MS-ISAC

MS-ISAC Security Primer

Tech Support Call Scams

March 2017, SP2017-1221

In a Tech Support Call Scam, a malicious actor, claiming to work for a well-known technology company, cold calls victims to convince them that their computer is being attacked, attacking another computer, or infected with viruses, and that the caller can remediate the problem. Victims who comply with the caller's requests are highly likely to compromise their computer and experience monetary loss.

RECOMMENDATIONS:

IF YOU RECEIVE A CALL:

- If you receive an unsolicited telephone call from a technology company, hang up and report the incident to either your local police department, Information Technology (IT) department, or the Internet Crime Complaint Center (IC3, www.ic3.gov). Most legitimate technology companies will not directly call a computer owner, unless the computer owner requested assistance.
- Do not rely on caller identification (Caller ID) to authenticate a caller. Callers can spoof telephone numbers so they appear to be coming from another location or entity.
- Never provide passwords or bank account information over the telephone; legitimate organizations will never call and ask for sensitive information.
- Do not turn computer monitors off at the request of callers; legitimate organizations will never request the computer monitor to be turned off and will not cold call users.

IF YOU PREVIOUSLY RECEIVED A CALL:

- If you provided password information, change the password for that account. Never use the same password for multiple accounts.
- Use a credible anti-virus program, and enable automatic installation of software patches. If malware may have been downloaded, run an anti-virus scan on the computer.
- If you provided credit card information and the caller charged the account, call the credit card provider and request to reverse those charges. Check financial statements for other unauthorized charges.
- Register your telephone number on the National Do Not Call Registry (www.donotcall.gov) and report any further solicitation calls.

RECOMMENDATIONS FOR AGENCIES AND DEPARTMENTS:

- Monitor agency credit card statements and be aware of any suspicious transactions for software packages or technology support, as victims may use government credit cards to pay for the service or the callers may gain access to government financial accounts.
- Implement the policy of least privilege, as this will aid in preventing users from installing some types of malware.
- Continuously monitor the network with active and up-to-date anti-virus and anti-spyware software, and firewalls. Any malware detected should be automatically sent to the IT department for review and mitigation.
- Train end users regarding social engineering tactics and inform users of the possibility of these tactics being used in a telephone call, as seen in the Tech Support Call Scam.

The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance for SLTT governments, is available at 866-787-4722, SOC@cisecurity.org, or https://msisac.cisecurity.org/. The MS-ISAC is interested in your comments - an anonymous feedback survey is available at: https://www.surveymonkey.com/r/MSISACProductEvaluation.