Learn about . . .

Online Fraud Detection and Recovery Steps

Online Fraud Is Growing

Internet fraud can be any type of scheme that uses the Internet – chat rooms, email, message boards or websites – to deceive prospective victims. These schemes, scams and frauds take advantage of the Internet's unique capabilities – sending email messages worldwide in seconds or posting website information that is readily accessible from anywhere in the world – to carry out fraud quicker than ever possible in the past. As a bank customer, you need to be especially vigilant to some of the newer frauds at work in cyberspace.

Phishing

Fraudulent emails, appearing to be from a trusted source such as your bank or a government agency, direct you to websites. Once there, you are asked to verify personal information such as a name, account and credit card numbers and passwords. These sites are often designed to look exactly like the site they are imitating.

Cyber-Defense Tactics

If you receive an email that warns you, with little or no notice, that your account will be shut down unless you reconfirm certain information, do not click on that email link. Instead, use a phone number or enter the web address yourself. Clicking on that link that looks legitimate may in fact direct you to a fraudulent website where crooks will steal your personal information. Remember, your bank or a government agency will never send you an alert asking you to disclose your personal information.

Before submitting any financial information to a legitimate website, look for the "lock" icon on the browser status bar, or look for "https" in the web address. Both are indications that the information is secure and encrypted during transmission.

Spoofing or Pharming

Web spoofing allows an attacker to create a "shadow copy" of any legitimate website. The spoofed site looks very much like the legitimate site. Access to the shadow web is funneled through the attacker's machine, allowing the attacker to monitor all of the victim's activities, including any passwords or account numbers the victim enters.

Cyber-Defense Tactics

If any part of the web site looks suspicious or unprofessional (misspelled words, poor grammar, sloppy logo), report it to the company you are visiting on the web site and confirm.

Identity Theft Frauds

Internet fraudsters often use identity theft as a starting point for larger crimes. In one case, criminals obtained the names and Social Security numbers of military personnel and then used them to apply to a bank over the Internet for credit cards. In another case, stolen personal data was used to submit car loan applications online.

Cyber-Defense Tactics

Keep a close eye on your account activity at your bank, either through statements or using their online services. Report anything that looks suspicious.

Your personal information can be obtained by “phishing,” “spoofing,” or the old fashioned way: dumpster diving. Make sure your unused checks, bills, and statements are shredded before discarding.

Malware

This is software designed to infiltrate or damage a computer system without the owner’s knowledge or consent. It is a blend of the word “malicious” and “software.” It includes computer viruses, worms, trojan horses, spyware, adware, and other malicious and unwanted software.

Cyber-Defense Tactics

You can purchase and install on your PC anti-malware and anti-virus software protection.

More Best Practices

Don’t Judge By Initial Appearances. Just because something appears on the Internet doesn’t mean it’s real. The ready availability of software that allows anyone, at minimal cost, to set up a professional-looking website means that criminals can make their websites look as impressive as those of legitimate businesses, banks or government agencies.

Be Careful About Giving Out Personal Data Online. If you receive emails from someone you don’t know asking for personal data, then don’t send the data without knowing more about who is asking. While secure transactions with known e-commerce sites should be safe, especially if you use a credit card, non-secure messages to both known and unknown recipients are not safe.

Be Especially Wary Of Emails Concealing Their True Identity. If someone sends you an email using a mail header that has no useful identifying data (e.g., W6T7S8@provider.com), that may be an indication that the person is hiding something and is not legitimate.

Review Credit Card and Account Statements as soon as you receive them to determine whether there are any unauthorized charges or suspicious charges/transactions. If your statement is late by more than a few days, call your credit card company or bank to confirm your billing address/account balances, and determine whether they have mailed your statement. If something seems irregular, contact your company to discuss it. An encouraging note: a recent study showed that customers who monitor their accounts online discover any problems sooner.

Check your credit report at least annually. You are entitled to one free credit report annually from each of the three major credit bureaus. If a hijacker is misusing your credit, clues are likely to show up here. For a free report www.annualcreditreport.com

Watch Out For “Advance-Fee” Demands. Look carefully at any online seller of goods or services that wants you to send checks or money orders immediately to a post office box before you receive the goods or services you’ve been promised.

Use Common Sense.

Filing Complaints: Resources

Contact any of these, as appropriate, to file complaints:

Federal Trade Commission (FTC) Consumer Response Center | www.ftc.gov
You can file a complaint with FTC against a company or organization that you believe has cheated you by contacting the Consumer Response Center by phone: toll free 877-FTC-HELP (382-4357).

Department of Justice, Consumer Fraud Division | www.usdoj.gov
"Fraud" is a link on this site under "Information for Individuals and Communities."

FirstGov (Your First Click to the U.S. Government) | www.firstgov.gov
"FirstGov" is a free-access website designed to give a centralized place to find information from local, state and U.S. Government Agency websites. Consumers may call toll free 1-800-333-4636.

Consumer.gov | www.consumer.gov
A "one-step" link to a broad range of federal information resources available online.

Social Security Administration | www.ssa.gov
Report Social Security fraud by calling 1-800-269-0271.

Identity Theft Resource Center | www.idtheftcenter.org
Call 858-693-7935.

Source: America's Community Bankers