



The New York State Consumer Protection Board's **PHISHING SCAM PREVENTION TIPS**



Phishing (also called *pharming* or *whaling*) e-mails trick people into sending money or providing personal information such as usernames, passwords, credit card details, and Social Security numbers to unauthorized individuals who hijack their information and use it to commit identity theft.

FOLLOW THESE TIPS TO HELP AVOID GETTING “HOOKED” BY A “PHISHERMAN.”

DO NOT:

- Respond to e-mails, mail, telephone solicitations, raffles or contests from unknown entities.
- Answer e-mail warnings that have “undisclosed recipients” in the address line, a blank space next to “Dear,” numerous spelling errors, and/or awkward English.
- E-mail personal or financial information including credit card or bank account numbers, passwords, Social Security numbers, etc. Most Internet e-mail is NOT secure.
- Be fooled by legitimate-looking e-mails even if they contain logos, pictures, copyrights or names of legitimate businesses.
- Reply to e-mails or pop-up messages requesting personal or financial information.
- Click on links in unsolicited messages which can connect to suspicious websites.
- Update personal information online in response to e-mailed requests.
- Cut and paste a link from an unsolicited message into a Web browser, as these links can be made to look like they go to one site, but are actually redirected to another to mine information.
- Respond to calls from alleged companies or government agencies which use a recorded message and ask you to call a phone number to update account information. Phishing can also occur by phone. Using Voice-over Internet Protocol technology, scammers request personal information, and then redirect calls to steal the information provided.

DO:

- Install, update and use anti-virus and anti-spyware software, as well as firewalls to help reduce the number of Phishing e-mails received. Firewalls are especially important with broadband connections as computers are open to the Internet whenever they're turned on. Go to www.onguardonline.gov or www.staysafeonline.org to learn more about how to keep your computer secure.
- Review financial account statements as soon as you receive them to check for unauthorized charges.
- Check credit reports regularly. This can be done free of charge three (3) times a year through the three (3) reporting agencies found online at www.annualcreditreport.com.
- Exercise caution when opening any attachment or downloading any files from e-mails received even from known sources, to avoid the possibility of infecting computers with viruses, malware, spyware or other software designed to impair your computer's security.
- Look for the “https” prefix and a closed padlock when entering any financial information for electronic transmission over the Internet.
- Contact organizations or institutions with whom you do business in response to unsolicited e-mails using their company name by calling the number provided on official company statements.
- Report suspected Phishing scams to spam@uce.gov, to the CPB at www.nysconsumer.gov, and to the institution or company targeted in the Phishing e-mail. You also may report Phishing e-mails to the Anti-Phishing Working Group at reportphishing@antiphishing.org.
- Act immediately if you provided personal identifiable information to unknown or unverified parties by notifying the companies with whom you have the accounts and by placing a security freeze or fraud alert on your files at credit reporting agencies.

