

Tech Tuesday: Building a Digital Defense Against Video Chat Platforms

January 18, 2022

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 this is the text 'TECH TUESDAY: Video Communication Systems' in bold white letters. Below this title is a bulleted list of four 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' in bold white letters.

TECH TUESDAY: Video Communication Systems

- Know what security systems are available for your platform & turn them on.
- Know what data the service is collecting about you & how it is storing, sharing, or selling it.
- Make sure group calls are password-protected and confirm participants' identities before proceeding.
- Report scams 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 with video communication systems.

Over the past two years, many people have had crash courses in how to use video communications systems. Personal apps such as FaceTime and Skype have made it easier to keep in touch with friends and family during COVID times. Other services – such as Zoom, Teams, and Google Meet – were lifelines for schools, businesses, and community groups.

Just because most of us are back in school or back to work doesn't mean the bad actors aren't still trying to use these video communications systems to bilk your bank account.

Here are some reminders on how to stay safe:

- Make sure to research what security settings are available – and turn them on – for whatever platforms you are using.

- Avoid connecting your video communications apps or systems to your social media accounts whenever possible.
- Don't accept calls or chats from unknown people or numbers.
- Review the app or service's privacy and terms of service policies before using. Check back for updates periodically and only allow the app or service the minimal amount of permissions necessary.
- Know exactly what kind of data the app or service is collecting about you and how it is storing, sharing, or selling that information.
- Make sure group calls are password-protected and confirm participants' identities before proceeding.
- Make sure to leave or end the call every time. Don't count on the host to do it.
- Password protect your account and use multi-factor authentication whenever possible.
- Check your visual background or use a virtual background. You may be leaking personal information about yourself or others.

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 or call your FBI local office.