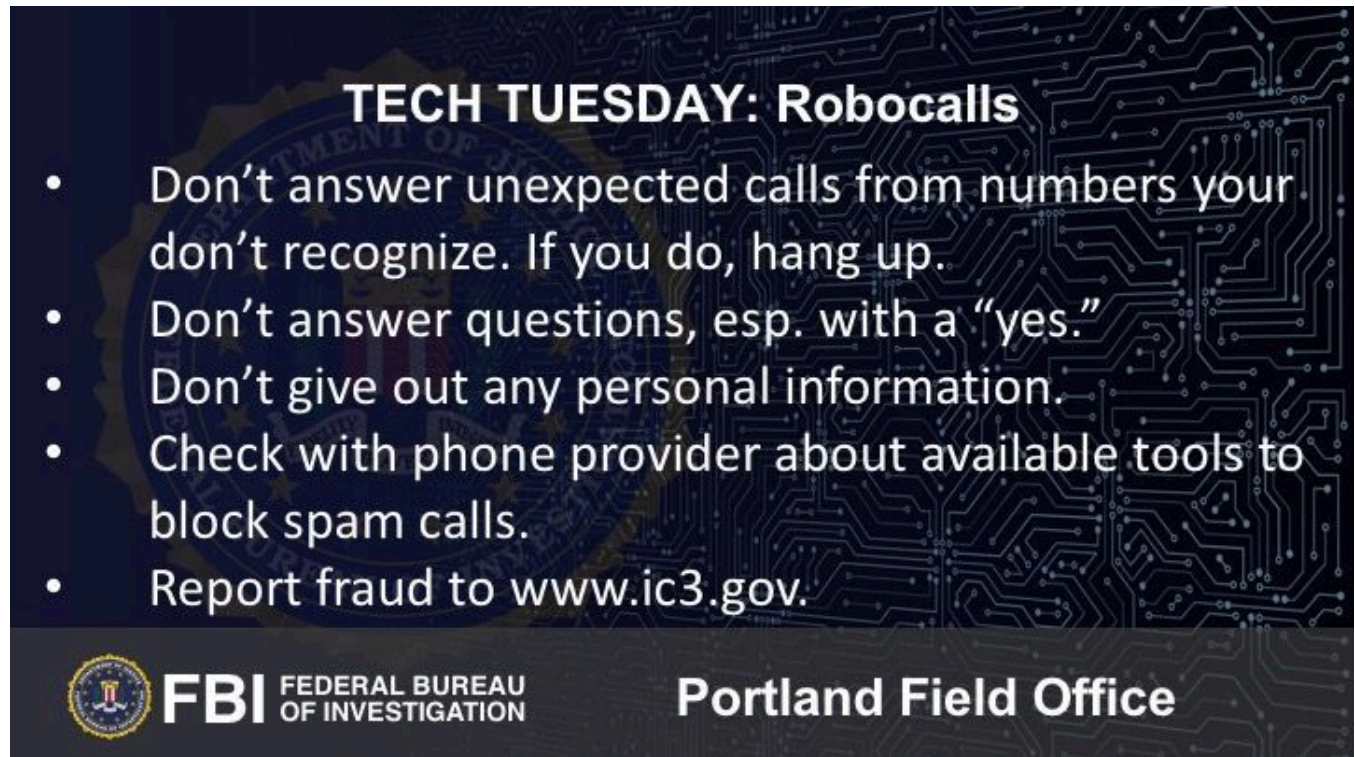


Tech Tuesday: Building a digital defense against robo text and email scams

May 11, 2021

An infographic titled "TECH TUESDAY: Robocalls" with a background of circuitry and a faint FBI seal. It lists five bullet points: "Don't answer unexpected calls from numbers you don't recognize. If you do, hang up.", "Don't answer questions, esp. with a 'yes.'", "Don't give out any personal information.", "Check with phone provider about available tools to block spam calls.", and "Report fraud to www.ic3.gov." At the bottom, it features the FBI logo and the text "FBI FEDERAL BUREAU OF INVESTIGATION" and "Portland Field Office".

TECH TUESDAY: Robocalls

- Don't answer unexpected calls from numbers you don't recognize. If you do, hang up.
- Don't answer questions, esp. with a "yes."
- Don't give out any personal information.
- Check with phone provider about available tools to block spam calls.
- Report fraud to www.ic3.gov.

 **FBI** FEDERAL BUREAU OF INVESTIGATION

Portland Field Office

This week, we have some information from our partners at the Federal Trade Commission about robo text and email scams.

We are not talking about messages you get from a company or agency when you signed up to receive those – things like newsletters or coupons. Subscribe and unsubscribe to those as you wish. We are talking about unsolicited messages from unknown people or groups who are either trying to download malware onto your device or trying to get you to give up personal info.

You think you're doing the right thing to stop the harassment by clicking "unsubscribe." Don't do it! By clicking "unsubscribe" links or texting "stop" in reply, the spammers literally take that to mean "subscribe" and "please, go on."

As these spammers blast out millions of texts or emails every day, they aren't actually targeting you specifically — in fact, they might not know if your email or phone number is even valid. They are looking

for signs of an active account. By hitting “unsubscribe” or replying in any way, you validate your contact information and risk inviting even more spam and scams.

There are various ways to mark messages as spam, depending on your type of device and service provider. You can also forward messages to the FTC directly. (More info on how to do that can be found here: <https://www.consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages>)

At the very least, if you get a suspicious email, mark it as spam and delete it without opening it. If you get a suspicious text, delete without replying and block that number on your phone.

According to the FTC, here’s how to avoid those spam texts and emails in the first place:

Avoid displaying your email address in public. Spammers scrape blog posts, chat rooms, social networking sites, and forums — so the less of you that’s out there, the better.

Use two email addresses — one for personal messages and one for everything else. Ideally, this second public-facing email address should be one you are willing to delete one day, if needed.

Use a truly original address that’s unlikely to be created by spammers. Spammers send out millions of messages to probable name combinations hoping to find a valid address. That means common first name/last name email addresses are more likely to attract spam.

If you believe are a victim of an online scam, you should report the incident to the FBI’s Internet Crime Complaint Center at www.ic3.gov or call your FBI local office.