

# FRAUD ALERT: BE AWARE OF PHISHING SCAMS

## WHAT IS PHISHING?

There's a new type of Internet piracy called "phishing." It's pronounced "fishing," and that's exactly what these thieves are doing: "fishing" for your personal financial information. What they want are account numbers, passwords, Social Security numbers, and other confidential information that they can use to loot your checking account or run up bills on your credit cards. In the worst case, you could find yourself a victim of identity theft. With the sensitive information obtained from a successful phishing scam, these thieves can take out loans or obtain credit cards and even driver's licenses in your name. They can do damage to your financial history and personal reputation that can take years to unravel. But if you understand how phishing works and how to protect yourself, you can help stop this crime.



## HOW PHISHING WORKS

In a typical case, you'll receive an email that appears to come from a reputable company that you recognize and do business with, such as your financial institution. In some cases, the email may appear to come from a government agency, including one of the federal financial institution regulatory agencies. The email will probably warn you of a serious problem that requires your immediate attention. It may use phrases, such as "Immediate attention required," or "Please contact us immediately about your account." The email will then encourage you to click on a button to go to the institution's web site. In a phishing scam, you could be redirected to a phony web site that may look exactly like the real thing. Sometimes, in fact, it may be the company's actual web site. In those cases, a pop-up window will quickly appear for the purpose of harvesting your financial information. In either case, you may be asked to update your account information or to provide information for verification purposes: your Social Security number, your account number, your password, or the information you use to verify your identity when speaking to a real financial institution, such as your mother's maiden name or your place of birth. **WARNING:** If you provide the requested information, you may find yourself the victim of identity theft.

## HOW TO PROTECT YOURSELF

- ✔ Never provide your personal information in response to an unsolicited request, whether it is over the phone or over the Internet or even a fax or letter. Emails and Internet pages created by phishers may look exactly like the real thing. They may even have a fake padlock icon that ordinarily is used to denote a secure site. (It is important to keep anti-virus and anti-spam filtering software up-to-date on your computer.) If you did not initiate the communication, you should not provide any information.
- ✔ If you believe the contact may be legitimate, contact the financial institution yourself. You can find phone numbers and web sites on the monthly statements you receive from your financial institution, or you can look the company up in a phone book or on the Internet. The key is that you should be the one to initiate the contact, using contact information that you have verified yourself.
- ✔ Never provide your password over the phone or in response to an unsolicited Internet request. A financial institution would never ask you to verify your account information online. Thieves armed with this information and your account number can help themselves to your savings. (It is a good idea to periodically change your passwords and PIN numbers to improve security.)
- ✔ Review account statements regularly to ensure all charges are correct. If your account statement is late in arriving, call your financial institution to find out why. If your financial institution offers electronic account access, periodically review activity online to catch suspicious activity.
- ✔ Report suspicious emails or calls to the Federal Trade Commission through the Internet at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), or by calling 1-877-IDTHEFT.

*A message from the federal bank, thrift and credit union regulatory agencies  
Board of Governors of the Federal Reserve System  
Federal Deposit Insurance Corporation  
National Credit Union Administration  
Office of the Comptroller of the Currency  
Office of Thrift Supervision*