



05/21/2007

Avoid 'Phishing' Credit Scams

Because your credit information is used so regularly in your business and financial ventures, for everything from getting approved for a mortgage loan to being hired for that new job position, protecting your credit from scams and theft is essential. These scams come in all shapes and sizes, but one you should acquaint yourself with is the 'free credit report' offer that falls within the genre of 'phishing.'

According to the nation's consumer protection agency, the Federal Trade Commission (FTC), phishing is "a high-tech scam that uses spam or fraudulent Web sites to deceive consumers into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, and other sensitive information." One way scammers use phishing to steal and use your credit information is by creating deceptive emails offering consumers a copy of their credit report, often promising it for free. Some people get sucked into these advertisements and give out all sorts of personal information on unsecured websites. The scammers may or may not actually furnish you with the promised credit report, but they will definitely steal your personal information in order to commit identity fraud, or they may sell your information to others who will use it for the same purpose.

In order to spot the difference between a legitimate company and credit report offer and a fraudulent one you should keep a few tips in mind. First, simply be on your guard if you receive unsolicited email from a company offering you a copy of your credit report. It is probably safer to do your own search for a helpful company than to trust fliers coming into your box uninvited. Beware of advertisements that come from odd-looking emails addresses or have strange suffixes like .ru or .de rather than from a .com or a .net.

If you do receive an email in your box that looks legitimate, instead of clicking on any of the links within the email, try finding a phone number you can call or a company website address you can visit. You should also find out if the company has a valid street address or if the one listed is simply some made-up address. Taking these measures will help you find out if this offer is the 'real deal.'

You might also be able to spot a shady offer by looking for misspellings and grammatical errors. If the email was shoddily put together, there is a good chance it is not from a reputable company.

Steer clear of any email offers that require highly sensitive information, like your passport number or debit card pin number. According to the FTC's website, "legitimate sites don't ask for this information." The FTC also counsels consumers to look for secure sites, ones that have "https" in the URL line. This will insure that your information will be protected.

And of course, don't forget that you can completely avoid credit report scam operations by simply pulling your credit report yourself from any of the three major credit reporting bureaus: Experian, Equifax, or TransUnion. You can even request a copy for free from each bureau once a year. (You will have to pay to find out your credit score though.) The bottom line is to play it safe when it comes to protecting your credit information!