PENNSYLVANIA STATE POLICE

COMMUNITY AWARENESS BULLETIN

CAB 001-25 June 4, 2025

MICROSOFT OFFICE POP-UP SCAMS

The Pennsylvania State Police (PSP) is advising residents of an increase in Microsoft Office pop-up scams, particularly targeting elderly victims. During these scams, a Microsoft Office pop-up is displayed on the victim's computer indicating there is a virus or some type of computer malfunction and they should immediately contact the Microsoft Office support phone number. Similar languages observed on the pop-up messages include, "Your computer has been hacked, please call Microsoft to reinstate your service" and listed a number to call. In some instances, the victim receives a phone call from a perpetrator pretending to be an employee with Microsoft or with the Federal Bureau of Investigation (FBI) advising the victim their computer or bank account have been compromised.

To remedy the problem, victims are demanded by the perpetrators to deplete their bank accounts of all funds. The perpetrators either arrive at the victim's residence to take possession of the money or demand victims purchase gift cards, gold coins, or bitcoin, and coordinate a pick-up or have the items mailed. Some victims have lost over $100,000 in these scams.

RECOMMENDATIONS

- Recognize scam attempts and immediately end communication with the perpetrator.
- Disconnect from the internet and shut down your device if you see a pop-up message or locked screen. Pop-ups are regularly used by perpetrators to spread malicious software. Enable pop-up blockers to avoid accidentally clicking on a pop-up.
- Keep computer anti-virus, security software, and malware protections up to date. Use reputable anti-virus software and firewalls.
- Be careful of what you download. Never open an email attachment from someone you do not know and be wary of email attachments forwarded to you.
- Take precautions to protect your identity if a criminal gains access to your device or account. Immediately contact your financial institutions to place protections on your accounts and monitor your personal information for suspicious activity.
- Financial institutions will never ask for personal information through text, email, or telephone calls. Telephone calls, texts, and emails can be easily spoofed to fool you into thinking they are from your financial institution. If your financial institution calls, texts, or emails claiming there is a problem with your account that you must resolve immediately, do not give them any personal information. Log in through a bookmarked link on your computer or through the mobile app to see if there really is a problem. Never use a link in an email or respond to a text to log into a financial or any other account – these links often contain malware to steal your information.
- Check financial accounts on secure Wi-Fi or over cellular data. If you frequently use unsecure Wi-Fi, consider using a Virtual Private Network (VPN). You can also look for mobile apps that check whether a Wi-Fi signal is secure in your app store.

Contact your local police department or the Federal Trade Commission at https://reportfraud.ftc.gov/ to report the incident immediately.