

How to Protect Yourself from Scams



Tips to Protect from Phishing & Scams

Many scams start with an intimidating phone call. A “*debt collector*” needs you to pay immediately or a “*police officer*” claims to have a warrant for your arrest. The latest variation involves a phony process server & a non-existent court case against you. The Better Business Bureau (BBB) Scam Tracker has gotten numerous reports of this new twist.

How to Avoid Phishing Scams

- **Be wary of scare tactics.** Scammers love to threaten people with legal action or hefty fines, scaring them into giving up their personal information. They hope fear will make you act without thinking.
- **Search your local court website.** If you think there’s a chance someone has filed a lawsuit against you, check your local court’s website. Search your name to see if any lawsuit has been filed. If nothing comes up, you’re in the clear.
- **The scammer may have some personal information. Don’t give them more!** Scammers may have some of your personal information already from a previous phishing scam, a data breach, or some other source. They may use these stolen details to get even more information from you.



Examples of Imposter Scams

1. Power / Utility
2. IRS Imposters
3. Emergency Scams
4. Favor for a "Friend"
5. Tech Support Scams
6. Better Business Bureau (BBB)
7. Phony Banking Texts / Phishing Schemes



How the Scam Works:

- 1 First, you receive a call from an unknown or blocked number from a person claiming to be a process server. They might say there is a lien on your home or someone is taking you to court over unpaid medical bills. In other cases, the scammer may be secretive, saying they can’t reveal details until your papers are served.
- 2 Next, they’ll ask you to “confirm” sensitive personal information, such as your date of birth and Social Security number. When you’re hesitant to give out this information, they stress the urgency of the matter – after all, you’re being taken to court! If you ask too many questions about who is making a complaint or what company the process server works for, the scammer will get angry. Sometimes, the caller may be phishing for information about your family members.
 - **Example Experience:** “I received a call from some lady who stated that my phone number was provided to them by my mother, and they wanted me to verify her Social Security number and date of birth. I refused and asked her what the phone call was about. She stated that there was a lawsuit pending against my mother, but she declined to state who the complainant was and said there would be a process server coming through to serve papers. They refused to provide my mother with any information regarding a lawsuit against her. We waited for a process server, and of course, none showed up.”

FOR MORE INFORMATION:

Reading up on **phishing & impostor scams** can help you spot a con before it’s too late. You may also visit **BBB’s Spot a Scam page** for tips on recognizing scam tactics. If a scammer contacts you, report your experience to **[BBB.org/ScamTracker](https://www.bbb.org/ScamTracker)**. Your report can help us boost awareness & make scammers’ tactics less effective.



The people behind these scams don’t have any legal papers to deliver, they want to get their hands on your personal information to commit identity theft.