# New Phone, Who’s This? Oh, A Scam!

**Image:** Included in toolkit.

**Suggested Alt Text:** Communications on a fishing hook.

Cybercriminals are often anonymous individuals deploying large-scale [**phishing**](https://digital.va.gov/articles/hook-line-and-sinker-how-to-up-your-phishing-game/)attacks across the web. While this is often the case, you may receive a call from them appearing to be from your local bank.

Vishing is a phone scam where a caller will try to convince you to divulge personal information through a voice message or live call. The Federal Trade Commission (FTC) found that 2.2 million Americans reported fraud in 2020, with the phone being the top threat. Scammers may call to inform you one of your accounts was compromised, offer an investment opportunity, or claim to be from a federal agency. Vishing attacks are becoming more advanced as scammers [**spoof phone numbers**](https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing) to appear as if they are local to their targets, and they may already have some pieces of your personal information.

Despite efforts to hide their intentions, there are some actions you can take to protect yourself from vishing.

* If you receive a call from **someone claiming to be from a federal agency** and they are requesting your personal information, you are talking to a scammer. Federal agencies will not contact you unless you make a request.
* Add your number to the [**National Do Not Call Registry**](https://www.donotcall.gov/). Companies contacting numbers registered on the Do Not Call list can face civil enforcement from the FTC.
* **Ignore the phone call** if you do not recognize the number. If a voicemail is left, you can do your research and determine whether to call the individual back.
* **Reject any prompts** given during a robocall. If you interact with the robocall, scammers might use your voice for automated phone prompts in the future.

As soon as you suspect a Vishing attack may have successfully targeted you, it is critical to take immediate actions to protect yourself. For example, you should immediately [**put a freeze on your credit report**](https://www.usa.gov/credit-reports#item-214215)if any new accounts have been opened in your name. You should also contact your financial institutions to determine if any other fraudulent activity has occurred.