Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

September 29, 2023

Alert Number
I-091223-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

"Phantom Hacker" Scams Target Senior Citizens and Result in Victims Losing their Life Savings

The FBI is warning the public of a recent nationwide increase in "Phantom Hacker" scams, significantly impacting senior citizens. This Phantom Hacker scam is an evolution of more general tech support scams, layering imposter tech support, financial institution, and government personas to enhance the trust victims place in the scammers and identify the most lucrative accounts to target. Victims often suffer the loss of entire banking, savings, retirement, or investment accounts under the guise of "protecting" their assets. Between January and June 2023, 19,000 complaints related to tech support scams were submitted to the FBI Internet Crime Complaint Center (IC3), with estimated victim losses of over $542 million. Almost 50% of the victims reported to IC3 were over 60 years-old, comprising 66% of the total losses. As of August 2023, losses have already exceeded those in 2022 by 40%.

THE SCAM
Phase 1 - Tech Support Imposter

1. A scammer posing as a tech or customer support representative from a legitimate company contacts the victim through a phone call, text, email, or a pop-up window on the victim's computer and instructs the victim to call a number for "assistance."
2. Once the victim calls the number, a scammer directs the victim to download a software program, allowing the scammer remote access to the victim's computer. The scammer pretends to run a virus scan on the victim's computer and falsely claims the computer has been or is at risk of being hacked.
3. Next, the scammer requests the victim open their financial accounts to determine whether there have been any unauthorized charges - a tactic the scammer uses to determine which financial account is most lucrative for targeting. The scammer chooses an account to target and tells the victim they will receive a call with further instructions from the fraud department of the respective financial institution hosting that account.

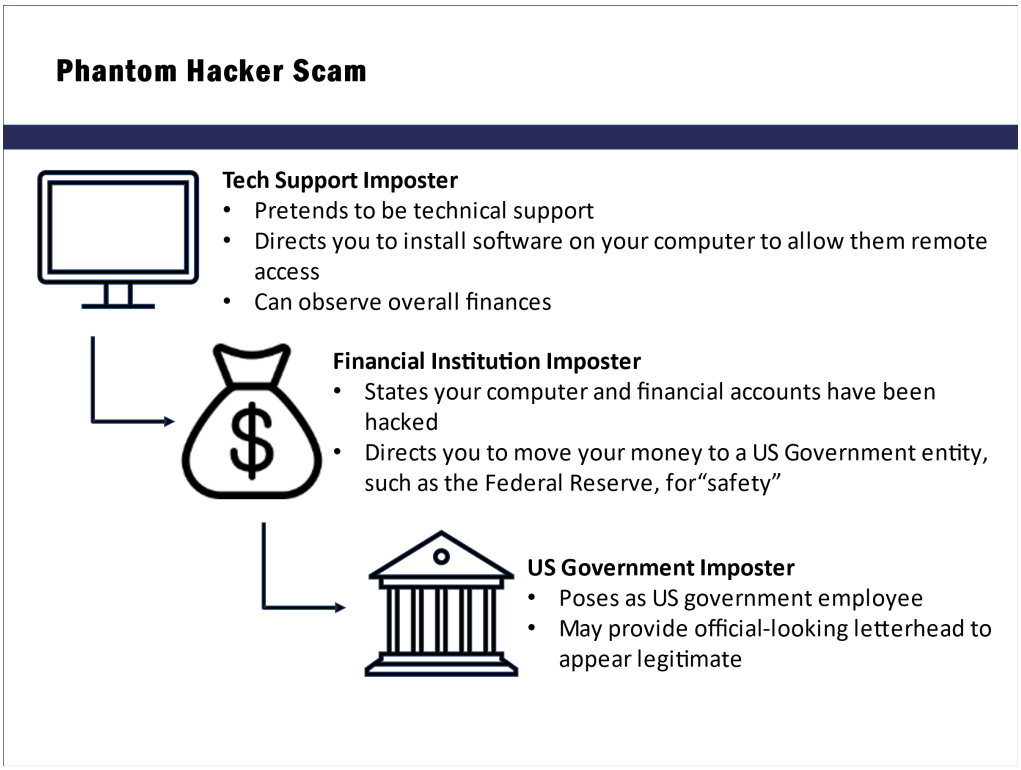
Phase 2 - Financial Institution Imposter

1. A scammer posing as a representative of the financial institution mentioned in phase 1, such as a bank or a brokerage firm, contacts the victim. The scammer falsely informs the victim their computer and financial accounts have been accessed by a foreign hacker and the victim must move their money to a "safe" third-party account, such as an account with the Federal Reserve or another US Government agency.
2. The scammer directs the victim to transfer money via a wire transfer, cash, or cryptocurrency, often directly to overseas recipients. The scammer may instruct the victim to send multiple transactions over a

span of days or months.
3. The scammer tells the victim to not inform anyone of the real reason they are moving their money.

Phase 3 - US Government Imposter

1. The victim may also be contacted by a scammer posing as an employee at the Federal Reserve or another US Government agency. If the victim becomes suspicious of the government imposter, the scammer may send an email or a letter on what appears to be official US Government letterhead to legitimize the scam.
2. The scammer continues to emphasize the victim's funds are "unsafe" and they must be moved to a new "alias" account for protection until the victim concedes.



TIPS TO PROTECT YOURSELF

- Do not click on unsolicited pop-ups, links sent via text messages, or email links or attachments.
- Do not contact the telephone number provided in a pop-up, text, or email.
- Do not download software at the request of an unknown individual who contacted you.
- Do not allow an unknown individual who contacted you to have control of your computer.
- The US Government will never request you send money via wire transfer to foreign accounts, cryptocurrency, or gift/prepaid cards.

REPORT IT

The FBI requests victims report these fraudulent or suspicious activities to their local FBI field office and the FBI IC3 at www.ic3.gov. Be sure to include as much information as possible.

- The name of the person or company that contacted you.
- Methods of communication used, to include websites, emails, and telephone numbers.
- The bank account number(s) where the funds were wired to and the recipient's name(s).

For additional information on similar scams, please see previous Public

Service Announcements published on the FBI IC3 website.

IC3 | Technical and Customer Support Fraud
IC3 | Increase in Tech Support Scams Targeting Older Adults and Directing Victims to Send Cash through Shipping Companies
IC3 | Scammers Using Computer-Technical Support Impersonation Scams to Target Victims and Conduct Wire Transfers