Monthly Cybersecurity Newsletter

July 2019 Issue

NC DIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Maria Thompson

IRS "Security Six"

While the tax season has come and gone, the Internal Revenue Service (IRS) is urging tax professionals to review their cybersecurity practices. Being cautious of cybersecurity threats is an ongoing effort. Cybercriminals do not take a break regardless of the time of year, and neither should we. Digital thieves use stolen data from tax professionals to create fraudulent returns that are harder to detect.

To keep cybersecurity at the forefront, the IRS recently published a list of security protections they claim are critical to ensure tax professionals are protecting their systems and safeguarding sensitive taxpayer data. The list is the result of a joint effort by the Security Summit partners – the IRS, states and the tax industry – that is an effort to urge tax professionals to give their data safeguards a thorough review. Called the "Security Six" protections, this list is the first of a series of steps to improve the cybersecurity posture of tax professionals.

IRS Commissioner Chuck Rettig claims "these six steps are simple actions that anyone can take." Rettig also adds, "The important thing to remember is that every tax professional, whether a sole practitioner or a partner in a large firm, is a potential target for cybercriminals." While these security protections are primarily directed to tax professionals, they are so *essential* that they apply to *any computer user* and should be used to help reduce the risk of identity theft. So, what are these six essential security steps:

1. **Install and Maintain Anti-Virus Software:** Anti-virus (AV) software scans a computer's files or memory for certain patterns that may indicate the presence of malicious software (malware). It is important to not only have a reputable AV product installed, but to make sure it is up to date.

2. **Configure Firewalls:** Hardware and software firewalls help protect your computer against external threats by blocking traffic from certain suspicious locations or applications. It is important to remember that firewalls help protect you from malicious traffic, but not against malicious programs (malware).

3. **Enable Multi-Factor Authentication (MFA):** Multi-factor authentication helps by adding an additional layer of protection to the user's simple username and password credentials. With MFA, a thief may steal your username and password, but it is unlikely they will be able to access your system and data as they need another "factor", such as a mobile phone text or some biometric data (e.g. fingerprint).

4. **Routinely Backup Data:** Data should be frequently backed up to external sources in the event something bad happens to their systems. It is important to also enable encryption on the backed-up data so that it, too, is not at risk of exposure.

5. **Employ Full-Disk Encryption (FDE):** Users should consider full disk encryption, which transforms computer data into an unreadable format. This protects the data from an unauthorized person accessing the data. Drive encryption may be installed separately as a stand-alone product or it may come with the computer or storage device.

6. **Use Virtual Private Networks (VPNs):** If you must connect to or via unknown or risky networks, it is a good idea to establish an encrypted virtual private network (VPN) with a known reputable security vendor. VPNs allow for a more secure, encrypted "tunnel" to transmit data, so that your data is not at risk of being intercepted.

For more information, visit the IRS' "Security Six" protections page.

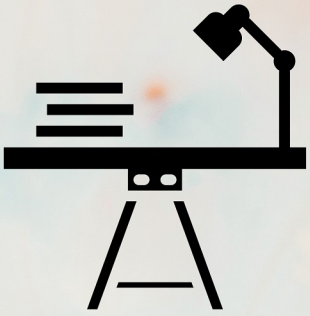
Firefox to Mark All HTTP pages "Not Secure"

Is the website you are visiting secure? For many, looking for the "padlock" icon in the address bar indicates whether the site is secure or not. Internet browser software are making it easier to determine this. Following in the footsteps of Google's Chrome browser, Mozilla's Firefox will soon begin marking all HTTP web pages as not secure. Previously, Firefox has shown "not secure" only on sites that contained forms or login fields. Starting with Firefox version 70, however, which is scheduled to be released in October 2019, Firefox will begin to show a "not secure" indicator for *all* HTTP websites visited in Firefox. Chrome has been using "not secure" labels on all HTTP websites since Chrome version 68, which was released in July 2018. According to one source, more than 80% of all internet pages are now served via HTTPS.

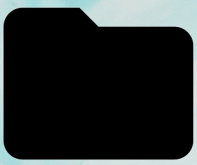
The "not secure" warning helps a person understand when the connection to a site is not secure. Non-HTTPS traffic is open to cyberattacks such as "man in the middle" attacks as cyber attackers attempt to intercept the data that is transmitted. It is important to realize, however, that the presence of a "secure" indicator on a web page does not mean the site is safe. Many cyber attackers utilize a secure connection to their sites in an attempt to lure individuals into a false sense of security and perpetuate a phishing scam or malware attack. What the "secure" indicator does mean is that any communication between the end user and the site should be protected from unauthorized access, such as usernames and passwords that are entered on a login page. In addition to alerting on non-secure sites, Mozilla also plans to incorporate other enhanced security features such as alerting users if their email addresses or passwords have been found in any reported data breaches.

SUPER SIMPLE STEPS TO SECURITY

STAY ALERT



KEEP A CLEAN DESK



ORGANIZE EVERYTHING

REPORT SECURITY INCIDENTS

ALWAYS FOLLOW POLICY

© The Security Awareness Company, LLC

CYBERSECURITY NEWSLETTERS

Security Awareness Newsletter: Monthly security awareness newsletter provided by KnowBe4 for all State employees.
***Note**: You must have a valid State employee O365 account.*

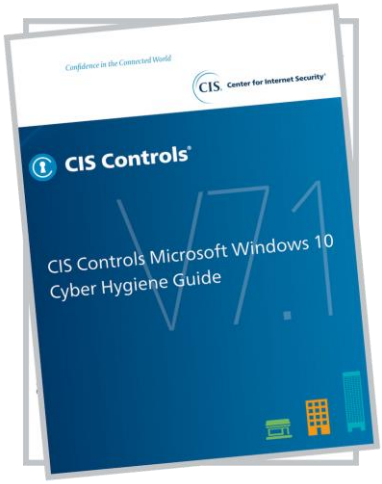
- https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News/2019

Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security (CIS). This month the newsletter covers ***Cleaning Out Your Old Data and Devices***.

- https://www.cisecurity.org/resources/?type=newsletter

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month's edition is titled ***Virtual Private Networks (VPNs).***

- https://www.sans.org/security-awareness-training/ouch-newsletter



The Center for Internet Security (CIS) has provided a new resource to help offer practical guidance on "cyber hygiene" to Windows 10 users. Cyber hygiene can be considered as a set of baseline cybersecurity protections that help to secure an organization. CIS has developed cybersecurity best practices, called the CIS Controls, that mitigate the most common attacks against systems and networks and improve cyber hygiene. The CIS Controls were developed by a community of Information Technology (IT) experts who have applied their first-hand experience to create industry accepted security best practices. The experts who developed the CIS Controls come from a wide range of sectors including retail, healthcare, education, government, defense, and others.

This new resource is called CIS Controls® Microsoft® Windows® 10 Cyber Hygiene Guide. CIS developed the guide to make cybersecurity basics for Microsoft Windows 10 easier to follow. The guide provides practical step-by-step assistance for securing computers running on Windows 10 without the need for advanced technical knowledge. It is targeted to organizations concerned with stopping theft of company information, website defacement, phishing attacks, ransomware, and data loss! By implementing the CIS Controls, an organization can significantly reduce their risk of cyber attack by addressing the *most common security practices*, such as regular patching and secure configurations.

To read more about the guide or to download it, visit the CIS Blog site. There is no form needed to complete to download the guide.

KnowBe4, a cybersecurity training and awareness partner to the the State of NC, has provided a free online webinar called "**Empowering Your Human Firewall**". In this webinar, Perry Carpenter, Chief Evangelist and Strategy Officer for KnowBe4, dives into ideas like how to use "Trojan Horses for the Mind," how to leverage social dynamics to drive behavior and shape culture, and unveils some exciting new behavior models that will help you stop the bad guys in their tracks. Click here to view this webinar.

Penetration Testing: From a Hacker's Perspective

Coalfire, a PCI compliance validation services vendor, will be hosting a 1-hour webinar for the State of NC's merchant community on **September 3, 2019 at 10:00am**. Information about the webinar is below.

Date/Time: 9/3/2019 10:00am-11:00am EST

Webinar Title: Penetration Testing: From a Hacker's Perspective

Webinar Description: Luke McOmie will discuss the importance of pentesting, stories from past assessments, and will step through the methodology and process of how Coalfire conducts blended threat, real world, impact and risk-based assessments (Red Teaming) and the importance it plays in securing modern businesses.

Speaker Bio: Luke McOmie is a senior security leader with 20+ years of experience guiding security professionals within Fortune 100 enterprises to start ups, federal agencies, and both private and public-sector organizations to better secure their organizations. Highly skilled in developing and executing enterprise security strategies, leading technical and tactical programs, with the goal of helping organizations understand their security challenges and mitigating the risks that threaten the modern business and operating environment. Luke has directed research groups, labs teams, risk and compliance programs, and red teams.

Please join the webinar via https://global.gotomeeting.com/join/694641885.

You can also dial in using your phone.

United States: +1 (571) 317-3116
Access Code: 694-641-885

- **September 1** – Agency Compliance Reports Due
- **September 2** – Labor Day
- **October** – National Cybersecurity Awareness Month
- **October 10-11** – NC Cybersecurity Symposium