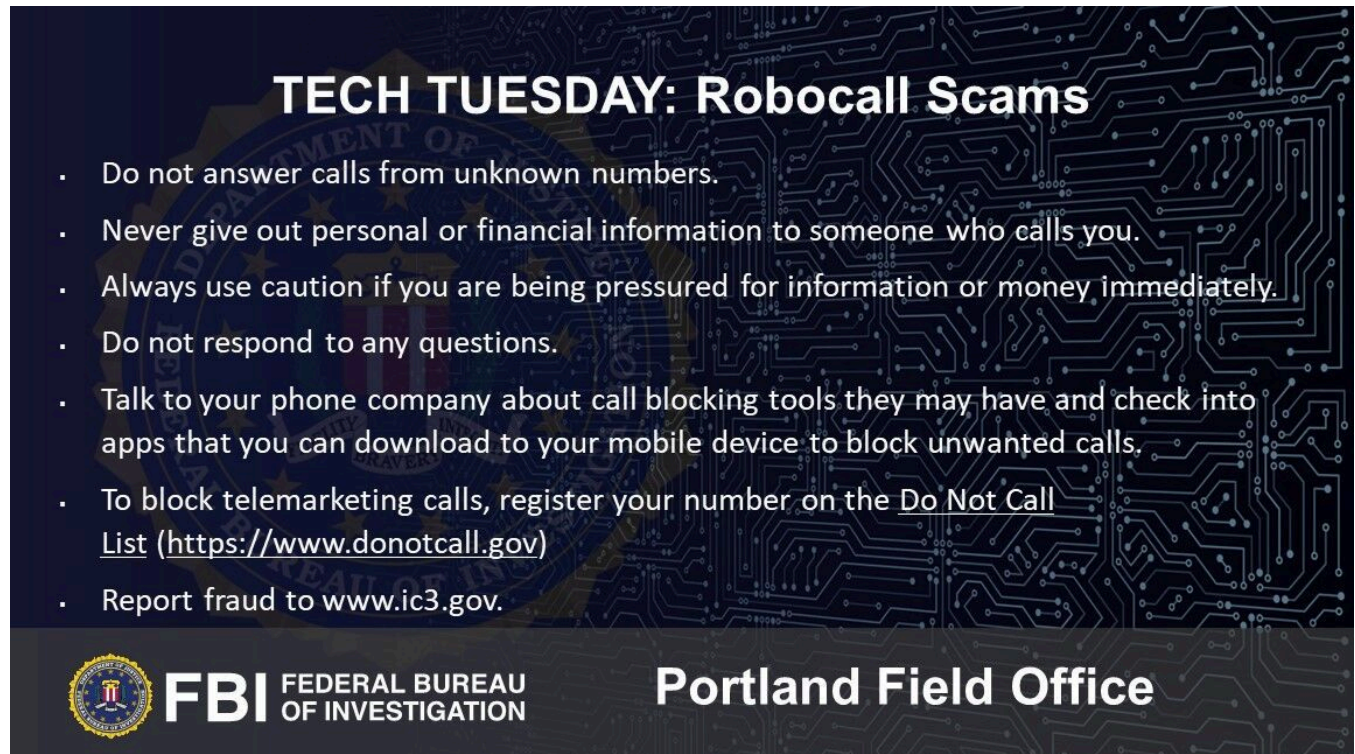


Tech Tuesday: Building a Digital Defense Against Robocalls

April 26, 2022

A graphic with a dark blue background featuring a circuit board pattern. On the left, a faint, large circular seal of the Federal Bureau of Investigation is visible. The text is white and centered. At the bottom left is the FBI logo and name, and at the bottom right is the text 'Portland Field Office'.

TECH TUESDAY: Robocall Scams

- Do not answer calls from unknown numbers.
- Never give out personal or financial information to someone who calls you.
- Always use caution if you are being pressured for information or money immediately.
- Do not respond to any questions.
- Talk to your phone company about call blocking tools they may have and check into apps that you can download to your mobile device to block unwanted calls.
- To block telemarketing calls, register your number on the Do Not Call List (<https://www.donotcall.gov>)
- Report fraud to www.ic3.gov.

 **FBI** FEDERAL BUREAU OF INVESTIGATION

Portland Field Office

Welcome to the Oregon FBI's Tech Tuesday segment. Today: Building a digital defense against robocalls.

If you're like most American's you've probably received a call, or twenty, regarding your cars extended warranty. For the second year in a row, auto warranty renewal calls were the top robocall complaint filed with the FCC by consumers in 2021.

Most of the reports received mention that the unwanted call begins with an automated or pre-recorded message that may instruct you to press a number to speak to a live operator or remove you from their call list, but pressing that number might lead to more robocalls instead.

The calls often include specific information about your particular car and warranty that can make the call seem more legitimate.

Other common scams include social security number phishing scam calls, credit card scams, fake insurance and healthcare, and phony lawsuit or criminal charges.

To avoid robocall scams follow these top tips from our partners at the Federal Communications Commission (FCC) on how to protect yourself:

Do not answer calls from unknown numbers. If you do so by mistake, hang up immediately.

Never give out personal or financial information to someone who calls you.

Always use caution if you are being pressured for information or money immediately.

If you answer the phone and the caller—or a recording—asks you to hit a button to stop getting the calls, you should just hang up. Scammers often use this trick to identify potential targets.

Do not respond to any questions, especially those that can be answered with “Yes.” The scammer is likely recording you and can use that verbal “yes” later to pretend you agreed to something you did not.

If you get an inquiry from someone who says they represent a company or a government agency, hang up and call the phone number on your account statement or on the company’s or government agency’s website to verify the authenticity of the request. You will usually get a written statement in the mail before you get a phone call from a legitimate source, particularly if the caller is asking for a payment.

Talk to your phone company about call blocking tools they may have and check into apps that you can download to your mobile device to block unwanted calls.

To block telemarketing calls, register your number on the [Do Not Call List](https://www.donotcall.gov) (<https://www.donotcall.gov>)

Legitimate telemarketers consult the list to avoid calling both landline and wireless phone numbers on the list.

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.

###

Sources:

<https://www.fcc.gov/data-spotlight-top-robocall-complaints-2021>
and <https://consumer.ftc.gov/articles/robocalls>