U.S. Department of Homeland Security

United States Secret Service

October 5, 2016
Contact: (202) 406-5708

CYBER HYGIENE & CYBER SECURITY RECOMMENDATIONS

With Cyber Security Awareness Month on the horizon, the U.S. Secret Service would like to take this opportunity to remind private citizens and business owners using Point-Of-Sale systems of the importance of developing and practicing good cyber hygiene and provide some basic cyber security recommendations. Additionally, it is important to offer some brief discussion points and highlight current trends.

Recommendations for Protecting Your Personal Computer:

Maintain Complex Passwords: Develop lengthy and complex passwords. We strongly recommend that you use different passwords for social networking sites, email accounts and online banking sites. You should not use the same password for all of your respective devices and accounts.

Ensure Your Operating System Is Up-To-Date: Operating systems are usually configured to automatically update or at least prompt you that updates are available. You should not disable this feature. The majority of updates are released due to some type of security issue making it extremely important that you install the updates to ensure your computer has the latest protections known within the industry.

Ensure Remote Desktop Protocol (RDP) Is Disabled: Remote desktop software allows you or others not physically at the keyboard to access your computer over a network or the internet. This is very useful in terms of remote servicing of the computer by an authorized technician, but can also be exploited by hackers to take complete control of your computer and compromise your data. To check if RDP is enabled you should consult your Operating System User's Guide as operating systems vary.

Install and Update Antivirus/Antispyware Software: Viruses and other malicious software programs can infect your personal computer without your knowledge. Ensuring that antivirus

software from a reputable company is installed and set to update automatically will help protect your computer.

Secure Your Internet Browser and Browser Add-ons: Keep your browser(s) set to auto update and consider disabling JavaScript, Java and ActiveX controls when they are not in use. Active content on the internet has long been used to exploit browsers and transfer malware to computers.

Consider Using a Firewall: A firewall can help protect your computer from a variety of threats and is easy to use. For single computers, software firewalls are recommended and either come with your operating system or can be purchased. Set the firewall to the highest security level you think is appropriate keeping in mind that you can always scale back the security control if needed.

Carefully Scrutinize Email Attachments: It is good practice to never open or download an email attachment from someone you do not know or from someone that has rarely ever made contact with you. It is just as important to not open forwarded email attachments from someone you do know as he/she may have just unknowingly forwarded you an email attachment containing a virus or some other malicious software.

Password Protect Your Wi-Fi: Securing your wireless network with a strong password is essential. Consider naming your wireless network something innocuous. Using your last name or some other personally identifiable information to identify your home wireless network is inviting trouble.

Back-Up Your Important Data: Consider periodically backing up your important data. The important thing to remember is to store this data "off line", meaning transferring your important files to a storage device that you DETACH from your computer after you have copied all of your files.

Recommendations for Protecting Your Point-Of-Sale (POS) Terminal

Use Strong Passwords: For convenience, many companies fail to change the default password on their POS systems or vendor supplied equipment after installation. Cyber criminals can easily obtain these default passwords and gain access to your system. POS system passwords should be changed on a regular basis using unique account names and complex passwords. All passwords should be at least 8 characters long, contain a mix of upper and lower case letters, and include numbers and special characters. Finally, you can insist that the vendor use a unique password on equipment associated with your POS system, and that the vendor disable unnecessary accounts on all components associated with your system.

Restrict Access to the Internet: Computers used in a POS system should not be used for checking email or internet browsing. Using POS systems online for anything other than conducting POS-related activities can expose the POS system to security threats and create vulnerabilities.

Utilize Two-Factor Authentication: Many POS systems allow remote users to log into the system to service the POS system. Cyber criminals will exploit this remote access configuration to gain access to your network. Utilize two-factor authentication such as a password and SMS text code or a password and a security token to prevent unauthorized remote access.

Install a Firewall: A firewall is a hardware device or software that can prevent traffic from hackers, viruses, worms or other malware that is specifically designed to compromise a POS system.

Use Antivirus: Antivirus programs will recognize software that fits its definition of being malicious and attempt to restrict its access to a system. Ensure that it is continually updated and configured to quarantine and/or delete any detected file.

Update POS Software Applications: If POS system software is not updated / patched, it leaves your system vulnerable to cyber criminals who seek to exploit known software design flaws.

Access Control: We recommend that you physically inspect your POS terminals and associated devices on a daily basis. Ensure there is no unknown hardware attached to the terminal. Devices such as skimmers, skimmer overlays, hidden cameras, USB drives or other devices connected to the POS system can be easily identified after a physical inspection. Also, ensure there are no active USB ports or other media devices open on a POS terminal.

Third-Party Service Provider - Adequate Security: Merchants who engage the assistance of a third-party to oversee the installation and management of their POS system should ensure that the third-party service provider applies all aspects of cyber hygiene identified in this document. An excellent private resource to use as a guide for the third-party business operation model is contained within the PCI Data Security Standard (PCI DSS) – Information Supplement: "Third-party Security Assurance". For additional information regarding Third-Party Service Providers and PCI Data Security Standards, visit https://www.pcisecuritystandards.org.

If you suspect that your POS system has been compromised, contact the nearest local Secret Service Field Office http://www.secretservice.gov/investigation/#field for a listing of all Secret Service Electronic Crimes Task Forces.

Current Trends

Ransomware: In the past several months, the U.S. Secret Service has seen an increased number of individuals who have reported being a victim of ransomware. Ransomware is a type of malware that restricts access to infected computers and requires victims to pay a ransom in order to regain full access to their data. Ransomware is typically spread through spear phishing emails or by unknowingly visiting infected websites.

Business E-mail Compromise (BEC) & E-mail Account Compromise (EAC): In recent months, the U.S. Secret Service has noted a growing number of e-mail fraud schemes in which cyber criminals deceive financial institutions and their customers into conducting illegitimate wire transfers. This fraudulent scheme involves criminals compromising the e-mail accounts of company executives in order to trick the company in to facilitating fraudulent wire transfers. Once the funds have been successfully transferred, they may be transferred several more times through multiple institutions making it virtually impossible to recover the stolen funds. A BEC scheme targets a financial institution's commercial customer while an EAC scheme targets a victim's personal account.

For more information regarding this e-mail scheme visit the Financial Crimes Enforcement Network (FINCEN) website at
https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a003

If you feel that you have been a victim of a BEC or EAC scheme, or to report any other cyber related suspicious activity, contact the nearest local Secret Service Field Office http://www.secretservice.gov/investigation/#field for a listing of all Secret Service Electronic

Crimes Task Forces.