

“PHISHING” SCAMS

When Internet scammers go casting about for people’s financial information, “phishing” (pronounced fishing) is one of the newest ways to lure unsuspecting. Phishing, also called “carding,” is a high-tech scam that uses spam to deceive consumers into disclosing their credit-card numbers, bank-account information, social security numbers, passwords, and other sensitive information.

Here’s how it works: The consumer receives an e-mail that claims to be from businesses the potential victim deals with – such as their Internet service provider, online payment service, or bank. The fraudsters tell the consumer to “update” or “validate” their billing information to keep the account active, and a link directs the consumer to a “look-alike” website of the legitimate business, further tricking the consumer into thinking it is a bona fide request. Unknowingly, consumers submit their financial information – not to the businesses, but to the scammers, who use it to order goods and services and obtain credit. The consumer has just become a victim of identity theft.

Sometimes scammers pose as the IRS. In recent months, some taxpayers have received e-mails that appear to come from the IRS. A typical e-mail notifies a taxpayer of an outstanding refund and urges the taxpayer to click on a hyperlink and visit an official-looking Web site. The Web site then solicits a social security and credit card number. In a variation of this scheme, criminals have used e-mail to announce to unsuspecting taxpayers they are “under audit” and could make things right by divulging selected private financial information. Taxpayers should take note: The IRS **does not** use e-mail to initiate contact with taxpayers about issues related to their accounts. However, if a taxpayer has any doubt whether a contact from the IRS is authentic, the taxpayer should always first call 1-800-829-1040 to confirm it.

To avoid getting caught by these scams, here are some guidelines to follow:

- If you get an e-mail that warns you, with little or no notice, that an account of yours will be shut down unless you reconfirm your billing or other information, **do not** reply or click on the link in the e-mail. Instead, contact the company cited in the e-mail using the telephone number or website address you know to be genuine
- Avoid e-mailing personal and financial information. Before submitting financial information through a website, look for the “lock” icon on the browser’s status bar. It signals that your information is secure during transmission.
- Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- Recent phishing scams cleverly copied the web pages of well-known companies like E-Bay, Pay-Pal, and Credit Unions. Using these authentic looking but fake web pages, the conmen then collected personal information from Internet consumers who thought they were visiting the real E-Bay, Pay-Pal or their Credit Union.
- If you have any doubt about the authenticity of e-mails requesting financial, personal, or other confidential information, OR if you think you have been scammed, please contact the Attorney General’s Consumer Protection Division toll-free at 1-800-472-2600 with your question or concerns.