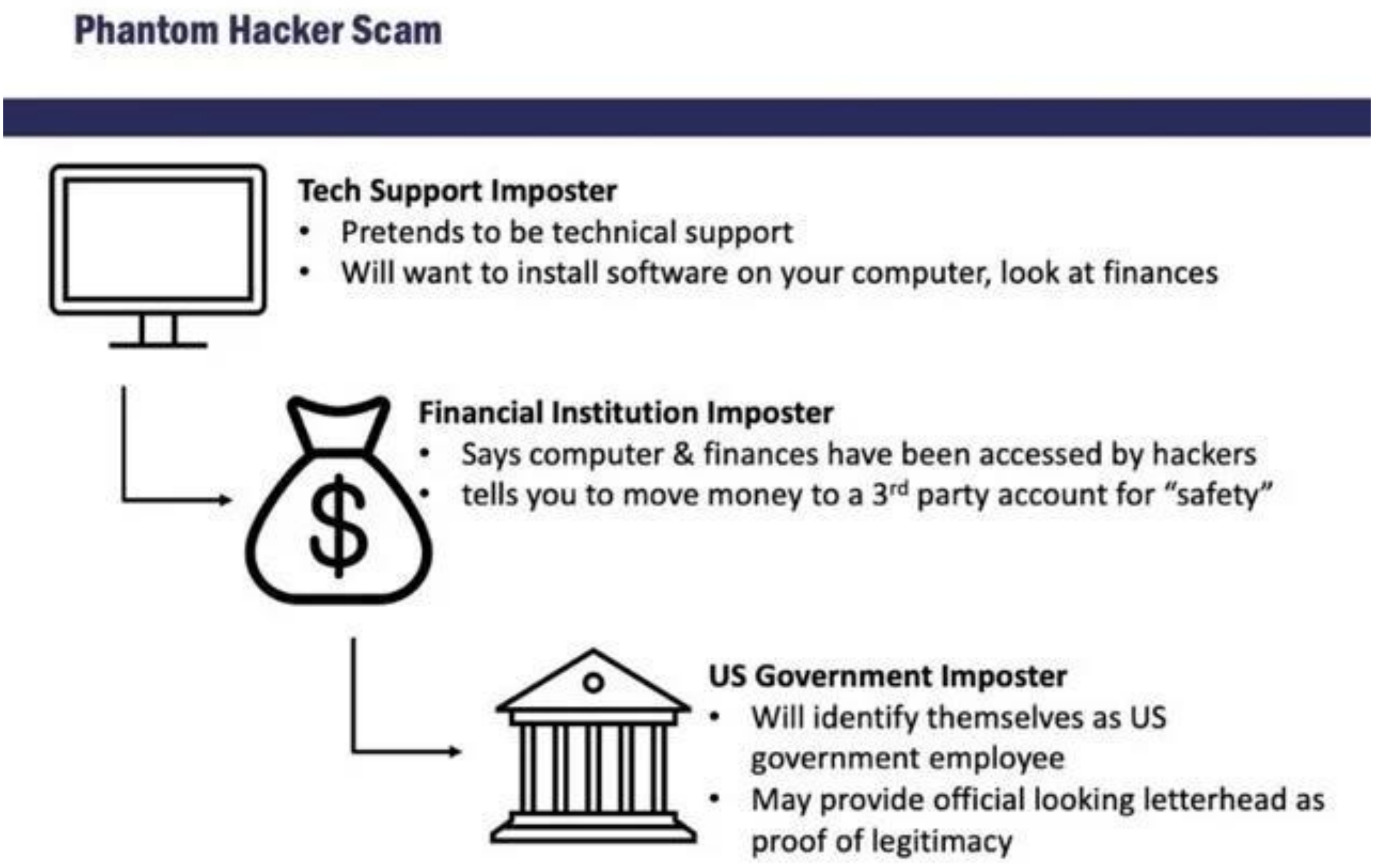

Phantom Hacker Scam

Tech Support Imposter

- Pretends to be technical support
- Will want to install software on your computer, look at finances

Financial Institution Imposter

- Says computer & finances have been accessed by hackers
- tells you to move money to a 3rd party account for "safety"

US Government Imposter

- Will identify themselves as US government employee
- May provide official looking letterhead as proof of legitimacy

View original article

"The Phantom Hacker" Scam: How It Works

The FBI has observed repeated behavior by criminals involved in "The Phantom Hacker" scam. The ruse is often perpetrated in three major steps:

Step 1 – Tech Support Imposter

In the first step, a scammer posing as customer support representative from a legitimate technology company initiates contact with the victim through a phone call, text, email, or a pop-up window on their computer and instructs the victim to call a number for "assistance."

Once the victim calls the phone 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 victim's computer either has been or is at risk of being hacked.

Next, the scammer requests the victim open their financial accounts to determine whether there have been any unauthorized charges – a tactic to allow the scammer to determine which financial account is most lucrative for targeting. The scammer informs the victim they will receive a call from that financial institution's fraud department with further instructions.

Step 2 – Financial Institution Imposter

In the second step, a scammer, posing as a representative of the financial institution mentioned above, 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 U.S. Government agency.

The victim is directed to transfer money via a wire transfer, cash, or wire conversion to cryptocurrency, often directly to overseas recipients. The victim is also told not to inform anyone of the real reason they are moving their money. The scammer may instruct the victim to send multiple transactions over a span of days or months.

Step 3 – U.S. Government Imposter

In the third step, the victim may be contacted by a scammer posing as the Federal Reserve or another U.S. Government agency. If the victim becomes suspicious, the scammer may send an email or a letter on what appears to be official U.S. Government letterhead to legitimize the scam. The scammer will continue to emphasize the victim’s funds are “unsafe” and they must be moved to a new “alias” account for protection until the victim concedes.

Victims often suffer the loss of entire banking, savings, retirement, and investment accounts under the guise of “protecting” their assets.

Tips to Protect Yourself

The FBI recommends that the public take the following steps to protect themselves from “The Phantom Hacker” scam:

- 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 to them via wire transfer, cryptocurrency, or gift/prepaid cards.

Reporting Suspected Fraud

The FBI requests victims report these fraudulent or suspicious activities to the FBI Internet Crime Complaint Center (IC3) at www.ic3.gov. Be sure to include as much information as possible, such as:

- 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 where the funds were wired to and the recipient’s name(s).