

Tech Tuesday: Building a digital defense against utility scams

November 16, 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 and background is the text "TECH TUESDAY: Utility Scams" in white. Below this, there is a bulleted list of three items. 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".

TECH TUESDAY: Utility Scams

- Fraudsters will ask for payment by gift cards, cryptocurrency or pre-paid cards. Don't pay this way!
- Utilities will always send late-payment & cutoff notices, giving you time to pay. Demands for immediate payment should be a warning.
- Report online crimes 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 utility scams.

As we head into the heart of winter, no one wants to hear that their power, gas, or water might be cut off. Even if you are sure that you paid your bills, just the threat that there is a problem could be enough to get you to act without thinking.

Utility scams can happen online, by phone, or even in person. Someone pretending to be a utility provider will threaten shut-off if you do not pay immediately. Sometimes they ask for payment via cash, a popular money transfer app, or even a gift card.

Beyond the threat of non-payment, bad actors may also try to tell you that you have overpaid. They just need your bank account info to transfer the money back. Or, they may tell you that you need a special service or piece of equipment. Again, they need you to pre-pay.

Here's how to protect yourself:

- Don't be rushed to act. Utilities will always send you late payment and cut-off notices with time for you to respond.
- Utilities will ask for payment in traditional ways. They will not demand payment through gift cards, pre-paid debit cards, or cryptocurrency.
- Don't click on links or open attachments in text messages or emails.
- Don't give out account or other financial information to unsolicited callers.
- If someone shows up at your door, demand proof of identity and contact the utility to confirm the person is legitimate.
- Finally, the scammer may spoof the utility's phone number or email address. If you have any questions, contact the utility directly to confirm any issues. Use the contact information off your regular bill or its publicly-available website – not what the suspicious person provided to you.

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.