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.