**Phishing: Avoid Getting Hooked by Cybercriminals**

"Phishing" refers to hooking people online through deceptive emails and websites that ask for private information -- usually financial passwords or account numbers. These emails and phony sites can appear very authentic. Unless you follow the proper precautions, it can be very difficult to tell what is safe and what isn't. Follow these helpful tips to avoid the phishing hook:

**1. Don't follow links asking for information.**
Phishing emails are stuffing inboxes everywhere. Some telltale signs to look for include vague salutations like "Dear Account Holder," along with a dire warning to "take action immediately." They also typically arrive proclaiming they hail from your financial institution. Maybe they'll ask you to resubmit or confirm your password or perhaps your account number.

But no matter how authentic the email may appear, do not respond. Instead of following a link in an email or an online advertisement, type the address of your bank or financial institution directly into the address line of your browser. (It is still safe to bank and shop online, you just need to make certain the site you are banking on is actually your bank and not a decoy). If you have a problem logging into your account, call your bank or credit card company first to find out if there are any issues with your account -- and ask for a password reset. The point is, there is no reason for a bank to email you to ask for your account information. After all, they already have it. Why wouldn't the company just call you?

**2. Be suspicious of hidden URLs.**
If an email prompts you to click on a link, be aware that the URL may be different from what you think it is. Therein lies the potential for a con.

Some links can be shortened using sites that reduce long URLs (aka Uniform Resource Locators -- the "www." address you use to visit Internet sites) into shorter, more manageable ones. It's a helpful, legitimate service but one that the bad guys can use to obscure a link's true location. Other URLs might appear legitimate, but a subtle character change or space is all it takes to lead you to a phishing site. Be aware. Never reply to an email with your financial or personal information.

**3. Change your passwords periodically.**
Memorizing passwords can be annoying. But it's a vital part to remaining secure online. Far too many of us rely on easy-to-guess passwords and stick with them for years. Drop this bad habit ASAP. Create passwords that use letters and numbers with both upper- and lower-case characters thrown into the mix.

Think you'll never be able to remember them? A good, secure password management system can help alleviate the pain, keeping track of all of your logins and shielding them from prying eyes. Remember: The greater the complexity, the stronger the security -- something especially important for financial sites.

**4. Check your financial accounts regularly.**
Reading your monthly statements may not top curling up with the latest best-seller, but a few minutes here can avoid hours of headaches later.

Check for suspicious charges or debits, and if you spot any, inquire about them immediately. Often, these charges turn out to be benign, like a purchased placed by your spouse or a forgotten transaction. But if they aren't, you need to alert your bank or credit card company right away.

Cybercriminals are relying on people being complacent. Don't fall into their trap. If your information has been stolen, the sooner you report it, the better. Go to the Federal Trade Commission's Identity Theft Web site for more information on how to do this.