ROLL CALL RELEASE
INTELLIGENCE FOR POLICE, FIRE, EMS, AND SECURITY PERSONNEL
11 March 2014

(U//FOUO) Fake Help Desk Scams an Ongoing Problem

(U//FOUO) Law enforcement continues to see reporting of malicious cyber actors using fake help desk scams, also known as technical support scams. These scams, if successful, seek to compromise and take control of computer systems. Malicious cyber actors send users an e-mail or they make cold calls, purportedly representing a help desk from a legitimate software or hardware vendor. The malicious cyber actors try to trick users into believing that their computer is malfunctioning—often by having them look at a system log that typically shows scores of harmless or low-level errors—then convincing them to download software or let the "technician" remotely access the personal computer to "repair" it.

- (U) Colleges, universities, and private organizations have reported attempts by fake help desks to gain personal information or access through e-mails spoofed to appear from the organization's real help desk. The e-mails request that users "click" on a URL and enter their personal information.
- (U//FOUO) A US government agency (USGA) reported on 14 January 2014 that while using a virtual private network from home, a user unknowingly called a fake support phone number, enabling the "help desk" to gain access to the computer's hard drive. The incident is under investigation for possible malware or backdoor access to the USGA machine.

(U) On 8 April 2014, support and updates for Windows XP will no longer be available—including security updates, non-security hotfixes, free or paid assisted support options, and online technical content updates. This action could present an opportunity for malicious cyber actors to initiate a new round of fake help desk scams targeting XP users with malicious e-mails or phone solicitations that could lead to compromise of users' systems.

(U//FOUO) **Best Practices if You Suspect a Fake Help Desk Scam**

(U//FOUO) **Employees and Individuals:**

- (U//FOUO) Be suspicious of any e-mail that asks you to divulge personal or financial information, is poorly written, is urgent, or contains a link to a website that does not match the organization sending the e-mail.
- (U//FOUO) Never give control of your computer to a third party unless you can confirm the party is a legitimate representative of a computer support team with whom you are already a customer or member of the organization.
- (U//FOUO) If contacted with a perceived fake request, take the caller's information down and immediately report it to your organizational help desk or local authorities.

(U//FOUO) **Organizations and Individuals Should:**

- (U//FOUO) Keep your software and security programs up to date.
- (U//FOUO) Block execution of embedded URLs within e-mails.

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to https://forms.us-cert.gov/report/ and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

IA-0107-14