Protect Your Identity! Beware of Phishing!

What is Phishing?
There's a new type of internet piracy called “phishing”. It's pronounced “fishing”, and that's exactly what they're doing: “fishing” for your personal 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.

Here's 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 e-mail may appear to come from a government agency, even one of the federal financial institution regulatory agencies.

The e-mail 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 e-mail will then encourage you to click on a button to go to the institution's website.

In a phishing scam, you could be redirected to a phony website that may look exactly like the real thing. Sometimes, in fact, it may be the company's actual website. 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.

How to Protect Yourself:
•Never provide personal financial information, including your Social Security number, account numbers or passwords, over the phone or Internet if you did not initiate the contact.
•Never click on the link provided in an email you believe is fraudulent. It may contain a virus that can contaminate your computer.
•Do not be intimidated by an e-mail or caller who suggests dire consequences if you do not immediately provide or verify financial information.
•If you believe the contact is legitimate, go the company's website by typing in the site address directly or using a page you have previously bookmarked, instead of a link provided in the e-mail.
•If you fall victim to an attack, act immediately to protect yourself. Alert your financial institution. Place fraud alerts on your credit files. Monitor your credit files and account statements closely.
•Report suspicious e-mails or websites to the US Government Computer Emergency Readiness Team through the internet at **http://www.us-cert.gov/nav/report_phishing.html**
•For more information or to report identity theft, contact the Federal Trade Commission at **http://www.ftc.gov/bcp/edu/microsites/idtheft/** or call 1-877-IDTHEFT.