Cybersecurity Tools:

Your Guide to a **Safe** School Year

Office of Information Technology
Division of Information Security
SEPTEMBER 2023

With the back- to-school season in full swing, the threat of cyberattacks is on the rise. As students increasingly rely on online learning systems, video conferencing apps, and research through search engines like Google, they are more likely to fall victim to phishing scams. It is important that parents and students alike remain mindful of the risks, as cybersecurity breaches can have long-lasting consequences to their privacy and safety. Here are some cybersecurity tips and tools for both students and parents to use throughout the school year to ensure their online safety:

For K-12 Students:

Educate your children on cybersecurity matters
Begin teaching your children about online safety as soon as soon as they begin using digital devices. Age- appropriate discussions and lessons should start as early as preschool. Lead by example by practicing good cybersecurity habits and protecting your child's phone with a lock screen. Teach your child not to talk to strangers online or offline and not to leave their devices unattended. Teach them to never download apps and software without an adult to supervise them. Conduct regular check-ins to reinforce the cybersecurity lessons and ensure that they understand the information and feel comfortable voicing their concerns. There are also a plethora of Kid- safe browsers and search sites. Here are a few to get started: Kid info, Kiddle, Zilladog, and FactMonster.

Avoid oversharing on social media
Always use discretion when sharing online, because your social media presence represents your online identity. Parents should avoid disclosing personal information on social media platforms, such as their child's name, school, or school-related photos. Posting adorable back-to-school photos that can accidentally expose school uniforms, home addresses, or license plate numbers can also expose children to online risks. When sharing photos of your child, remember to limit access to trusted close family and friends. Also, educate your child on the importance of not sharing personal information and encourage them to connect only with people they know in real life.

Make use of the parental controls and privacy settings
Set strict age-appropriate parental controls and monitoring tools on your child's devices when necessary. Always set controls over who can see your posts and your children's information. Research all platforms because they may collect personal information or have suspicious privacy practices. Review and adjust your privacy settings on social media platforms and gaming apps regularly.

Stay up to date on important cybersecurity matters regarding your child's school and national events
Stay informed about the latest cybersecurity threats and trends so that you can provide guidance to your children. Cybersecurity matters that could eventually affect you or your child on a local level can begin nationally. Parents can stay current on cybersecurity matters by visiting trusted websites such as Stay Safe Online, Cybersecurity Awareness Program Parent and Educator Resources | CISA, local and national news sources.

Ensure all webcams are covered when they are not in use.
When not in use, cover any webcams to avoid spying and unwanted access and to ensure your privacy. Remember to turn off the microphone so that apps cannot use the webcam while your device is in use. Many devices allow you to set permissions for each application you have loaded using the device's settings function.

Say No to Cyberbullying
Bullying occurs not only in school; it can also occurs outside of school in the form of cyberbullying. Communication is an excellent tool that parents can use to prevent or stop cyberbullying. Build trust with your child by regularly discussing the negative impacts and repercussions of cyberbullying such as causing harm to others and, in some instances, breaking the law. Encourage your children not to retaliate or respond to cyberbullying, because doing so will only intensify the situation. Parents can prevent cyberbullying by monitoring their children's devices, becoming familiar with their social media profiles, blocking the bully and reporting the incidents to the appropriate authorities when necessary. Additionally, provide support to your child by sharing your own childhood experiences and how you overcame any challenges.

For College Students:

Protect your passwords and use two- factor authentication
The best way to practice online security is to choose a strong password that has a unique combination of special characters, letters, and numbers, and to consider using a password manager to store passwords. By using two- factor authentication (2FA), or multi-factor authentication (MFA), you add an extra layer of security to your online accounts in the event a hacker can accurately guess your passwords.

Do not respond to suspicious messages
Be caution of emails, texts, and phone calls that request personal information or require "immediate action." If you receive an email with an offer that sounds too good be true, it probably is. Never click

on suspicious links or download attachments from unknown sources. Some known source may not be who they claim to be, such as a family member requesting an immediate transfer of money. Report any suspicious messages or cybersecurity incidents to your department immediately. If you receive a suspicious message on your personal account report it to Cybersecurity and Infrastructure Security Agency, Federal Trade Commission, and FBI Internet Crime Complaint Center.

Limit activities on public Wi-Fi and avoid using free charging stations
When on campus, always use the school's secure Wi-Fi network, and when off campus or traveling, consider using a virtual private network (VPN) to get secure internet access. Avoid using unsecured public Wi-Fi networks to shop online, access online banking, access personal information, or visit other sensitive websites. Consider purchasing a personal hotspot to use while on vacation, field trips, or a study sessions at the coffee shop for an extra layer of protection. Avoid using free charging stations at hotels, amusement parks, airports or shopping centers. Hackers can use public USB ports to install malware and monitoring software on devices. Always use your personal charger and USB cord, and connect directly to an electrical outlet.

Keep apps and software up to date
Outdated software can be a security risk, making your device vulnerable to cybersecurity attacks. To minimize the risk of cybersecurity attacks, set up automatic updates for all of your devices and restart them on a regular basis to complete the updates. Think of it as giving them a regular spa day! Just like you'd backup your favorite photos, make sure to back up your device's data. It's your safety net against any unexpected digital mishaps or sneaky cyberattacks. Stay updated, stay safe!

Be aware of your surroundings
Be cautious when accessing websites, downloading files, responding to emails, or entering sensitive information in public places. To prevent hackers from shoulder surfing to steal your information, consider using a privacy screen protector on your devices. When talking on the phone or thorough your device, use discretion and a headset when discussing sensitive information. Maintain a comfortable distance from others when using your devices, especially in crowded spaces. Never leave your device unattended!

Be a good online citizen
When speaking online, especially at school and in professional settings, always be respectful and mindful. Avoid sharing false, harmful, or offensive information online. Always consider the potential consequences of your online actions before posting or sharing content. In the event that you encounter cyberbullying or witness abusive behavior online, report it to the platform administrators. If it occurs at school, also report it to your college or university's administration.

By following these cybersecurity tips, you can have a safe and productive school year. Keep in mind that your online safety is just as important as your physical safety!

For questions, please contact cybersecurity@ihs.gov.
NOTE: *Products mentioned in this document are for informational purposes only and do not signify an endorsement.*