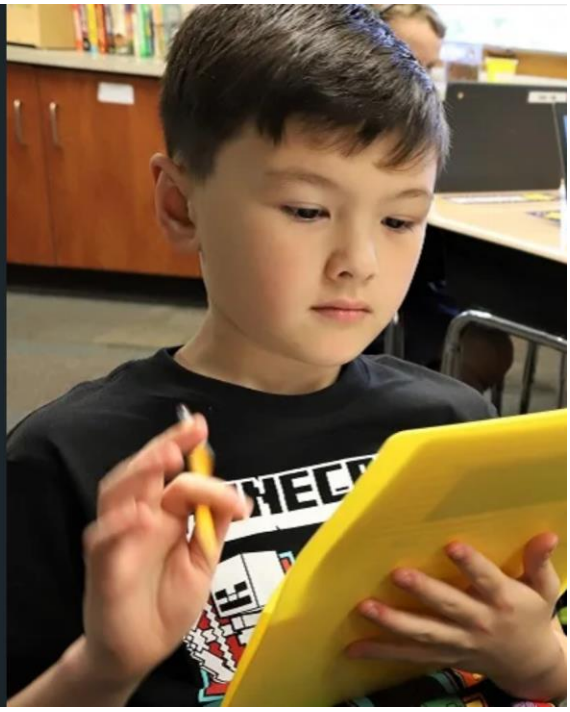
Cybersecurity for Education Toolkit 2.0

Cybersafe Best Practices, Resources & Tips for Indiana's School Communities



Cybersecurity for Education Toolkit 2.0

Developed by the Indiana Executive Council on Cybersecurity
August 2023

Table of Contents

HOW TO USE THIS TOOLKIT

Regardless of the important role you play in educating our children and young adults, this *Cybersecurity for Education Toolkit 2.0* is designed for you.

Whether you are a superintendent, administrator, teacher, or staff member, we encourage you to use these materials – and share them with your colleagues, students, and others in your school community – as a turnkey resource; saving you precious time as you focus on the rapidly increasing challenges that are taking place in education as the school year gets underway.

Likewise, if you're a parent, concerned citizen or a school board member, we know that the quality of education is an important factor in the quality of life for a community, whether you live in a large city, suburb, or small town. Cybersecurity is a part of our daily life, whether we're at home, at work, or at school. That's why this Toolkit is also for you to use because of the role you play in your school community.

In fact, we have created the toolkit as a PDF that can easily be saved as a Word Document that will enable you to cut and paste, copy and/or repurpose all the articles, images, and social media posts in the *Toolkit 2.0* as needed.

In the fall of 2020, we created the Cybersecurity for Education Toolkit. Within the past two years, a lot has happened with education and with cybersecurity. Because of that, we're pleased to share with you an updated version for you to use and share with others.

In addition to these materials, we invite you to visit our Cybersecurity Hub Page located on the website of the State of Indiana at www.in.gov/cybersecurity. There, you will find even more resources – updated frequently -- that will help you with everything from tips on maintaining good cyber hygiene to the steps you should take if you are the victim of a cybercrime.

Developed by the members of the Indiana Executive Council on Cybersecurity (IECC) including the Indiana Department of Education, as well as our federal partners with the Cybersecurity Infrastructure and Security Agency (CISA) and the U.S. Department of Homeland Security, our Indiana Cyber Hub website features sections for Education, Teachers, Students and much more!

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Dear School Community Member:

As education continues to be empowered by emerging technologies and devices across Indiana, cybersecurity continues to be critical to achieving a higher level of education, safely and securely.

To help our school communities continue to be strong and protected while staying connected, the Indiana Executive Council on Cybersecurity (IECC) along with the Indiana Department of Education has developed this updated *Cybersecurity for Education Toolkit 2.0* for everyone, including:

- Superintendents and school board members
- Teachers, staff, and administrators
- Students of all ages and their families
- Every person who lives in our school communities

Our toolkit is designed to be easy-to-understand resource, complete with tips and helpful information to make sure you are cybersafe and practicing good habits that will help:

- Students protect their identity and schoolwork.
- Teachers and staff manage their lesson plans and keep safe their student's data, including their grades and assignments.
- Administrators protect their students and schools.
- Members of the public can engage and communicate with schools and educators.

Most importantly, this guide is intended to provide you with resources to get started and more information about improving your educational institution's cybersecurity posture. You are also welcome to visit the website for the Indiana Department of Education, We have included a selection of blogs and brief bylined articles – from a variety of trusted sources – that the IECC encourages you to share with teachers, families, and your communities.

You are also welcome to visit Indiana's Cybersecurity Hub Page (www.in.gov/cybersecurity) for even more resources you'll find valuable -- inside and outside of the classroom. We look forward to your input on this toolkit as we continue updating the content and that it will serve as a helpful guide for being safe when you and our children are online.

Sincerely,

Chetrice L. Mosley-Romero
Cybersecurity State Coordinator, Indiana
Cybersecurity and Infrastructure Security Agency (CISA)
Chetrice.Romero@cisa.dhs.gov

Dr. John Keller
CTO, Indiana Department of Education
jkeller@doe.in.gov

David Ayers, Program Communications Manager
Indiana Executive Council on Cybersecurity (IECC)
dayers@iot.in.gov

PROTECT YOUR SCHOOL

Article 1:
The Importance of Cybersecurity to Your School's Infrastructure

As a school superintendent, together with your administrators, you are tasked with the day-to-day responsibility of protecting your schools, students, teachers, and staff on behalf of the community.

And, in collaboration with the members of your school board, you are always working proactively to adopt policies to accelerate learning for all students in an environment that is safe and secure. Improving your **cybersecurity posture is a key step in this process**.

There is a great deal of resources out there to help guide your school's approach to being cyber safe for everything from your technical infrastructure to the security of your student's personal data, as well as your curriculum and the lesson plans created by your teachers and staff.

Here are some great resources to start assessing and improving your cybersecurity posture:

- Indiana Cybersecurity Hub (https://www.in.gov/cybersecurity/)
- IDOE School Cybersecurity Moodle Community (https://moodle.doe.in.gov/course/view.php?id=355)
- CISA Shields Up (https://www.cisa.gov/shields-up)
- CISA.gov - Partnering to Safeguard K-12 Organizations from Cybersecurity Threats report and toolkit
- MS-ISAC (https://www.cisecurity.org/ms_isac)
- K12 Six (https://www.k12six.org/)

Administrators, teachers, and students should follow these four tips from CISA to keep anyone who relies upon computers in your school district safe, including:

- Enable Multi-Factor Authentication - Adversaries are increasingly capable of phishing or harvesting passwords to gain unauthorized access to information systems. Multi-factor authentication (MFA) is a layered approach to securing online accounts and the data they contain that requires users to provide two or more authenticators to verify their identity. Users who enable MFA are significantly less likely to be hacked because even if a password is compromised, unauthorized users will not be able to meet the second authentication requirement, stopping them from gaining access to online systems and data.

- Use Strong Passwords - Passwords are the most common means of authentication, and many systems have been successfully breached because of non-secure and inadequate passwords. Tips for creating a strong password include applying a combination of varying character types; avoiding common words, numerical patterns, and personal information; and using the longest password or passphrase permissible. School staff can also consider using a password manager program, which stores randomly generated passwords across multiple accounts and is only accessible with a master password.

- Recognize and Report Phishing - Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. Common signs of a phishing attempt include suspicious sender addresses, generic greetings and signatures, spoofed hyperlinks and websites, misspellings, poor grammar and sentence structure, and suspicious attachments. Schools can reduce the risk of phishing emails by enabling strong spam filters and implementing a cybersecurity awareness and training program to educate students and staff on the ways to recognize and report suspicious activity.

- Update Your Software - Outdated software can contain vulnerabilities that can be exploited by threat actors. When vendors become aware of vulnerabilities in their products, they often issue patches. Schools and districts should install updates as soon as possible to protect their systems, as well as enable automatic software updates whenever possible.

It's also a good idea to raise awareness with your students on why being cybersafe is important and use social media to disseminate information and encourage students, faculty, and staff to learn more about staying safe online visit www.in.gov/cyber, staysafeonline.org, www.commonsense.org/education/digital-citizenship, stopthinkconnect.org and CISA's "Stop Ransomware" K-12 Resources.

Article 2:
Collaborate with Your School Board Members About Cybersecurity

For school board members, adopting acceptable/responsible use policies and other important standards related to the use of technology, is at the heart of your responsibilities to the public and the larger school community.

It is important to know that cybersecurity is associated with risks that can catch even the most experienced board members off guard. Cybersecurity treats should be treated like any other kind of risk for your school district. Because of that, the same amount of detail and preparation associated with mitigating financial risks should be implemented when preparing for, conducting, and participating in school board cybersecurity training.

According to *Diligent Insights*, to begin to develop and establish cybersecurity training for your school board, there are core steps that need to be explored and addressed.

Diligent Insights and *K-12 Cyber Secure* highly recommends your school board members collaborate on adopting cybersafe and acceptable use policies for your school community, which include the following:

1. Note any cyber incidents that have occurred in your district the last few years.
2. Identify cybersecurity risks and issues that the board and district may face.
3. Determine who will be involved in the board's cybersecurity training.
4. Develop a plan of action regarding cybersecurity in your school district.
5. Identify how to measure the sufficiency and effectiveness of your district's cybersecurity program.
6. Determine how much your IT budget is being spent on cybersecurity-related activities and risk management.

For more information, visit:

- Core Steps for Establishing Board Cybersecurity Training https://insights.diligent.com/cybersecurity-public-education/core-steps-establishing-board-cybersecurity-training.
- K-12 Cybersecurity: Role of the School Board https://k12cybersecure.com/blog/k-12-cybersecurity-the-role-of-the-school-board/
- Campus Safety Magazine Webinar -- Here's How an Indiana School District Used Integrated Access Control to Bolster Security https://www.campussafetymagazine.com/webcast/heres-how-an-indiana-school-district-used-integrated-access-control-to-bolster-security/
- Protecting Our Future: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats (CISA)
- Indiana Cyber Hub – Education Resources – https://www.in.gov/cybersecurity/education/

PROTECT YOUR TEACHERS

PLEASE SHARE THE BELOW ARTICLES WITH YOUR TEACHERS VIA NEWSLETTERS, EMAIL, MESSAGE FROM THE SUPERINTENDENT, MESSAGE FROM THE PRINCIPAL, STAFF MEETING, ETC. THROUGHOUT THE SCHOOL YEAR.

Article 1:

Keeping Your Classroom Secure Online

For your dedicated teachers and staff, practicing good cyber hygiene is an important part of the school day and, especially so, when working from home or conducting class remotely.

There are four important steps to keep in mind:

- Beware of Phishing Scams - Use caution when opening emails even those that appear to be from trusted sources or from senders who ask you to provide sensitive information – i.e., share student data or requests.
- Encrypt Your Data (both for yourself and your students)
- Secure Your Devices from Physical Attacks - Use a VPN (Virtual Private Network) and Multi-Factor Authentication to provide the greater measure of protection when it is necessary to work from home or out-of-school setting.
- Follow Your School's Cybersecurity Protocols - Work with your IT staff on system updates/Acceptable Use Policies

Throughout a school district, everyone can benefit from a reminder, to be vigilant when it comes to practicing good habits while working online, including making sure to always:

- Keep an updated machine. Having the latest security software, web browser and operating systems is the best defense against viruses, malware, and other online threats.
- Protect ALL devices that connect to the Internet – It's not just computers, smartphones, and other web-enabled devices, it is crucial to provide cybersecurity for your school system's critical infrastructure systems, installed on servers that are separate from those used to store student data and your school corporation's financial systems.

- **Plug and Scan:** Be aware as USBs and other external devices can be infected by viruses and malware. Work closely with your IT staff to use your system's security software to scan them (if permissible) or follow your school's policy on removable media.
- **Back It Up:** Protect your valuable work, music, photos, and other digital information by making electronic copies of all information files and storing them safely.

For additional resources, you can also visit https://www.in.gov/cybersecurity/education/teachers/.

Article 2:
Passwords Matter

Teachers and staff are uniquely positioned to educate their students about good cyber hygiene as part of their everyday assignments and in-class interaction.

An area that is important to teach kids from a young age, especially with the many education apps they use is password management.

Here are basic tips teachers can use not only for themselves, but can share with their students when dealing with passwords:

- The first step is to **create complex passwords**. A strong password should be a mixture of upper and lowercase letters and include numbers and symbols, as this will make it less likely to be guessed by cybercriminals. You can use tools like a password meter, which calculate how difficult or easy it would be to guess or hack your password and aim for a high score for each password you create.

- Create **unique passwords for each online account**. For instance, the password for your personal Facebook account should be different from that of your personal email, which in turn should be different from the one you use to access the learning portal at school. This means that if someone guesses or hacks one password, they won't be able to access all of your accounts.

- Try to **change your passwords frequently**. It is recommended to do this at least twice a year, but once every three months is even better and more secure, especially since the sheer number of online accounts accessed at school is so high.

- Creating complex and unique passwords and changing them continuously is a great memory exercise.

- But if it turns out to be too difficult, **try using a password manager** to generate and store your passwords on your device or browser. A password manager uses a special

database to create and store strong passwords, so you don't have to remember them. But you do have to be careful with that one master password.

- While using public computers or other public devices and networks, **never allow the public computer to remember or store your password**. This can open the door for others to sign in after you and access your online profiles and any other personal information that might have been saved.

- Finally, take advantage of **two-factor verification/authentication** when it is available. These systems typically require you to enter both your password and a special code sent to your phone or email. This type of authentication offers the best protection for those of your accounts that hold personal and sensitive information about you.

For additional resources, you can also visit https://www.in.gov/cybersecurity/education/teachers/.

Article 3:
Don't Fall For the PHISH!

According to the U. S. Department of Homeland Security, phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by manipulating them into providing personal information to the attacker.

There are several ways online phishing scams can happen. Some are through emails, SMS text messages, social media, and even fake tech support phone calls/voicemails.

The best way to avoid these scams is to ***not*** take action based on the email – don't text the number back, don't answer phone calls when you don't recognize the number, and never give your personal information out via email to someone you don't recognize from your contact list. If you keep being targeted by the same number or email, block them, or talk to your cell phone provider about blocking the number from reaching your phone.

But before you can decide not to interact with phishing scams you need to be able to recognize them. Here are a few signs that should make you suspicious:

- **Unfamiliar sources.** If you've never interacted with this person or company before, be wary.

- **Odd email addresses.** Anyone can create a Gmail or Yahoo email account, but an established company will have its own email system, such as: cocacola@yahoo.ph versus name.surname@coca-cola.com.
- **Too many recipients of the same message.** You should be the sole recipient of the email, or at least to know the other few people addressed in case you're not.
- **Direct requests for personal information or money.** Social Security numbers, bank account information or other passwords should not be shared with strangers just because they asked.
- **Text riddled with errors.** Cybercriminals send badly written messages to increase their chances — if grammar and spelling errors don't ring any alarm, someone is more likely to hand over the required personal information.
- **Too good to be true offers.** Murphy's law is not a law for nothing. If something seems unlikely, unrealistic, or too good to be true, then it probably is.
- **Strange attachments.** An attachment should be necessary and related to the message. If not, or if the extension is odd (.exe instead of .docx), it's better to not open it.

Article 4:
Use Anti-Virus Protection

Malware, or "malicious software," is an umbrella term that describes any malicious program or code that is harmful to systems. It includes computer viruses, ransomware, adware, spyware, scareware, worms and more. The damages made by malware vary from making your device more difficult to use by slowing down its functions, to more serious consequences, like controlling your device or stealing your data.

One rather famous way of malware spreading throughout a school is the use of infected removable drives. As Microsoft's Windows Security noted, "many worms spread by infecting removable drives such as USB flash drives or external hard drives. The malware can be automatically installed when you connect the infected drive to your PC. Some worms can also spread by infecting PCs connected to the same network." Working directly in the cloud is a better option, as long as the cloud is in its turn protected.

The most important thing you must do is to ***install antivirus software on all your devices*** to make sure you're protected no matter what you're using. (Your technology department will likely have done this for you on any device provided by your school.) This will ensure you will avoid many cyberattacks by default or at least you'll get a notification on what seems suspect and needs more attention from your part.

Visit https://www.vpnmentor.com/blog/teachers-guide-to-cybersecurity/ for a "Teacher's Guide to Cybersecurity." For additional resources, you can also visit https://www.in.gov/cybersecurity/education/teachers/.

Article 5:
Working Remotely — How to Be Safe & Secure

Between working at the office, or school, or remotely, the principles of security can become something of a moving target. For some, this creates an uncertainty with making sure that the right policies are applied. Reducing risk on at-home networks, keeping information secure during virtual meetings, and having a strong password policy are some best practices that can be implemented quickly and effectively from wherever you are working.

REDUCING RISK ON HOME NETWORKS

Home information technology devices, such as unsecured off-site routers, modems, and other network devices are subject to many of the same threats as on-site business devices. They can be attacked from any device on the internet. Remote devices are also vulnerable to unauthorized access from neighbors and passersby.

To help improve the security of your home network, the following is a list of questions to consider. In many instances, you can find answers and solutions online from trusted sources that are FREE and includes step-by-step instructions to help you. You can also consider working with an IT professional as an investment in your cyber safety.

Here's the list:

- Are your network devices physically secured?
- Have you changed the default manufacturer/administrative account password on your network devices (modem and router)? Many routers will come preconfigured with a password. The default password for most router models is easily accessible on the internet, making it extremely important to change the administrative passwords and not use the default.
- Do you have a unique password and two-factor authentication (2FA) enabled on your network devices (modem and router)?
- Do you have a password policy in place? Do you have a unique password and 2FA enabled on your internet service provider's web portal?
- If you use a mobile application for network management, do you have a unique password and 2FA enabled?
- Have you installed the latest updates for your network devices (i.e., modem, router, laptop/PC) or have you enabled auto-update with the device's administration page?
- Does your network device (router/modem) support Wi-Fi Protected Access Version 2 (WPA2) or Wi-Fi Protected Access Version 3 (WPA3)? WPA2 should be the minimum.

- Have you turned off/disabled Wireless Protected Setup (WPS) and Universal Plug and Play (UPnP) on your network? If enabled, these might allow attackers to connect to your devices without permission.
- Have you changed the Wi-Fi network name to something unique that doesn't provide any identifying information?
- Have you enabled firewall on your network devices?
- Have you disabled remote management? Most routers offer the option to view and modify their settings over the internet. Turn this feature off to guard against unauthorized individuals accessing and changing your router's configuration.
- Have you hardened your device by removing ports, software or services that are unused or unwanted?
- Do you run updated antivirus and malware protection on your device?

Asking yourself these questions will give you a better idea of where you stand with cybersecurity in your home.

For additional resources, visit: www.in.gov/cybersecurity

Article 6:
Securing Your Virtual Meetings

In order to help protect you and your organization from potential threats, here are some cybersecurity tips on how to securely configure your virtual meetings, whether they be for work or your classroom experience.

Sharing of Your Information Assets During Virtual Meetings

- Avoid adding your meeting to any public calendars or posting it on social media.
- Require participants to enter an access code.
- Avoid reusing access codes or meeting pins.
- Distribute the meeting link and access code directly to the intended participants.
- Remind invited guests not to share the access code.
- Before sharing your screen, close unused windows to ensure you do not share sensitive or confidential information.
- Use a privacy shield or cover over your webcam when it is not in use.

Managing Your Information Assets and Password Policy

- Use your organization's provided services and devices.
- Do not record the meeting unless it is necessary and be aware that others may be able to record the meeting.
- Disable the "Anyone Can Share" feature to prevent unauthorized screen sharing.
- Muting users on entry can prevent potential disruptions.
- Prevent users from sharing video by default; allow video sharing only when necessary.
- Validate the participant list against invited attendees, or have participants identify themselves as they join the meeting.
- Do not trust the safety of links shared in meeting chats.
- Schedule "Unlisted" meetings and hide specific details, such as its host, topic, and starting time.
- Do not allow attendees to "Join Before Host."
- Set up each meeting to require all attendees to enter a password.
- Create a unique password comprised of upper, lower case, numbers, and special characters for each meeting.
- Exclude the meeting password from attendee email invitations. Provide the password to attendees via a separate email or by phone.
- On reoccurring meetings, always check to ensure one-time attendees are not included in subsequent meetings or meeting chat threads.
- Do not list personal information, such as location, phone number, or date of birth on your Skype profile.

Remember, just like you protect your physical assets (shed, kayak, or bike) with a padlock, you need to be sure and protect the connectivity of your devices to protect your personal information!

Have you identified more risk than you initially realized?

More information and mitigation techniques - as part of CISA's FREE online cybersecurity toolkit - can be found at https://www.cisa.gov/resources-tools/resources/partnering-safeguard-k-12-organizations-cybersecurity-threats-online.

PROTECT YOUR FAMILIES

There is no greater responsibility for schools than providing students with a safe and secure learning environment.

There has never been a greater opportunity to capitalize on the opportunity to educate children and young adults about the importance of digital citizenship and safely communicating online; lessons they can share at home with their families.

At the same time, it's good policy to 1) provide important information digitally to the families of your students – especially for those in elementary school and, *separately*, 2) send out content directly to your middle school and high school students as it relates to classwork, assignments, and other relevant school information.

For families, including parents and guardians, it is OK if they are not tech-savvy. If there is something they don't understand, encourage them to reach out to other parents, to their child's school, or trusted family members. The goal here is not to make them or the student a security expert, but to make online learning a safe space.

For more information about how you can assess your cybersecurity knowledge as an individual or an organization, visit: https://www.in.gov/cybersecurity/government/assess-yourself/.

SHARE THE FOLLOWING ARTICLES WITH STUDENT PARENTS & GUARDIANS INCLUDING YOUR LOCAL PARENT SUPPORT GROUP OR PARENT TEACHER ASSOCIATIONS VIA EMAIL, NEWSLETTERS, ANNOUNCMENTS, ETC. THROUGHOUT THE SCHOOL YEAR.

Article 1:
Keeping Your Child Cyber Safe at Home

It has become even more important for families to make their homes more secure when connecting online for school and work.

As families, including parents and guardians, try to navigate emerging technologies (like ChatGPT), it is OK if they are not tech-savvy. If there is something you don't understand, reach out to other parents, to your child's school, or trusted family members. The goal here is not to make them or the student a security expert, but to make online learning a safe space.

The National Cybersecurity Alliance offers eight tips to share with families, including:

- NEW TECH? If the school issues or requires a technology that you and/or your child are not familiar with, explore its features together. Configure the security and privacy settings together immediately.

- APPLY YOUR RESEARCH. Apps are a great way for students to learn and apply their knowledge. Before downloading any new learning app on your child's device, make sure it is a legitimate app. Who created the app? What do the user reviews say? Are there any articles published online about the app's privacy & security features (or lack thereof)?

- DON'T HESITATE TO UPDATE. Having the latest security software, web browser, and operating system on devices children are using for their virtual schooling is one of the best defenses against online threats. When the computer or device says it's time to update the software, don't click postpone. Update.

- STRONG PASSWORDS IN PLAY KEEP CYBER CRIMINALS AT BAY. When is the last time you changed your home's router password, if ever? Change passwords for routers and smart devices from their default manufacturer's password to one that is long (at least 12 characters) and unique.

- PARENTAL CONTROLS. Parental controls are a great way to establish parameters around what kids can and can't do online. They do not replace candid discussions with your kids about online security and safety. Children may not recognize the dangers of visiting unknown websites or communicating with strangers online, so talk with them about these threats.

- NETWORK SEPARATELY. Students are not the only ones spending more time on the home network. Parents are also working from home at an unprecedented scale. *If you and your children are all working from home, consider using separate networks to enhance your security--particularly if your work involves access to sensitive information.*

- KNOW YOUR ROLE. Sometimes it is unavoidable for children to use the same computer that parents use for their work. If you are sharing devices, set up different user accounts so that children have access to a guest account with limited permissions and access. For instance, restrict your child's ability to install and run software applications.

- CONFIGURE PRIVACY SETTINGS. Go through accounts with children to configure privacy and security settings to limit over-sharing of information--such as location and camera sharing. Walk the kids through why certain settings need to be changed.

For additional resources, visit: www.in.gov/cybersecurity/individual/parents/

Article 2:
Keep Your Elementary Student Cyber Safe

Elementary students have grown up surrounded by electronics and the internet. From games and videos on a tablet to synchronous Zoom calls with their third-grade class; young students are subjected to cyber risks everywhere.

Incorporating good cyber habits at a young age, particularly as the workforce becomes more embedded on the internet, will prevent hacks, theft, and fraud in the future.

Parents are the guiding force when it comes to teaching kids how to be safe when they are online. Introducing good cyber habits can be as simple as playing fishing games to teach about the dangers of "phishing" scams. Here are a few examples of how to teach cybersecurity tips to children, and how parents can protect children:

- Understanding passwords: It can become a habit, especially in children, to create one "master password" for all devices and accounts to make them easy to remember. And while passwords are often controlled and created by parents rather than children, it is important to ingrain the concept of having unique and *complicated* passwords for all accounts and devices to protect information.

- The App Store: There are thousands of apps and games that can be accessed through tablets, computers, and cell phones. However, not all of these are meant for children. Be sure that content restrictions are set in place through online accounts to ensure that only kid-friendly content is in the hands of kids.

- Monitor who they are talking to regularly. It is 10 p.m. Do you know who your child is talking to? Whether it is on a game, social media, messengers, and more, it is important to establish rules with your kids that if they have not met the person, they do not talk to the person unless you have approved it. So many child predators count on parents allowing their young kids to be unsupervised with their phones, tablets, and game

systems. Talk to your kids regularly about who they are talking to and report any suspicious chats from unknown sources to local police.

While children may not seem like a main target of bad actors, they can be vulnerable. Child activity on unprotected networks can be a gateway for the bad guys to sensitive information such as financial records or other data. It is important to introduce these concepts early so that both you and your children can remain safe.

For additional resources, visit: www.in.gov/cybersecurity/individual/parents/

Article 3:
Keep Your Middle School and High School Student Cyber Safe

Just as they did while in elementary school, students, today, are familiar – and somewhat tech-savvy – when it comes to computers and being online, both for schoolwork and socially.

And, as students become teenagers, they are more likely to go places without their parents or even an adult. The same is true with the amount of time middle and high school students spend on their laptops, tablets, and phones.

Working with your child is key, especially as it involves being aware and having conversations with them about the sites they are visiting and who they are communicating with.

Tips include:

- Understanding passwords: It can become a habit, especially in children, to create one "master password" for all devices and accounts to make them easy to remember. And while passwords are often controlled and created by parents rather than children, it is important to ingrain the concept of having unique and *complicated* passwords for all accounts and devices to protect information.

- Protecting personal information on social media: It can be tempting to make funny posts on TikTok that reference the names of friends, names of schools, etc., but this can be incredibly dangerous. Social media is the newest form of communication for kids and adults alike, but it's also an easy way for people to gather information that can be used by bad actors for a variety of things. It's important to teach kids that personal information is *personal* and shouldn't be shared online.

- **The App Store:** There are thousands of apps and games that can be accessed through tablets, computers, and cell phones. However, not all of these are meant for children. Be sure that content restrictions are set in place through online accounts to ensure that only kid-friendly content is in the hands of kids.

While children and teens may not seem like a main target of bad actors, they can be vulnerable. Adolescent activity on unprotected networks can be a gateway for the bad guys to sensitive information such as financial records or other data. It is important to introduce these concepts early so that both you and your children can remain safe.

Article 4:
12 Ways to Cope with Working from Home with Kids

Even before the Pandemic, it was not unusual for family members, working from home, to be sharing space with their children, who, upon arriving home from school, are starting on their homework and class assignments.

To help working parents adjust to our even more connected lives an article on BetterUp.com highlights 12 tips for parents working at home with children. Among the suggestions involving a shared space with your kids as they work on that homework as you are also trying to work includes:

> **1. Stop multitasking**. Despite the popularity of the myth, multitasking isn't a good idea. The brain is far less efficient when working on more than one task at a time. Unfortunately, working from home without childcare is basically a masterclass in multitasking -- meaning you're already starting at a disadvantage. So instead of multitasking, set up and take advantage of pockets of time when you have the luxury of focus. Having moments where you're fully present will make you feel less overwhelmed.
>
> **2. Pick something to let go of.** You can't do it all, no matter what the self-help books tell you. However, you can have everything that's important to you. Remember, you can pick your priorities — your friends, boss, coworkers, and social media shouldn't choose them for you. Letting go might mean letting the kids put away their own laundry, ordering take-out, or allowing the dishes to chill in the sink for a bit.
>
> **3. Communicate with key people at work.** Work-from-home parents need to remember that they are not alone. Most managers are more understanding than they've been at possibly any point in modern history — and they might even be in the same boat. In this case, honesty about your home life is the best policy.

4. Set up a home office. Parents working from home long term need to get off the kitchen table and into a home office. If you don't have a dedicated space, family members are more likely to interrupt your work time. A home office for any remote job is a visual reminder to everyone that when you're sitting there, it's probably not the best time to bother you. Here are a few tips to help you start building your workspace.

5. Get out of the house sometimes. One of the challenges of working from home is that you may find yourself sitting indoors for hours on end. A change of pace and scenery can be medicinal. Time in the sun is one of the best ways to quickly boost your mood and your energy. Try reducing your screen time by taking a conference call outside or enjoying a midday walk. You could even treat your kids to an alfresco lunch in the neighborhood park.

6. Go easy on yourself. Give yourself some credit for everything you're trying to manage. Try to release the anxiety and guilt around not being able to keep things to the standard you're used to. If you tend to be particularly hard on yourself, think of this as a great time to model grace under pressure for your kids. Throughout the workday, listen to your self-talk. Support yourself like you would support someone you love. Working from home with kids is challenging, and you're doing the best you can.

7. Prioritize self-care. When your work schedule is full and your family life is busy, making time for yourself is easier said than done. However, without self-care, stress is a recipe for burnout and overwhelm. Remember: in the long run, prioritizing your well-being make you both a better caregiver and employee. If you just build a few healthy habits into your daily schedule, it can make a big difference in your happiness.

8. Meditate. Consider using some of your precious free time to meditate. In addition to lowering stress, meditation builds several other useful skills. It helps you regulate your emotions and learn to focus more effectively (when you are able to focus, that is). It can also help you become a more mindful parent. When you're in hustle mode, it's tempting to just power through — but taking breaks actually improves your ability to work effectively.

9. Ask for help. You might be able to lean on friends, grandparents, or your spouse for support. For example, you can ask loved ones for practical help like driving your older children to sports practice or keeping your little ones entertained during an important Zoom call. If that's not feasible, though, see if it's possible to recruit professional help. Hire a housekeeper, get a babysitter for a couple of days a week, or use an app to get the laundry picked up. Getting help for even a couple of hours a week can be life changing.

10. Tire the kids out. Every parent knows that sometimes the best strategy to get a little peace and quiet is to run down your kids' batteries. Staying in the house all day quickly leads to cabin fever, so get outside and engaged when you can.

11. Create a family schedule. When everyone in the house has different work, school, and social schedules, it might be time to put it all on a calendar. Whether it's digital or pinned to the fridge, you can create a daily schedule that includes quiet time for your meetings, homework time for your older kids, and family fun time, too. It might take some time to adjust, but boundaries are key to thriving when you're working remotely. If you get interrupted during your focus time, just gently remind your child or spouse that you're busy and will be able to catch up with them later. Ultimately, a schedule can help everyone get on the same page and reduce stress.

12. Take a mental health day. When all else fails, it's time to call in sick and take a mental health day. Sometimes, everything is just too much, and that's okay to admit. Mental health is health, after all. Use your day off to recharge, relax, and reflect. You may want to ask yourself, why are you doing what you're doing? Is it still aligned with your personal and family values? Going back to your "why" will help you return to work the next day with more energy and peace.

For additional resources, visit www.in.gov/cybersecurity/individual/parents/.

Article 5:
Working Remotely — How to Be Safe & Secure

Between working at the office, or school, or remotely, the principles of security can become something of a moving target. For some, this creates an uncertainty with making sure that the right policies are applied. Reducing risk on at-home networks, keeping information secure during virtual meetings, and having a strong password policy are some best practices that can be implemented quickly and effectively from wherever you are working.

REDUCING RISK ON HOME NETWORKS

Home information technology devices, such as unsecured off-site routers, modems, and other network devices are subject to many of the same threats as on-site business devices. They can be attacked from any device on the internet. Remote devices are also vulnerable to unauthorized access from neighbors and passersby.

To help improve the security of your home network, the following is a list of questions to consider. In many instances, you can find answers and solutions online from trusted sources that are FREE and includes step-by-step instructions to help you. You can also consider working with an IT professional as an investment in your cyber safety.

Here's the list:

- Are your network devices physically secured?
- Have you changed the default manufacturer/administrative account password on your network devices (modem and router)? Many routers will come preconfigured with a password. The default password for most router models is easily accessible on the internet, making it extremely important to change the administrative passwords and not use the default.
- Do you have a unique password and two-factor authentication (2FA) enabled on your network devices (modem and router)?
- Do you have a password policy in place? Do you have a unique password and 2FA enabled on your internet service provider's web portal?
- If you use a mobile application for network management, do you have a unique password and 2FA enabled?
- Have you installed the latest updates for your network devices (i.e., modem, router, laptop/PC) or have you enabled auto-update with the device's administration page?
- Does your network device (router/modem) support Wi-Fi Protected Access Version 2 (WPA2) or Wi-Fi Protected Access Version 3 (WPA3)? WPA2 should be the minimum.

- Have you turned off/disabled Wireless Protected Setup (WPS) and Universal Plug and Play (UPnP) on your network? If enabled, these might allow attackers to connect to your devices without permission.
- Have you changed the Wi-Fi network name to something unique that doesn't provide any identifying information?
- Have you enabled firewall on your network devices?
- Have you disabled remote management? Most routers offer the option to view and modify their settings over the internet. Turn this feature off to guard against unauthorized individuals accessing and changing your router's configuration.
- Have you hardened your device by removing ports, software or services that are unused or unwanted?
- Do you run updated antivirus and malware protection on your device?

Asking yourself these questions will give you a better idea of where you stand with cybersecurity in your home.

For additional resources, visit: www.in.gov/cybersecurity

Article 6:
Securing Your Virtual Meetings

In order to help protect you and your organization from potential threats, here are some cybersecurity tips on how to securely configure your virtual meetings, whether they be for work or your classroom experience.

Sharing of Your Information Assets During Virtual Meetings

- Avoid adding your meeting to any public calendars or posting it on social media.
- Require participants to enter an access code.
- Avoid reusing access codes or meeting pins.
- Distribute the meeting link and access code directly to the intended participants.
- Remind invited guests not to share the access code.
- Before sharing your screen, close unused windows to ensure you do not share sensitive or confidential information.
- Use a privacy shield or cover over your webcam when it is not in use.

Managing Your Information Assets and Password Policy

- Use your organization's provided services and devices.
- Do not record the meeting unless it is necessary and be aware that others may be able to record the meeting.
- Disable the "Anyone Can Share" feature to prevent unauthorized screen sharing.
- Muting users on entry can prevent potential disruptions.
- Prevent users from sharing video by default; allow video sharing only when necessary.
- Validate the participant list against invited attendees, or have participants identify themselves as they join the meeting.
- Do not trust the safety of links shared in meeting chats.
- Schedule "Unlisted" meetings and hide specific details, such as its host, topic, and starting time.
- Do not allow attendees to "Join Before Host."
- Set up each meeting to require all attendees to enter a password.
- Create a unique password comprised of upper, lower case, numbers, and special characters for each meeting.
- Exclude the meeting password from attendee email invitations. Provide the password to attendees via a separate email or by phone.
- On reoccurring meetings, always check to ensure one-time attendees are not included in subsequent meetings or meeting chat threads.
- Do not list personal information, such as location, phone number, or date of birth on your Skype profile.

Remember, just like you protect your physical assets (shed, kayak, or bike) with a padlock, you need to be sure and protect the connectivity of your devices to protect your personal information!

Have you identified more risk than you initially realized?

For additional resources, visit: www.in.gov/cybersecurity

PROTECT YOUR STUDENTS

SHARE THE FOLLOWING ARTICLES WITH STUDENTS VIA EMAIL, NEWSLETTERS, ANNOUNCMENTS, ETC. THROUGHOUT THE SCHOOL YEAR.

Article 1:
Protecting Yourself Online

Whether you are a sixth grader entering middle school or a senior preparing for graduation, you have grown up surrounded by electronics of every variety and the Internet.

From games and videos on a tablet to completing your homework and engaging others on social media, you are online, often for hours at a time each day. And, while it's OK to have fun, whether you're on your laptop or phone, at school or at home, there are several things you can do to protect yourself from people who are looking to steal your identity or target you for abduction or worse.

Here are some helpful tips from Norton (a recognized authority on cybersecurity):

- Don't use the same password twice.
- Direct messages from unknown accounts are usually not reliable. Report and block these accounts and be sure to *not* open any links they send.
- Avoid sharing too much personal information like where you live, your whole name, what time you are home alone, etc.
- Put a lock on your phone – a pattern, a code, facial recognition etc.; this will ensure that, if your phone is taken by another person, they cannot access your phone, personal data, or your social media accounts.
- The block button is not something to fear! It will help keep bad people away from your information, keep you safe, and your feed uncluttered.

For more, visit www.in.gov/cybersecurity/individual/cyber-tips/.

Article 2:
Don't Get Hacked

When you're at school or you are working on completing your class assignments, there are some important things you can do to make sure your computer is protected against viruses and hackers, and you are not exposed to any sort of security risks (like someone hacking your microphone or camera to take illegal audio and video of you).

- Enable Automatic Updates so your computer is the most secure.
- Shut down or restart your computer once a week to allow updates to take effect.
- For all your devices, remember to back up your photos, documents, etc. in case you lose your device, or it gets hacked, and you have to erase your device.
- Always install updates when your carrier tells you they are available.
- Be sure to always use legal filesharing services for obtaining music, movies, TV, games, books, etc. on the Internet. A large list of digital music, videos, and other services is available from Educause at http://www.educause.edu/legalcontent. If you use illegal services, know that many people include links to malware to hack your computer.
- When you are not using your computer, turn it off. If you are using your computer, put a protective cover on your webcam so it *cannot* take pictures of videos without you knowing.

For more helpful tips for protecting yourself online, be sure to check out https://its.ucsc.edu/security/student.html.

You can also learn to best protect yourself on social media, by looking over a *Social Media Guide* and additional resources at: www.in.gov/cybersecurity/education/students/.

Article 3:
Top 5 Cyber Tips To Start NOW

Whether doing research, finishing assignments, emailing teachers or classmates, or just communicating, your computer and phone is a gateway to a lot of problems you don't need, especially now.

Here are five cybersecurity tips for students according to MYKI.com (a reputable digital identity management company):

1- Be careful what you share

You might want to consider the impact of what you post online. We'd all like to show off that we passed our driving test, or that we're going on vacation, but posting pictures of things like driver's licenses, boarding passes, or credit cards makes you a prime target for identity theft.

2- Lock up and shut down

Leaving your laptop or phone unlocked is a big mistake. The damage might be as minor as your annoying roommate changing your Facebook profile picture to something silly, or as major as some stranger in the cafe you're working at messing with your bank account. If you're going to leave your laptop or phone unattended, make sure you lock it, or set it to sleep or shut down after a certain period of inactivity.

3- Avoid phishing emails

Think twice before you reply to that Nigerian prince.

There are plenty of thieves and scammers on the web, and phishing emails are one of their tried-and-true tactics. These are emails that might look like they're from a trustworthy source but are actually trying to trick you into providing sensitive data, like your password or credit card details.

All you have to do to prevent yourself from being "phished" is have some common sense and make sure the sender of an email is really who they say they are.

4- Stick to HTTPS websites

Here's something you may have never stopped to consider. Look up at the address bar of your browser: the URL begins with "https".

This means that unlike HHTP protocol websites, the site you're currently on uses a secure protocol, and all communication between your browser and that site is encrypted. In other words, no third party can eavesdrop on you and intercept the data you provide that site. That's not to say that all HTTP websites are malicious, but it's always best to proceed with caution.

5- Use a password manager

Last but not least, you'll need to get yourself a good password manager.

On top of the dozen social media accounts you've already got, you're probably going to need some new academic accounts, which means a *whole lot* of passwords to remember.

But since you're only human, you'll be very tempted to use the same easy-to-remember password for everything, which is actually quite risky.

This is why it is highly recommended that you use strong and unique passwords, which you can securely store with a password manager. For more information, be sure to check out our blog to learn more about using a password manager at: https://www.in.gov/cybersecurity/blog/posts/one-password-to-rule-them-all/.

SOCIAL MEDIA CONTENT #4YOU2SHARE

Social media is a platform for learning, especially when it comes to cybersecurity.

And, whether you're sending out a Tweet, sharing a post on Facebook, or you have information to provide to others in the business world on sites, such as LinkedIn, it's important that you make sure you are communicating in a way that is safe and secure.

Although it is true that good advice can often be shared in as little as 40 characters or to a link that takes you to a credible source, so, too, it's important to follow best practices whenever you are online.

Here is some content and quick links we invite you to share with your family, friends, colleagues, and community members. You can use this content on your social media platforms or as part of any digital newsletters and other communication you are providing to families and students.

Content for Students

- Read the *Social Media Guide for Students, Parents, and Bloggers* at https://www.cisa.gov/sites/default/files/publications/Social%20Media%20Guide_1.pdf

- Cyberbullying is not a thing of the past. Learn how young people can identify and protect themselves from cyberbullies here: https://www.cisa.gov/news-events/news/dealing-cyberbullies

- Cybersecurity Tips for Teens & Families: Things I Wish My Parents Had Told Me About Internet Safety.

- Back to school season is coming right up! Pens and pencils are important, but so is staying cyber safe! Learn more student cyber safety here: https://securityboulevard.com/2019/08/back-to-school-tips-the-abcs-of-online-security/

- Series on Student safety
    - https://ets.hawaii.gov/wp-content/uploads/2016/09/Cyber-Tips-for-Students.pdf
    - Cyber Safety for Students | CISA
    - https://www.marquette.edu/remote-learning/cyber-security-tips.php. - remote learning

- Cybersecurity Tips for Student Bloggers
- https://www.apzomedia.com/8-essential-cybersecurity-tips-for-student-bloggers/

Content for Parents

- 5 Cyber Safety Tips Every Parent Should Know.

- Top 5 Questions Parents Have About Cybersecurity https://www.connectsafely.org/wp-content/uploads/securityguide.pdf

- Tips for Parents - Protecting Kids Online https://www.consumer.ftc.gov/topics/protecting-kids-online

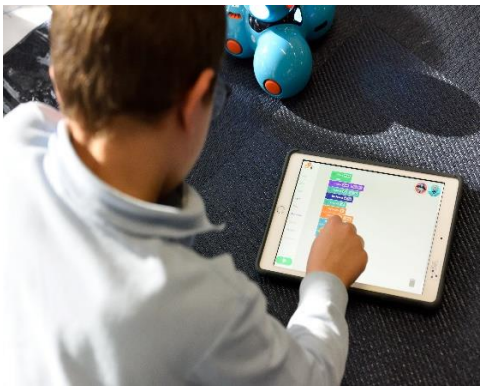
- 13 Apps Every Parent Should Know in 2020 https://educateempowerkids.org/13-apps-every-parent-should-know-in-2020

- Parents: With kids spending more time online, it is important to teach them how to be cyber safe. Learn more about social media safety here https://au.norton.com/internetsecurity-kids-safety-parents-best-practices-to-social-media-security.html

- Tips for Parents Raising Privacy-Savvy Kids https://documentcloud.adobe.com/link/review?uri=urn:aaid:scds:US:09e0015f-3bc7-4504-b008-88692c8ef737

Images for Social Media

As you use the social media content and develop your own content for your school district with the many tips in the *Cybersecurity for Education Toolkit*, feel free to copy and paste the below images with your messages.



SCHOOL COMMUNITY PATRONS

Who are your school community's patrons? They are the people who help make up your town or city; everyone from your grandparents to that young couple who just moved in next door.

In other words, it is everyone who is *not* a student, teacher, staff member, administrator, or school board member. Yet, they are invested in living in a place that values education and understands that good schools contribute to the quality of life within the community.

School districts routinely communicate information with people through newsletters, stories in the news media and through their family members and friends.

Because of this, it is important for members of the public to know and understand the importance of being cybersafe and there are resources out there for everyone.

STOP. THINK. CONNECT. ™ is the global online safety awareness campaign to help all digital citizens stay safer and more secure online. The message was created by an unprecedented coalition of private companies, non-profits and government organizations with leadership provided by the National Cyber Security Alliance (NCSA) and the APWG.

The campaign was launched in October of 2010 by the STOP. THINK. CONNECT. Messaging Convention in partnership with the U.S. government, including the White House. NCSA, in partnership with the APWG, continue to lead the campaign. The Department of Homeland Security leads the federal engagement in the campaign at:
https://stopthinkconnect.org/

For additional resources, visit www.in.gov/cybersecurity.