

## Tech Support

Scammers use pop-ups, warning messages, or unsolicited contact to get your attention and steal money and / or personal info. They say there's something wrong with your device or that your financial accounts have been hacked or are about to be hacked – and they can fix it.

Ruth receives a call from someone pretending to be tech support from a legit company. “We found a problem with your computer. To fix it we need to download special software; we need your password.” Later that day Ruth found someone had accessed all her online bank accounts.

Jimmy clicks on an ad that offers free tech support. He's redirected to a page that asks for his password. A few days later he finds someone has changed his social media accounts, asking his contacts for money.

Bruce is doing his taxes online when a popup warns him of suspicious activity on his computer. He calls the number. “We can fix your computer right away, but we need your password for remote access.” A few minutes later Bruce gets notifications of bank transactions he knows nothing about.

Posing as tech support companies, scammers may bring in others to pose as bank or government officials or officials from other legitimate organizations. They say you need to protect your device and encourage you to sign up for a fake subscription – to install software to protect yourself.

## WARNING SIGNS FOR TECH SUPPORT SCAMS

- Unsolicited pop-ups or calls.
- Requests for remote access, passwords.
- Claims of expired software, illegal content, or other problems.
- Urgency and threats.
- Unusual, hard-to-trace payment methods.

## IF YOU SUSPECT A SCAM ...

- PAUSE. Do NOT click on a link. Do NOT call numbers on warning messages.
- VERIFY. Check the official website for tech support. Try a 'google search' to see if others have had this experience with scammers.
- Ignore unsolicited messages and popups.
- Do NOT allow them to access your device or install software.
- Do NOT share any personal info. E.g. passwords, financial info, etc.