February 2, 2016

OCR Cyber-Awareness Monthly Update

As we begin the New Year, OCR is launching a new Cyber-Awareness initiative to help our regulated community become more knowledgeable about the various security threats and vulnerabilities that currently exist in the healthcare sector; what security measures can be taken to decrease the possibility of being exposed by these threats; and how to reduce breaches of ePHI.

January 2016 Topics

- Ransomware
- "Tech Support" Scam
- New Tool: Better Business Bureau (BBB) Scam Tracker

Ransomware – Ransomware is malicious software that, when deployed, effectively walls off data so that it is inaccessible to authorized users. Ransomware frequently infects devices and systems through spam and phishing messages, botnets, exploit kits, compromised websites, and malvertising. Ransomware uses a social engineering trick to get potential victims to click on malicious email attachments or open crafted Short Message Service (SMS or text) messages, which lure them to compromised or malicious websites. Ransomware targets all sizes of businesses and institutions, home computers, mobile phones, and other devices.

According to the FBI, use of ransomware by cybercriminals has increased significantly recently. Reports by IBTimes claim that cybercriminals from many different countries are increasing ransomware attacks on U.S. targets. Also, a joint study conducted by several security firms estimates that creators of "CryptoWall 3.0," a ransomware, have obtained over $325 million from victims since its January 2015 launch. Fox-IT, a cybersecurity company, reported that "CryptoWall," "CTB-Locker," and "TorrentLocker" are three top active ransomware programs.

Cybercriminals charge from hundreds to thousands of dollars to unlock the data, and have been collecting ransom payments using digital payments systems such as "MoneyPak," "CashU," "Reloadit," and "Bitcoin."

To combat the threat of ransomware, Covered Entities and Business Associates should consider:

- Backing up data onto segmented networks or external devices and making sure backups are current.
- Ensuring software patches and anti-virus are current and updated.
- Installing pop-up blockers and ad-blocking software.
- Implementing browser filters and smart email practices.

Resources:

The Department of Homeland Security (DHS): https://www.us-cert.gov/ - *(For Ransomware remediation)*

The Federal Bureau of Investigations (FBI): http://www.ic3.gov/default.aspx - *(To Report ransomware schemes)*

Tech Support Scam - This scam involves a criminal posing as a computer support technician that makes an unsolicited call to trick a potential victim into believing his/her computer is infected with malware. A victim is then persuaded to visit websites to download malicious software that gives the criminal the capability to remotely access and control the victim's machine. Once the criminal has gained the victim's trust, the criminal charges hundreds of dollars for "phony" assistance with malicious software removal or for the purchase of fraudulent support plans or software.

Other forms of scam tactics have been used besides phone call scams. These include: pop-up ads seeded into websites that claim a victim's computer is infected with malware; promoting promises to increase the speed and performance of a victim's PC, which leads a victim to a malicious website; and malicious search ads that attract an unsuspecting victim seeking online support.

Reports of this type of scam have increased recently, especially among older individuals. According to Microsoft's Digital Crime Unity, tech support scams are the single largest consumer scam perpetrated in America today, with approximately 3.3 million victims, and criminals who are collecting $1.5 billion annually.

To combat the threat of this type of scam, Covered Entities and Business Associates should consider training staff to:

- Hang up the phone if you are suspicious of the caller.
- Never allow a third-party to have remote access to your computer if the caller's authenticity cannot be verified directly through the CE or BA.
- Do not trust unsolicited phone calls.
- Do not provide any personal information over the telephone.
- Do not download any unknown software or purchase online services.
- Verify the identity of the caller directly with the CE or BA, or with the company the caller claims to represent.
- Record the caller's information and report it to the CE or BA and to law enforcement.

Further, for those who suspect they are a victim of a tech support scam, immediately change passwords for all accounts including email passwords and online banking accounts; and conduct a scan for malware. In some cases, re-imaging the system would be the best option, to be sure that all malware has been removed.

A New Resource for Covered Entities and Business Associates: Better Business Bureau (BBB) Scam Tracker - Earlier this year, the Better Business Bureau launched a website that allows consumers to track scams that have been reported in their area. This is a free platform for information-sharing and awareness of scams in the United States and Canada. The website features a "heat map" that shows the number of scams reported in each area, based on area codes. Also, anyone can use the tracker feature "Report Scam" to provide details such as specific information about the scam; information about the scammer(s); information about the individual(s) scammed; and information about the individual reporting the scam.

There are multiple reportable scam types recognized by the BBB: phone scams, phishing emails, illegal business schemes, and fraud. Visit the BBB Scam Tracker website https://www.bbb.org/scamtracker/us for additional information.