



Enterprise Information Security Office

Monthly Security Tips NEWSLETTER

December 2013

Volume 8, Issue 12

Cyber Hygiene with the Top 20 Critical Security Controls

From the Desk of Thomas D. Smith, Chief Information Security Officer

In this digital age, we rely on our computers and devices for so many aspects of our lives resulting in a need to be proactive and vigilant to protect against cyber threats. However, in order to be as secure as possible, we need to use good cyber hygiene – that is, making sure we are protecting and maintaining systems and devices appropriately and using cyber security best practices.

Many key best practices are outlined in the Top 20 Critical Security Controls, managed by the Council on Cyber Security. These Controls assist in mitigating the most prevalent vulnerabilities that often result in many of today's cyber security intrusions and incidents. The Center for Internet Security (CIS) provides free, PDF-formatted configuration guides (Benchmarks) that can be used to implement the Controls and improve cyber security.

Below are several best practice strategies for strengthening defenses. The numbers that follow each best practice are the related Control and the CIS Benchmark. The CIS Mitigation Strategies Crosswalk link below details a complete mapping of the Controls to Benchmarks.

Update Your Applications, Software, and Operating Systems

Even though you may be diligent in keeping your software up-to-date, you are still at risk from malware infections. Malware can infect your computer from a variety of different vectors, including compromised websites, malicious attachments in email, and infected thumb drives. This is why strong malware defenses are crucial. Anti-virus and anti-spyware will scan your files to see if there's any malware in the files. It may even tell you if you're about to download a potentially malicious file. Update your anti-virus software regularly. Keeping applications, software, and operating systems patched will help keep you more secure by providing you with the most recent and secure version.

Critical Security Control(s): [2](#), [3](#), [5](#)

Securely Configure Your Systems and Devices

The “out-of-the-box” configurations of many devices and system components are default settings that are often set for ease-of-use rather than security. This often results in vulnerabilities that offer easy targets for hackers to exploit, often using automated programs that scan for holes. To mitigate risk, systems and devices should be configured according to industry-accepted system hardening standards.

Critical Security Control(s): [3](#)

Secure Your Browser and Browser Add-ons

Cyber attackers search for programming errors and other flaws in web browsers and associated plug-ins in order to exploit them. These vulnerabilities, if successfully exploited, can give cyber criminals access – and sometimes control over – your computer system. To minimize these risks, keep your browser(s) updated and patched, and set to auto update. In addition, keep any programs (known as plug-ins) updated and patched, block pop-up windows, as this may help prevent malicious software from being downloaded to your computer, and consider disabling JavaScript, Java, and ActiveX controls when not being used. Activate these features only when necessary.

Critical Security Control(s): [2](#)

Back Up Your Data

Be sure to back up your important data so you can retrieve it if your computer fails. Most operating systems provide backup software designed to make the process easier. External hard drives and online backup services are two popular vehicles for backing up files. Remember to back up data at regular intervals and periodically review your backups to determine if all your data has been backed up accurately.

Critical Security Control(s): [8](#)

Secure Your Wireless Network

Before the days of wireless (Wi-Fi) home networks, it was rather easy to see who was linked into your home network; you could simply follow the wires. You wouldn't allow a stranger to connect to your wired network, so check to see who is connected to your wireless network. The first step is to lock down your wireless network with a strong password and encryption. This will prevent people who don't have the password from connecting to your network.

While there are fewer wires to follow, you can still follow some digital breadcrumbs to see who is connected to your network. Connect to your router (for more information refer to the manufacturer's user guide) to see who the clients (the connected devices) are. Are there more devices connected to your network than you expect? If there are some devices you don't recognize, change your security settings and passwords. Don't forget about your printers, many of which can connect to your network and are Wi-Fi enabled.

Critical Security Control(s): [7](#)

Protect Your Administrative Accounts

Administrator or "admin" accounts give a user more control over programs and settings for a computer than a typical user account. If an intruder accesses an admin account, he could potentially take over your computer. Non-administrator accounts, or guest accounts, can limit the ability of someone gaining unauthorized access. It is important to change the default password on your admin accounts and to always log on to your computer as a non-administrator or non-admin account.

Another aspect to protecting admin accounts is to change default passwords on your devices. Many of them are published on the Internet, so be sure to change them to something unique and strong. Default passwords are especially prevalent in routers, wireless access points and other networked devices.

Critical Security Control(s): [3](#), [12](#)

Use Firewalls

Many computer defaults are set for ease of use, which is convenient not only for us, but also for cyber criminals. Cyber criminals can use weak or unnecessary services as a first step to compromising your computer. Many computers and routers already come with a firewall built in to prevent malicious access to these services. It is recommended that you set the firewall to the securest level you think is appropriate: if this is a laptop you'll use for traveling and connecting to public networks, it is recommended that you choose the strictest level of security and only allow exceptions for services you need. You can always relax the controls if necessary.

Critical Security Control(s): [10](#)

For More Information:

- National Initiative for Cybersecurity Education Framework - <http://csrc.nist.gov/nice/framework/>
- Council on CyberSecurity - <http://www.counciloncybersecurity.org/>
- Center for Internet Security Benchmarks - <http://benchmarks.cisecurity.org/downloads/benchmarks/>
- CIS Mitigation Strategies Crosswalk - <http://benchmarks.cisecurity.org/downloads/crosswalk/>
- Twenty Security Critical Controls - <http://www.sans.org/critical-security-controls/>

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Brought to you by:

