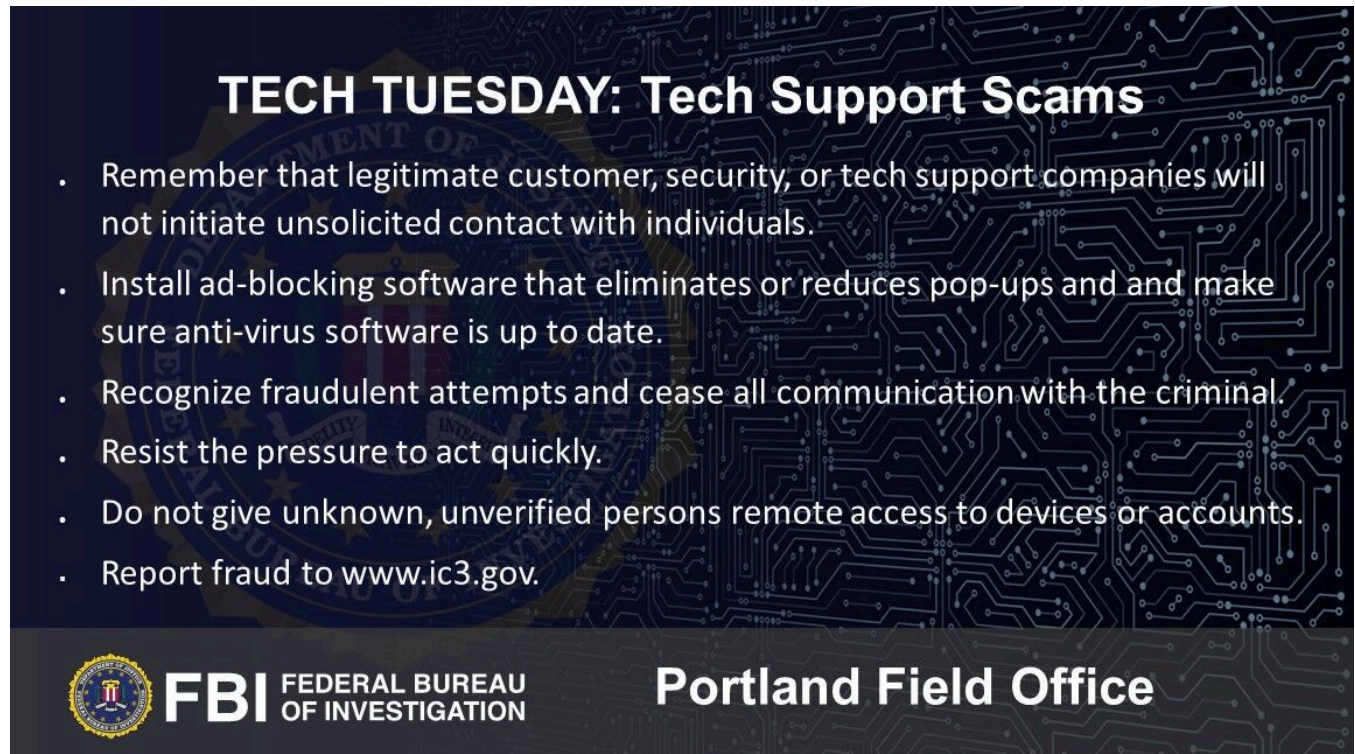


Tech Tuesday: Building a Digital Defense Against Tech Support Fraud

April 19, 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: Tech Support Scams' in white. Below the title is a list of six bullet points 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.

TECH TUESDAY: Tech Support Scams

- Remember that legitimate customer, security, or tech support companies will not initiate unsolicited contact with individuals.
- Install ad-blocking software that eliminates or reduces pop-ups and and make sure anti-virus software is up to date.
- Recognize fraudulent attempts and cease all communication with the criminal.
- Resist the pressure to act quickly.
- Do not give unknown, unverified persons remote access to devices or 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 against Tech Support Fraud.

Tech Support Fraud involves a criminal claiming to provide customer, security, or technical support or service to defraud unwitting individuals.

Criminals may pose as support or service representatives offering to resolve such issues as a compromised email or bank account, a virus on a computer, or a software license renewal.

Many victims report being directed to make wire transfers to overseas accounts or purchase large amounts of prepaid cards.

In 2021, the FBI's Internet Crime Complaint Center received nearly 24,000 complaints related to Tech Support Fraud from victims in 70 countries. The losses amounted to over \$347 million, which represents a 137 percent increase in losses from 2020.

Most victims, almost 60 percent, report to be over 60 years of age, and experience at least 68 percent of the losses (almost \$238 million).

Initial contact with the victim typically occurs through the following methods:

Telephone: an unsolicited telephone call from an individual claiming the victim's device or computer is infected with a virus or is sending error messages to the caller.

Search Engine Advertising: Criminals pay to have their fraudulent tech support company's link show higher in search results hoping victims will choose one of the top links in search results.

Pop-up message: The victim receives an on-screen pop-up message claiming a virus has been found on their computer. In order to receive assistance, the message requests the victim call a phone number associated with the fraudulent tech support company.

Locked screen on a device: The victim's device displays a frozen, locked screen with a phone number and instructions to contact a fraudulent tech support company.

SUGGESTIONS FOR PROTECTION

Remember that legitimate customer, security, or tech support companies will not initiate unsolicited contact with individuals.

Install ad-blocking software that eliminates or reduces pop-ups and malvertising (online advertising to spread malware).

Be cautious of customer support numbers obtained via open source searching.

Recognize fraudulent attempts and cease all communication with the criminal.

Resist the pressure to act quickly.

Do not give unknown, unverified persons remote access to devices or accounts.

Ensure all computer anti-virus, security, and malware protection is up to date.

If you are a victim

Individuals who receive a pop-up or locked screen, should shut down the device ***immediately***. Ignore any pop-ups instructing to not power off or restart the computer. Victims who reported shutting down the device and waiting a short time to restart usually find the pop-up or screen lock has disappeared.

Do not re-contact fraudulent tech scam companies. Expect additional fraudulent calls as these companies often share their customer database information.

Should a criminal gain access to a device or an account, individuals should take precautions to protect their identity. Immediately contact financial institutions to place protection on accounts as well as change passwords and actively monitor accounts and personal information for suspicious activity.

As this type of fraud has become more commonplace, criminals have started to pose as government agents, even offering to recover supposed losses related to tech support fraud schemes or to request financial assistance with "apprehending" criminals.

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