Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

June 02, 2016

Alert Number
I-060216-PSA

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

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

TECH SUPPORT SCAM

The Internet Crime Complaint Center (IC3) is receiving an increase in complaints related to technical support scams, where the subject claims to be an employee (or an affiliate) of a major computer software or security company offering technical support to the victim. Recent complaints indicate some subjects are claiming to be support for cable and Internet companies to offer assistance with digital cable boxes and connections, modems, and routers. The subject claims the company has received notifications of errors, viruses, or security issues from the victim's internet connection. Subjects are also claiming to work on behalf of government agencies to resolve computer viruses and threats from possible foreign countries or terrorist organizations. From January 1, 2016, through April 30, 2016, the IC3 received 3,668 complaints with adjusted losses of $2,268,982.

Technical Details

Initial contact with the victims occurs by different methods. Any electronic device with Internet capabilities can be affected.

1. Telephone: This is the traditional contact method. Victims receive a "cold" call from a person who claims the victim's computer is sending error messages and numerous viruses were detected. Victims report the subjects have strong foreign accents.
2. Pop-up message: The victim receives an on-screen pop-up message claiming viruses are attacking the device. The message includes a phone number to call to receive assistance.
3. Locked screen on a device (Blue Screen of Death - BSOD): Victims report receiving a frozen, locked screen with a phone number and instructions to contact a (phony) tech support company. Some victims report being redirected to alternate websites before the BSOD occurs. This has been particularly noticed when the victim was accessing social media and financial websites.
4. Pop-up messages and locked screens are sometimes accompanied by a recorded, verbal message to contact a phone number for assistance.

Once the phony tech support company/representative makes verbal contact with the victim, the subject tries to convince the victim to provide remote access to their device.

If the device is mobile (a tablet, smart phone, etc.), the subject often instructs the victim to connect the device to a computer to be fixed. Once the subject is remotely connected to the device, they claim to have found multiple viruses, malware, and/or scareware that can be removed for a fee. Fees are collected via a personal debit or credit card, electronic check, wire transfer, or prepaid card. A few instances have occurred in which the victim paid by personal check.

Variations and Trends

An increasingly reported variation of the scam occurs when the subject contacts the victim offering a refund for tech support services previously rendered because the company has closed.

The victim is convinced to allow the subject access to their device and to log onto their online bank account to process the refund. The subject then has control of the victim's device and bank account. With this access, the subject appears to have "mistakenly" refunded too much money to the victim's account, and requests the victim wire the difference back to the subject company. In reality, the subject transferred funds among the victim's own accounts (checking, savings, retirement, etc.) to make it appear as though funds were deposited. The victim wires their own money back to the company, not finding out until later that the funds came from one of their own accounts. The refunding and wiring process can occur multiple times, which results in the victim losing thousands of dollars.

Victims are increasingly reporting subjects are becoming hostile, abusive, and utilizing foul language and threats when being challenged by victims.

Additional Threats

The tech support scam is an attempt by subjects to gain access to victim devices. However, more can happen once a subject is given access to the device. For example:

- The subject takes control of the victim's device and/or bank account, and will not release control until the victim pays a ransom.
- The subject can access computer files that may contain financial accounts, passwords, and personal data (health records, social security numbers, etc.).
- The subject may intentionally install viruses on the device.
- The subject threatens to destroy the victim's computer or continues to call in a harassing manner.

Defense and Mitigation

- Recognize the attempt and cease all communication with the subject.
- Resist the pressure to act quickly. The subjects will urge the victim to fast action in order to protect their device. The subjects create a sense of urgency to produce fear and lure the victim into immediate action.
- Do not give unknown, unverified persons remote access to devices or accounts. A legitimate software or security company will not directly contact individuals unless the contact is initiated by the customer.
- Ensure all computer anti-virus, security, and malware protection is up to date. Some victims report their anti-virus software provided warnings prior to the attempt.
- If a victim receives a pop-up or locked screen, shut down the device immediately. Victims report that shutting down the device and waiting a short time to restart usually removes the pop-up or screen lock.
- Should a subject gain access to a device or an account, victims should take precautions to protect their identity, immediately contact their financial institutions to place protection on their accounts, and monitor their accounts and personal information for suspicious activity.

Filing a Complaint

Individuals who believe they may be a victim of an online scam (regardless of dollar amount) can file a complaint with the IC3 at www.ic3.gov.

To report tech support scams, please be as descriptive as possible in the complaint including:

1. Name of the subject and company.
2. Phone numbers and email addresses used by the subject.
3. Websites used by the subject company.
4. Account names and numbers and financial institutions that received any funds (e.g., wire transfers, prepaid card payments).
5. Description of interaction with the subject.

Complainants are also encouraged to keep all original documentation, emails, faxes, and logs of all communications.

Because scams and fraudulent websites appear very quickly, individuals are encouraged to report possible Internet scams and fraudulent websites by filing a complaint with the IC3 at www.ic3.gov. To view previously released PSAs and Scam Alerts, visit the IC3 Press Room at www.ic3.gov/media/default.aspx.