Keeping Your Money Safe: Smishing

Ashlie Hagemann, Fraud Supervisor

Businesses and individuals lose billions of dollars every year due to fraud. While PlainsCapital Bank has a seasoned fraud prevention team in place to protect our customers, we understand that the best protection is education. To that end, our Fraud Prevention Series, "Keeping Your Money Safe," highlights the latest fraud scams with helpful tips on how you can avoid them.

As technology continues to become intertwined in our daily lives, cyber criminals are finding new ways to attempt to defraud you. One relatively new method they employ is known as smishing. According to Norton, this form of phishing is when someone tries to deceive you into giving them your private information via a text or SMS message. Following is information on how smishing works, and more importantly, how you protect yourself from being the victim of one.

How Does the Scam Work?

Smishing, though it might sound like a weird term, is simply a combination of the "s" in SMS (the standard format for text messages) and phishing. As in other phishing attacks, the criminals impersonate anyone from government workers and tech support representatives, to family and friends or financial institutions. Their goal is to try to lure people into divulging personal details that could lead to fraudulent credit card purchases, identity theft, or opening new credit cards in your name.

For example, you may get a text from an unknown number claiming to be your bank or the IRS and claiming you are due a refund because of some undisclosed error. Within the text is a link you are instructed to click to process the transaction. If you do, the cyber criminal may have access to a host your personal and confidential information.

How to Protect Yourself from Smishing Scams

1. Don't reply to a text from someone you don't know. Smishing text messages may go so far as to use your name. While they often come from unfamiliar numbers, sometimes they may seem to have originated from a phone number you recognize.

2. Beware of messages that claim to be from government agencies, such as the IRS or Social Security Administration. These agencies will never send you an unsolicited text message or initiate contact via text message, email, or social media.

3. Beware of requests with a sense of urgency. These types of scams often imply that an immediate response is required to take advantage of an offer or to avoid a penalty.

4. Never click embedded links from suspicious text messages. They can contain malicious code that could infect your mobile phone.

5. Make sure your phone's operating system is up to date. Android and iOS are constantly being updated with enhanced security features. On

Androids and iPhones, your phone's settings page should indicate what system you're using and whether an update is available.

Keeping Your Money Safe

As always, the "Keeping Your Money Safe" fraud prevention series is designed to help you thwart cyber criminals trying to acquire your personal information or infiltrate your devices. The key to protecting yourself is education and awareness. PlainsCapital Bank's Fraud Department provides educational resources for businesses and customers to help detect and prevent fraud on their accounts. For more information about our fraud prevention efforts, visit our fraud resources page.