Keeping Your Money Safe: Phone Spoofing

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.

Thieves and cyber criminals have many tools at their disposal when it comes to stealing your personally identifiable information. One such tool is phone spoofing, which occurs when a scammer transmits incorrect caller ID information to your phone to make it look like the call is coming from a trustworthy source, such as your bank or a government agency like the IRS.

How Does the Scam Work?

By manipulating caller ID information, the perpetrator is able make your phone display a number different from the actual originating number. They can send outgoing or incoming phone calls or texts that appear to be from any phone number. Typically, the fraudster will attempt to impersonate law enforcement personnel, utility companies, your bank, or even the IRS.

In any case, scammers that employ phone spoofing are trying to trick you into releasing private and confidential information, such as your bank account number, Social Security number, mother's maiden name, or credit card details. They do this by pretending they need your information to head off anything from a discontinuation of services or legal prosecution to loss of funds.

How to Prevent a Phone Spoofing Scam

The good news is that you can thwart phone-spoofing attempts easily if you know what to look for. Here are a few tactics to consider:

1. Don't give out personal information just because the caller asks for it. Many fraudsters will attempt to sound casual when asking for your information, as if they're just doing their job. Legitimate companies and organizations will not contact you over the phone for this type of personal information. They may ask for your name, date of birth, and perhaps even the last four digits of your Social Security number to identify you, but they won't ever ask for full confidential details.

2. If the call is from a company you know but it seems suspicious, tell the caller you'll get back to them and hang up. After hanging up, call the company back using a phone number found from a trusted source, such as their secure website or your bank statement.

3. Reverse-lookup the number they're using. A simple Google search can sometimes give you specific information for the number a malicious caller is spoofing. Just type in the exact number that appeared on your phone's caller ID to see if there is any history of scamming associated

with the number.

Keeping Your Money Safe

Unfortunately, fraudsters commonly use the phone numbers of financial institutions like banks, credit unions, and financial services firms to trick unsuspecting customers into providing them with crucial account information. While financial institutions monitor fraud reports regularly act quickly to notify their customers, it's nearly impossible to identify unreported phone spoofing attempts.

Keep in mind that PlainsCapital Bank will NEVER ask for your user name, passwords, account number, debit card number, PINs, or security/pass codes through unsolicited emails, texts, pop-up windows and in this case, phone calls. If we contact you about fraud on your account, we will only ask for limited account information for verification purposes to ensure we are speaking to the correct person. If you are ever suspicious about an inbound phone call, hang up and call PlainsCapital customer service at 866.762.8392.

The scammers behind phone spoofing can be extremely convincing. The best defense against falling prey is to stay alert, trust your instincts, and educate yourself about common fraud tactics. 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.