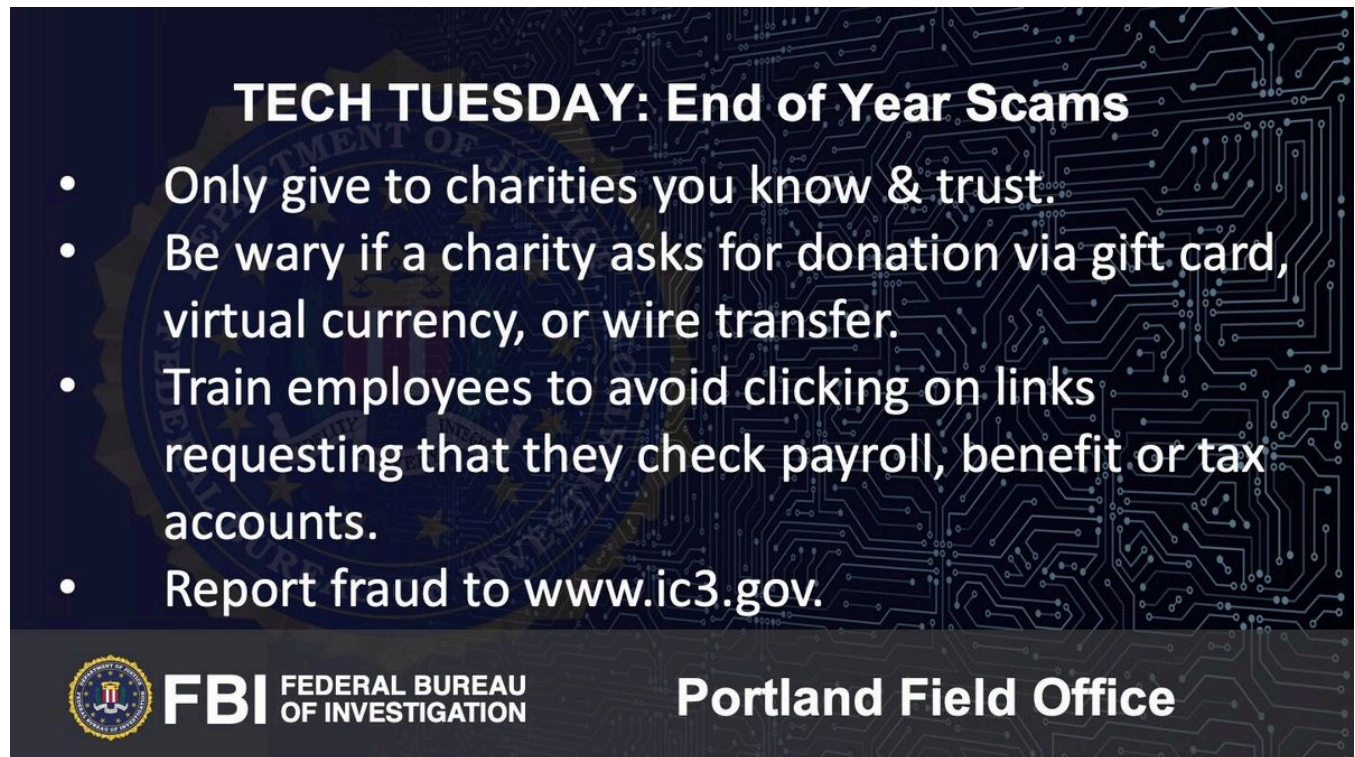


Tech Tuesday: End of Year Scams

December 28, 2021



TECH TUESDAY: End of Year Scams

- Only give to charities you know & trust.
- Be wary if a charity asks for donation via gift card, virtual currency, or wire transfer.
- Train employees to avoid clicking on links requesting that they check payroll, benefit or tax accounts.
- 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 as we close out 2021.

You managed to navigate the holiday season, and you have almost made it to the new year. There are just a few last-minute things you need to watch out for.

First up – charity fraud. You have until the 31st to make those end-of-year donations to charities so that you can claim the deductions on this year's taxes.

Charity scams can come to you in many forms: emails, social media posts, crowdfunding platforms, cold calls, or even text messages. Always use caution and do your research.

Give to established charities or groups whose work you know and trust.

Be aware of organizations with copycat names or names similar to reputable organizations.

Check the charity's track record on the **Federal Trade Commission's website**.

Give using a check or credit card. If a charity or organization asks you to donate through cash, gift card, virtual currency, or wire transfer, it's probably a scam.

Moving on – there are two more end-of-year concerns we want to warn you about. The first is payroll or benefit fraud. Employees may not be surprised to get a notice, purportedly from HR, to log into and check their online accounts as we hit the calendar change from one year to the next. As soon as the employee clicks on the conveniently-provided bad link, malware downloads to the system, and the bad actor now has access to your employee’s personal and financial info.

The second concern involves the payroll office itself. As your finance staff is preparing end-of-year reports, they may receive a bogus email – allegedly from the IRS – asking for Social Security numbers, bank account information, and the like.

In both cases, the best defense is a strong offense:

- Train your employees to never click on links or attachments.
- Train employees to never give out log-in credentials or personally identifying information in response to any email.
- Direct employees to forward suspicious requests for personal information to the IT or HR department.
- Ensure that log-in credentials used for payroll purposes differ from those used for other purposes, such as employee surveys.

That wraps it up for this year. Have a great and safe New Years.

And, as always, if you are the victim of this or any other 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.