Gone Phishing

As the holidays approach and more people are using the Internet to do their shopping and to pay bills, it’s a good idea to become familiar with a growing problem called “phishing.”

Phishing is a term used to describe the action of assuming the identity of a legitimate organization, or Web site, using forged e-mail or Web pages to convince consumers to share their user names, passwords, and personal financial information for the purpose of using it to commit fraud.

Phishing has quickly grown into one of the most frequent and effective scams on the Internet. It works by directing users toward fake Web sites that trick them into giving up personal information. This procedure has included account verification, invalid credit/debit card details, attempted account hacking, prize draws, and account suspension. Some victims have had their credit rating and financial livelihood destroyed when their identity has been used to raise capital, while others have seen their credit or debit cards used by imposters to buy goods online.

Experts recommend consumers protect themselves from phishing scams by entering Web site addresses into their browser (rather than clicking on provided links) and only calling numbers listed in the phone book or on bank-provided credit cards or statements.

You can avoid becoming a phishing scam victim by following these simple rules and watching for these signs:

- Treat all e-mail with suspicion. What you see in the e-mail body can be forged, the sender's address or return address can be forged, and the e-mail header can also be manipulated to disguise its true origin.
- Never use a link in an e-mail to get to any Web page. If you must go there, type the URL directly into your browser's address bar.
- Never send personal or financial information to any one via e-mail.
- Regularly log into your online accounts — check each one at least every three weeks.
- Scrutinize your bank, credit, and debit card statements and ensure that all transactions are legitimate. If anything looks suspicious, contact your bank and credit card issuers.
- Ensure that all of your software is up to date. For instance, if you use Microsoft Windows, run Windows Update every day when you first connect to the Internet. If you use other operating systems or browsers, then check daily for patches or updates. Security loop holes are regularly discovered in software.

One big problem is that phishing e-mails look so official and real — they're slick and well-designed, using official-sounding language and real company logos to make them look and feel authentic.

They appear to be from trusted banks, retailers, or other companies. The e-mail often says the company needs to verify your information, such as account numbers or passwords, for supposed security purposes.

They try to fool you with an address "spoof." In more than 90 percent of cases, the e-mail address looks like one from a real company. Although the address in the “From” line of the e-mail may contain a legitimate address, it conceals a scammer's address.

Here are some questions to help you recognize Phishing e-mails and sites:
- What is the tone of the e-mail?
- Does the e-mail convey a sense of urgency?
- What is the quality of the e-mail? Does it have misspellings and bad grammar? Is it fuzzy?
- Are the links in the e-mail valid?
- Is the e-mail personalized with your name and applicable account information instead of a generic greeting?
- Who is the e-mail from and does the e-mail address match the company represented?
- Does it ask you to fill out forms with your personal financial information?
- Does it point to links in the e-mail, urging you to click to "validate" or "confirm" your account?

Unfortunately, no matter how careful you are, you sometimes still end up falling prey to someone who has scammed you. So, here are a few important tips if you’ve divulged sensitive information:
- If you think you’ve been scammed, you can file a complaint with the Federal Trade Commission and the Internet Fraud Complaint Center. But, most importantly, the first thing you should do is to notify the bank or credit card issuer of the account that has been compromised. You’ll probably want to close the account and open a new one.
- If you’ve given away your Social Security number, you should also notify the big three credit reporting agencies — Experian, Equifax, and TransUnion — so that a fraud alert can be placed on your file. That way, if anyone applies for new accounts with your Social Security number, you can be notified at home. You should also always regularly monitor your credit reports, if you do not already.

Don’t let phishing ruin your holiday shopping plans. Be sure to take the appropriate safeguards so that the “Grinches” of the world don’t steal your Christmas out from under you.

AAA offers an array of financial products and services with exclusive rates and benefits designed especially for members to help you with those added expenses that arise during the holidays. They include credit cards, auto loans, certificates of deposit, money market and individual retirement accounts, and unsecured lines of credit. Visit www.AAA.com for current rates and detailed information.