The Smishing Attack: The mobile phone version of an email phishing scam, "smishing" (SMS phishing) occurs when an attacker contacts you by text to acquire financial information or other personal data by posing as a trustworthy entity such as your financial institution. In many cases, they'll tell you that there is a problem with your account in order to get you to reveal sensitive banking details such as your account number, password or PIN. For example, you might be asked to provide certain details in order to unlock your account or told to call their fraud prevention hotline, which will of course be answered by the fraudster. These texts may also prompt you to click on a link to a fraudulent website. As with your email, don't assume that a text message is authentic, and be aware that financial institutions like credit unions and banks will never ask you to reveal security details such as your PIN or password over the phone or via text. Even if a caller is appearing to be calling you from a legitimate number, keep in mind that it could be spoofed. To check the status of your account and any possible fraudulent activity, call the number on the back of your card right away. You should also check online for unauthorized transactions, but be sure to type the web address of your financial institution directly into your browser.

Quick Tips for Reducing Unwanted Calls and Dealing with Phone Scams

Of course, one of the best ways to fend off phone scams and unwanted phone solicitations is simply not to answer calls from numbers that you don't recognize. But again, remember that it's easy for scammers to fake a phone number. If you answer the phone and the caller seems suspicious, just say, "No thanks," and hang up right away. It's also a good idea to report your experience online to the Federal Trade Commission (FTC) or by calling their Consumer Response Center at 1.877.382.4357. This won't take long, and it can help authorities collect evidence against perpetrators. In addition, you may want to consider listing your home and cell phone number on the FTC's Do Not Call Registry at www.donotcall.gov or by calling 1.888.382.1222. Mobile apps such as Nomorobo, TrapCall and Hiya are also helpful tools for identifying robocalls and fraudulent callers. Looking for more pointers on fighting phone fraud? Visit http://bit.ly/ConsumerInformationPhoneScamsFTC.