

Beware of Internet Fraud!

While wading through all the SPAM in your email, have you ever been tempted to respond to an email asking you to “verify your account information?” Identity thieves rely on that momentary twinge of uncertainty to swindle millions of people worldwide with phishing scams.

Phishing is currently the fastest growing form of fraud. This type of scam involves fraudulent emails claiming to originate from financial institutions, government agencies, or other organizations, which ask for the “verification,” “update,” or “confirmation” of personal financial information. Some of these emails even contain Web site graphics and/or corporate logos to make the message seem authentic. The messages usually contain a link to a Web site, where users are asked to input personal financial information such as account numbers, passwords, PINs, Social Security Numbers, or other items.

Legitimate businesses do not send unsolicited emails that ask you for personal financial information. Therefore, treat any unexpected email asking for such information with suspicion. If you receive such an email:

1. Do NOT click on any links provided in the email. If you are unsure of the validity of the email, call the organization that allegedly sent the email. However, do not use a phone number provided in the email. Use a phone number from your personal files, a phone book, or other trusted source.
2. If you believe the email is a phishing scam, forward the email to ***spam@uce.gov*** and to the organization that the email is impersonating. Then delete the email as soon as possible.
3. If you believe you have mistakenly provided personal financial information through a phishing scam, contact the organization who allegedly asked for the information to verify whether the request was legitimate. If it was fraudulent, contact your financial institution immediately. Then contact all three credit bureaus and ask that they place a fraud alert on your credit report (see contact information below). You can also file a complaint at ***www.ftc.gov***, and visit the Federal Trade Commission (FTC) Identity Theft Web site at ***www.consumer.gov.idtheft*** for tips on recovery. Another helpful resource is the Internet Crime Complaint Center at ***www.ic3fbi.gov***.

There are a few basic guidelines that can help you protect yourself from Internet fraud. For example, keep your computer current with security updates from your Internet service provider and/or from your operating system manufacturer (i.e. Microsoft, Macintosh, Linux, etc.). Also, be vigilant in reviewing your credit card, bank account, and other financial statements to verify charges are legitimate. You should also periodically check your credit report for any suspicious activity, such as credit cards or lines of credit opened in your name that you are not aware of.

You can request one free credit report from each of the three major credit bureaus every year: Equifax (800-525-6285); Experian (888-397-3742); and TransUnion (800-680-7289). You can also visit ***www.annualcreditreport.com*** to request your free copies online.