August 2016
Volume 11, Issue 8

Back to School

From the Desk of Thomas F. Duffy, Chair, MS-ISAC

It feels like summer just began, and we hate to say it, but the start of another school year is right around the corner. It's time to purchase school books, pencils and pens, and a stash of Ramen Noodles for the semester. On the list may also be a new computer, laptop, or tablet computer. While students are getting back into the swing of doing homework, researching school projects, and focused on getting good grades, but also need to be aware of malware, phishing schemes, and safe computing practices.

Tips to stay safe this school year

Malicious cyber activity affects students in a variety of ways, ranging from malware and scams to cyber bullying. Fortunately, there are a few simple steps you can take to keep you, your kids, and your devices protected from the latest threats. Here are some cybersecurity tips for staying safe for the new school year:

- Keep Software Up-to-Date. Be sure to keep the operating system, browser software, and apps fully updated with patches. Even new machines can have out-of-date software that leaves you at risk. Operating systems and applications are constantly being updated to fix bugs and address security issues. You should use automatic updates to ensure you're using the most secure version of the software that is available. Also, review the privacy settings - when an app is updated, it may change your settings!
- Configure Your Device and Apps with Security in Mind. The "out-of-the-box" configurations of many devices and apps are default settings often geared more toward ease-of-use than security or protecting your information. Enable security settings on your device, and as you install software and apps, pay particular attention to those that control information sharing.
- Malware Protection. Make sure to have antivirus with anti-phishing support installed on all devices (desktops, laptops, tablets, etc.). Set it to update automatically and run virus scans at least once a week. Since malware today is increasingly sophisticated and can avoid detection by antivirus software, also consider installing script-blocking and/or ad-blocking browser plugins.
- Consider Comprehensive Internet Security. Consider using a comprehensive Internet security software in order to better keep your device safe. Most Internet security software suites offer parental controls, which are great for managing applications that can be downloaded and the time spent on the device, while making sure students are communicating with friends on social networks in a safe way. Be sure to have and turn on personal firewall software.
- Practice Safe Computer Usage. Use trusted apps and only browse to trusted websites. Malware is often hidden in apps that trick you into downloading them or in fake websites that lure you in with interesting pictures or stories! Make sure everyone who uses the device takes the same precautions.
- Think Before Sharing. It's easy to over share online. Be careful about divulging personal information –

like school names, team names, home addresses, and telephone numbers. Have your kids use safe search tools such as Google's safesearchkids.com.

- **Be a Smart Network User.** Don't access personal or financial information over unsecured public WiFi networks such as the free WiFi in coffee shops, bookstores, hotels, and schools, as this data can be easily "sniffed" (a.k.a. viewed) by others. Instead, consider using your smartphone's more secure cellular signal to surf the Web, and if you have other devices, "tether" them to your phone instead of using an open and unsecure WiFi.
- **Be on Guard for Phishing.** Don't open email attachments from untrusted sources. You may be expecting emails from group members or teachers, but use caution when opening any attachments. If you are not expecting an email or it just doesn't look right, don't open it. It could be a phishing attempt.
- **Use Strong Passwords.** To ensure a strong password, make sure you use a complex and unique password for each account/system. Use passwords that are at least 10 characters long, and contain upper and lowercase letters, numbers and symbols. For more information on how to create strong, unique password see the MS-ISAC Security Primer at: https://msisac.cisecurity.org/whitepaper/documents/Security%20Primer%20-%20Securing%20Login%20Credentials.pdf
- **Guard Against Physical Access.** A key problem for students continues to be the general lack of privacy and personal space they have at school. Whether it's a shared living space, crowded workspace, or the general communal environment of a college campus, they're constantly exposing their devices to access by others. Be aware of your surroundings and keep your computing devices with you or locked in a safe place.
- **Backup Your Data.** Saving important data is important given the growing risk of "ransomware" infections. Ransomware is a type of malware that locks up a person's files until the victim pays a ransom to the hacker. It is prudent to back up often, using both a physical storage device like a flash drive or external hard drive and a cloud-based account.
- **Don't Jailbreak/Root Your Device.** Jailbreaking a device is when you gain "root" access to the device, which means that you disable the manufacturer and operating system protections so that you can access areas you were not intended to have access to. This access can allow you to have greater functionality but also reduces the security on the device, making it more likely that you will be infected with malware. Jailbreaking your device puts you at a greater risk of getting hacked, and makes the device more susceptible to malware, malicious apps and sensitive information disclosure. It is best not to jailbreak your devices.

Provided By:

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™

STOP | THINK CONNECT™