

Tech Tuesday: Building a Digital Defense Against Click Scams

October 13, 2021

A graphic with a dark blue background featuring a circuit board pattern. In the center is a large, faint circular seal of the Federal Bureau of Investigation. Overlaid on the seal is the text "TECH TUESDAY: Click Scams" in white, bold, sans-serif font. Below this, there is a bulleted list of three items in white text. At the bottom left is the FBI logo and the text "FBI FEDERAL BUREAU OF INVESTIGATION". At the bottom right is the text "Portland Field Office" in white, bold, sans-serif font.

TECH TUESDAY: Click Scams

- Don't click – no matter how fearful, excited or curious you are.
- Never share personal or financial information via email, text message or phone unless you initiated the contact with a trusted entity.
- Report fraud to www.ic3.gov.

 **FBI** FEDERAL BUREAU OF INVESTIGATION

Portland Field Office

October is **#CybersecurityAwareness Month**. During this time, the FBI reminds everyone to **#BeCyberAware!** In honor of this recognition, today's Tech Tuesday report will focus on one of the most important things people can do to stay safe: Avoid the Click!

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

You've heard it time and again – DON'T click on that link! Whether it came by text, email, or a social media post, that link could cause you endless grief.

That link is part of what's called a phishing scam – phishing with a "ph". Scam artists need you to click on the link so they can download malware onto your device or trick you into logging into what you think is a legitimate website. In seconds, you have now given them access to your phone or laptop AND the user ID and password to your bank account.

Why do you click? That part of the scam is called social engineering. The bad actor's goal is to generate extreme fear or happiness in you – or maybe even just a strong sense of curiosity. He just needs you to act before you think.

For instance – you receive a text with a link claiming to be a video of you. It could be innocent enough (you were eating!) or distressing (you were caught naked or in an otherwise compromising act). You really, REALLY, want to see what that video shows. (See attached image.) Don't fall for it and certainly don't click!

Here are some helpful hints on how to stay safe, thanks to our partners at the Federal Communications Commission (FCC):

- Don't respond to calls or texts from unknown or suspicious numbers.
- Never share your personal or financial information via email, by text message, or over the phone.
- Be cautious if you're being pressured to share any information or make a payment immediately.
- Remember that government agencies will never call you to ask for personal information or money.
- Most importantly – don't click any links in a text message. If a friend sends you a text with a suspicious link that seems out of character, call them to make sure they weren't hacked.

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