Cybersecurity and K-12
Safe Summer Break

Office of Information Technology
Division of Information Security
JUNE 2024

As the school summer break sets in, enthusiasm starts growing over the freedom from routines and rigid schedules. Students easily turn their attention from school work to online amusement, gaming, social apps, video conferencing with their peers, and web surfing. Though summer break is generally thought of as time off, vacation, and fun time, the increased periods K-12 students spend online is a time to be more vigilant about cybersecurity, not less. Online privacy and safety best practices take center stage for students, parents, and local school communities during a summer break, and it is a time to revisit a few practical cybersecurity steps for a secure and fun-filled digital summer surfing.

Stay Cybersecurity Trained

Even if students have developed safe and steady cybersecurity habits during the school year, the start of the summer break may be a good time to take a **cybersecurity refresher tutorial** or attend a **cybersecurity summer camp**. Taking an age- and grade-level-appropriate course to safeguard online privacy and digital security is a good way to start the summer break. Cybersecurity resources found on secure sites like the FBI-SOS Cyber Surf Island, or FTC's Protecting Kids Online site offer ample tutorials and summer camp activities that for K-12 reinforce a culture of security, raise awareness that online risks and vulnerabilities are ongoing, increasing, and teach cybersecurity vigilance and digital safety.

Basic Safe Cybersecurity Habits

Since online safety is not seasonally limited, **safe digital practices** apply during the summer break as much as during the school year, if not more. For example, no sharing of digital devices, using a lock screen for all devices, not posting personal information, especially photos and personal information on social media platforms (a challenge for school-age children that needs steady parental supervision), avoiding random downloading of apps and software, avoiding online conversations and forming friendships with strangers – all remain safe online practices year-round.

For parents, repeating and reinforcing conversations, especially with their younger K-12 children, about **what personal information is, why not to share it, and why personal photo sharing may be dangerous**, is a continued effort to secure their children's privacy and safety, online and offline. Both students and their parents (who must lead by example in online safety) should practice security steps that protect people, devices, apps, and data no matter where and when they are located.

A **digital device lock screen** should be a security minimum. K-12 students should learn that strong passwords for all laptops, tablets, and smartphones must be a standard practice, and never leave any devices unattended in public places. Students need to be taught not to share their **digital devices or passwords**, no matter how tempted they may be by their peers. The **no device sharing** may be a huge challenge to school-age students since they tend to share a sense of comradery and group belonging. During summer break especially, parents should keep account of their child's devices and periodically talk with them about the reasons behind no device sharing matters. If a child begins to understand that cybersecurity safety is a mindset as much as a practice, then a win-win outcome may be expected.

Keeping their school-age children safe during summer break tasks the parents with more supervision responsibility than throughout the school year. Parents can find many resources on sites like the Cybersecurity and Infrastructure Security Agency, Federal Trade Commission, National Cybersecurity Alliance, and a long list of local community-based resources in cybersecurity and K-12 education. These trusted government sites have plenty of online safety awareness, tools, practical tips, and instructions for parents, K-12 students, college students, and the wider public.

Keep Your Software Secure

Various malware can lurk in several ways on students' devices through email attachments, websites, ads, social media sites, gaming apps, proxy sites, and faulty software. Installing security software on students' devices that can daily identify and filter new sites, and protect students from emerging threats is a sound security measure. Software like Qustodio Parental Control, Norton Family, Net Nanny, or just Google Parental Control settings offer various ways and levels of parental supervision and intervention in protecting their children's electronic devices. Installing protective software on children's devices that alerts children and parents maximizes parental control, allows regular parental check-ins, and ensures security threats are blocked and categorized as soon as possible. When a child tries to visit sites that pose a security risk, security software blocks the screen explaining why access was denied and alerts the parent. Security software and steady parental control settings on their children's devices protect the devices and educate children about cybersecurity while keeping them safe.

Ensure Network Safety

Using a safe network while traveling locally, nationally, or internationally in the summertime is an added layer of online safety. During summer travels, many internet users will connect to public Wi-Fi hotspots at airports, hotels, cafes, restaurants, bus stops, and other public places. Sadly, such public places have become hacker-prone and are used to infiltrate connected devices.

Public Wi-Fi hotspots are difficult to secure because anyone can connect to them without authentication. In that way, they stay public and available but are also cyber threat hotbeds open to hackers, fake wi-fi networks, eavesdropping, man-in-the-middle attacks, and domain name spoofing (DNS) as the most widespread. When using a public network, always check for **HTTPS**, a website URL that contains https:// at the beginning of the address, often with a padlock icon on some browsers, which encrypts all the data sent back and forth between a web browser and the website. Safe URLs use Secure Sockets Layer (SSL) encryption to scramble the contents of your data before it leaves your device, making it impossible for hackers in the WI-FI to decipher your data.

Whenever possible, use a Virtual Private Network (**VPN**), a service that encrypts all devices' internet traffic and routes it through an intermediary server where the user is located. Anyone who tries to intercept online traffic between the smartphone or laptop and the VPN server won't be able to decipher its contents, including Wi-Fi hackers. The data is encrypted and headed for a VPN server, but not for an actual website. There are a variety of VPNs, but the safest ones are paid subscription services, well worth investing in.

Beware of Cyberbullying

Because it is not a matter of "if" but "when" a school-age child will face some kind of online or offline bullying, parents should be ready to talk about this topic with their children. Many perilous consequences of cyberbullying among school-age children can be prevented through parental intervention, especially by monitoring their devices, social platforms, and apps. If a parent finds out their child is a bullying aggressor, their intervention is just as needed as when they discover that their child is subject to cyberbullying, and bullying in general. When reaching for help there are ample national anti-cyberbullying hotlines, and resources on government sites like schoolsafety.gov, stopbullying.gov, and other related sites. Reporting bullying to the local school administration can help when legal protection is needed, regardless if bullying or cyberbullying occurred during the summer break or a school year.

Honest, open, and continuous communication with school-age children is the first step in making them feel safe and open up about issues, emotional threats, or abuses they come across, online and offline.

NOTE: *The links and products in this document are for informational purposes only and do not signify an endorsement.*

Please contact cybersecurity@ihs.gov with any questions or comments about this newsletter.