Major Cybercrime Unit
U.S. Army Criminal Investigation Command

Cybercrime Prevention Flyer

Report a crime to U.S. Army Criminal Investigation Command

Major Cybercrime Unit

27130 Telegraph Road
Quantico, Virginia 22134

Email

MCU Web Page

CID LOOKOUT
ON POINT FOR THE ARMY

DISTRIBUTION:
This document is authorized for the widest release without restriction.

"Do What Has To Be Done"

CPF 00009-2021-CID361-9H **6 July 2021**

Tech Support Fraud

If you ever receive a pop-up on your screen, a random phone call, text message, or an email stating that your computer is infected, stop what you are doing; do not click the pop-up, answer any questions, click any links, or call the phone number provided. In 2020, the Internet Crime Complaint Center received many complaints related to tech support scams; so many, that losses amounted to over $146 million dollars. While COVID-19 restrictions are being lifted, telework and remote learning remain widely used, which provides fertile ground for the tech support scammer. However, with some awareness you can identify a tech support scam and reduce your chances of becoming a victim.

What are tech support scams?

Tech support scams are attempts to coerce victims to pay for useless services, install malware granting access to your system, or steal your Personally Identifiable Information (PII), financial, or credit card information.

Below are tech support scams you may encounter. This list is not meant to be all-inclusive.

Pop-up
A pop-up window opens warning that your device has been compromised and provides a link to click or a phone number to call. The pop-up says if you do not respond immediately, you risk losing all of your data and personal information. However, clicking the pop-up link might initiate the download of malicious software or lock down your device completely with ransomware. If you call the number the scammer will likely ask you for remote access to your computer, try to sell you worthless repair services, or bogus software which could be malware. The malware could cause serious, even permanent, damage to your computer.

Legitimate tech companies do not use pop-up notifications to tell users there is an issue with their computer.

Telephone Call
You receive an unsolicited phone call from someone claiming to be affiliated with a reputable tech company saying there is suspicious activity or a virus on your computer. The scammer may demand you pay immediately to have the matter fixed. The criminal might even try to persuade you to allow remote access to your device.

Legitimate tech companies will not call or text you to tell you about a problem with your computer or software.

Unsolicited Email
You receive an unsolicited email that looks like legitimate correspondence from a trusted tech company. The email might say that you need to install a software update or confirm account information. Scammers do this with the intention of tricking you into downloading malicious software to get control of your computer so they can then, get your PII, passwords, or financial information.

Legitimate tech companies will not email you to tell you that that you have a problem with your computer or software.

Online Advertisements and Paid Search Results
Be careful when searching for online tech support. Faux tech support companies sometimes pay to promote their services on reputable search engines. Search results could contain links to a scam and not the site you are looking for. Just clicking on the link of a fake tech support company's website might initiate the download of malware or give them access to your computer. If you purchase services from one of these illegal companies, you could expose the credit card you use for payment to fraud or compromise any personal information you provide.

Protect Yourself

- Use a virtual private network (VPN).
- Update your antivirus software regularly.
- Change your browser settings to block pop-ups.
- If you receive an unsolicited phone call for tech support, hang up.
- If you receive an unsolicited text for tech support, delete it.
- Do not give anyone control of your computer you do not trust.
- Do not download any unsolicited software or download software from unfamiliar sources.
- Ask your tech support questions; you are entitled to ask them to explain what they are doing.
- If you receive a pop-up notification, do not click any links, do not call any phone numbers; just close the pop-up.
- If you need technical support, go to the specific website of the manufacturer of your device or the specific website of the product you have a technical question about.
- If you receive an unsolicited email for tech support, do not click any links in the email and report it to your email service provider.
- If you provided funds to a scammer, report the scam to your bank and any relevant financial institutions as soon as possible.
- If you suspect a tech support scam attempt against your government or work computer, immediately contact your local IT department.
- If you suspect a tech support scam attempt against your personal device contact, report the scam to the Federal Trade Commission and Internet Crime Complaint Center.

Additional Resources

How to Identify and Protect Yourself from an Unsafe Website

Federal Trade Commission - Tech Support Scams

Ransomware Cybercrime Prevention Flyer

Phishing Scams and Email Spoofing Cybercrime Prevention Flyer

To receive future MCU Cybercrime Prevention Flyers, send an email to: Subscribe CPF

Disclaimer: The appearance of hyperlinks in this Cybercrime Prevention Flyer, along with the views and opinions of authors, products or services contained therein do not constitute endorsement by CID. These sites are used solely for authorized activities and information that support the organization's mission. CID does not exercise any editorial control over the information you may find at these link locations.