporting agencies- Experian, Equifax, and TransUnion and do the following:

- Request that the agencies place a fraud alert and a victim’s statement in your file

- Request a free copy of your credit report to check whether any accounts were opened without your consent.
- Request that the agencies remove inquiries and / or fraudulent accounts stemming from the theft.

How to Practice Safe Computing

The number and sophistication of phishing and spoofing scams sent out to consumers is continuing to increase dramatically. While online banking is widely considered to be as safe as or safer than in-branch or ATM banking, as a general rule you should be careful about giving out your personal financial information over the Internet. Remember, no reputable financial institution will ever request your personal information via email.

Here is a list of recommendations to follow in order to avoid becoming a victim of scams:

1. Be suspicious of any email with urgent requests for personal financial information
2. Be careful of e-mails that are not personalized and / or may contain spelling errors and/ or awkward syntax and phrasing.
3. Be careful of personalized e-mails that ask for personal financial information
4. Do not use links in an e-mail to get to any Web page
5. Do not complete forms in e-mail messages that ask for personal financial information.