When Scam Artists Go "Phishing," Don't Take the Bait

How to avoid being lured into giving out personal information

Law enforcement officials use the word "phishing" to describe a type of identity theft by which scammers use fake websites and e-mails to fish for valuable personal information. In the typical phishing scam, you receive an e-mail supposedly from a company, financial institution, or government agency. The e-mail describes a reason you must "verify" or "re-submit" confidential information — such as bank account and credit card numbers, Social Security Numbers, passwords and personal identification numbers (PINs) — using a return e-mail, a form on a linked website, or a pop-up message with the company name and logo.

Perhaps you're told that your bank account information has been lost or stolen or that limits may be imposed on your account unless you provide additional details. If you comply, the thieves hiding behind the seemingly legitimate message can use the information to make unauthorized withdrawals from your bank account, pay for online purchases using your credit card, or sell your personal information to other thieves.

Never provide your personal information in response to an unsolicited call, fax, letter, e-mail, or internet ad. If you did not initiate the communication, do not give this information, regardless of how legitimate or genuine these entities may appear to be. Some fraudulent, copycat sites deliberately use URLs that are very similar to, but not the same as, those for well-known companies or government agencies. When contacting your bank, use the phone number or web address listed on your monthly statements.

If you believe you're already a victim of ID theft immediately contact your financial institution and, if necessary, close existing accounts and open new ones. Also contact the police and request a copy of any police report or case number for later reference. In addition, call the three major credit bureaus (Equifax at 800-525-6285, Experian at 888-397-3742 and TransUnion at 800-680-7289) to request that a fraud alert be placed on your credit report.