

What is phishing?

Phishing is an online scam used to commit identity theft. A fraudulent, but official-looking e-mail is sent to a user in an attempt to con that user into divulging personal and/or private information, which is then used for identity theft.

How phishing operates

Phishers spam huge numbers of users with a seemingly credible e-mail that instructs the user to visit a Web site (also fraudulent) where they are prompted to enter or update their personal or private information (such as passwords and credit card, social security, and bank account numbers). Phishers also use pop-ups to try and scam users into entering sensitive information.

What actually happens, to the trusting users who submit this information in response to a Phishing attempt, is that identity thieves steal the user's information and their accounts are emptied.

Phishing attempts are extremely sophisticated and it can be extremely difficult to tell if the e-mail or Web site is real. However, no credible organization (like Paypal, your bank, credit card company or social security office) will ever ask you for those kinds of details in an e-mail.

Phishing got its name from the idea that bait is cast out among many fish, some of which actually bite, become hooked and are reeled in.

How do I identify a phishing attempt?

You may have seen a phishing expedition and not have known it. Many people fall prey to e-mail scams for the simple fact that such notifications look legitimate. Phishers will use a trusted company's logo, tag line, and seemingly, similar e-mail address.

There are several things to look out for regarding phishing attempts

Typical phishing e-mails will tell you that your account has come under review, may be in danger of being suspended and/or cancelled, and some piece of information needs to be verified or updated, i.e.: your credit card number, bank account number, social security number, or other personally identifiable data. Look for phishing e-mails with spelling typos, i.e.: "Account Veerification Request", or characters in odd placement: "Requesting : Account : Update"

When you think of phishing, think of fishing. Similar to how anglers use bait to lure fish, online scammers use certain tactics to lure us into giving them our valuable information under false pretenses. Since information is so readily available to everyone via the Internet, recognizing our online weaknesses will help us correct them.

What to do about phishing attempts

Merchants have done a great job of stepping up their customer ID protection services. Most banks and credit card companies utilize state of the art data encryption to protect you while you conduct your business online and most also post anti-fraud messages clearly on their homepages.

What to do if you think you have been a victim of phishing

Government information:

If you believe you've been scammed, file your complaint at <http://www.ftc.gov/>

If you receive spam that is phishing for information, forward it to spam@uce.gov

Be Online Safety Aware

Partnering with your merchants and staying current on scams will strengthen your knowledge and weaken the potential of becoming prey to phishers. Remember, you do not need to become a victim in order to stay informed!

Steps you can take to protect your personal data online and also, what to do if you receive a phishing e-mail:

- Do not reply to any e-mail asking to verify your personal data. You will find that legitimate vendors and merchants do not send such requests via e-mail.
- Contact your merchant right away to ask for clarification of such e-mails. (This will also make them more aware of the range of such problems.)
- Never divulge information, such as passwords and credit card, social security, and bank account numbers, to anyone making contact with you. Only give such information when you initiate a service call, and only do so with trusted sources and where appropriate.
- Use anti-virus software and/or firewalls on every computer you own/use. Remember that children are easy prey to the 'just click here' tactic.
- Stay up to date with current scams and **always report suspicious activity.**

More information on phishing:

<http://www.onguardonline.gov/>