How to Stop Scammers Who Sound Just Like Your Bank

If you ever get a call from someone claiming to be a customer service agent at your bank, pump the brakes before answering any questions — even if they have the right caller ID. Using "caller ID spoofing," scammers can make it look like they're calling from your bank's phone number.

Here's the tipoff that it might be a scam: Banks typically don't call you asking for personal information.

How to shut down a scam before it starts

One of the easiest ways to spot a scammer is that they reach out to you versus you contacting them, says Richard Crone, a payments expert and CEO of Crone Consulting, LLC.

"The best way to protect yourself is to say, 'No worries, let me call you right back,' and then you call the official bank number yourself," Crone said. "Never answer any questions from a random call from anybody. There may be a call from someone legitimate, but more often than not, it's nefarious."

A legitimate representative from your bank will never take issue with you hanging up and calling the number on the back of your debit or credit card.

Crone says you can be even more secure by refusing to answer the call, text or direct message in the first place.

If you run into a case of caller ID spoofing, report the activity to the Federal Communications Commission. "Once a scammer makes contact, they can distribute and sell your number in the criminal underworld," Crone said.

When something doesn't feel right

In one recent case, a number that appeared to be Wells Fargo called a customer, Cabel Sasser, and the "customer service agent" told him that his account had been compromised. Sasser, an entrepreneur from Portland, Oregon, was told that he needed to replace his card and change his debit card PIN by typing the old one into his phone's keypad. The "agent" had several accurate details from Sasser's account, including the last four numbers of his Social Security number, but something didn't feel right, he told USA TODAY.

Sasser said that he hung up and called the official Wells Fargo customer service number on the back of his card. It turned out his card hadn't been compromised. As Sasser recounted the story on Twitter, he said, "I was just four key presses away from having all of my cash drained by someone at an ATM."

Keep your banking information safe

So, if phone calls and texts seemingly from your bank are suspicious, how can you know if your bank account has been compromised? Here are a few tips:

Use your mobile bank app. "The best way for banks to reach out is through their official mobile app," Crone said. "Apps have multiple authentication systems, logins and biometrics like Touch ID or face recognition. That's your safety deposit box for interactions with your bank. It's the safest way to communicate; you can be assured that it's them, and they can be assured that it's you."

Set alerts for unauthorized account usage. When you enroll in your bank's account alert system, you'll be notified whenever a fishy transaction is made. Many banks also allow you to "freeze" the card so that it can't be used unless you "unfreeze" it through the app or online.

Keep a password lock on your phone and on your banking app. If you lose your phone, multiple passwords will help keep your information safe in case the phone is unlocked.

Don't use public Wi-Fi to check your bank accounts. Public Wi-Fi networks are more vulnerable to security risks, so use only a secure Wi-Fi connection to look at your bank accounts. If you must look at your accounts in public, your phone's internet connection via cellular data is more secure than a public Wi-Fi network.

Beware of "shoulder surfers." If you use only passwords — as opposed to biometrics — to keep your phone secure, make sure no one nearby is snooping over your shoulder to watch you enter your phone or banking app passwords. If that person steals your phone, they'll have easy access to your money.

Change passwords frequently. How frequently? "As often as you can endure it," Crone said. A strong password is complex, hard to guess and easy to remember. Consider making your passwords phrase-based — like a full sentence — and avoid using real words that can be found in a dictionary. Make it a combination of numbers, letters and symbols. If it gets difficult to keep track of, a password manager can help you maintain a record of your passwords across different sites and logins.

As scammers become more advanced, good security practices and vigilance are more important than ever for keeping your money safe. So rethink answering that call from your "bank," and get well-acquainted with your mobile app.

Chanelle Bessette is a writer at NerdWallet. Email: cbessette@nerdwallet.com.

The article How to Stop Scammers Who Sound Just Like Your Bank originally appeared on NerdWallet.