Cybersecurity for Students

Your school does a lot to protect you, but you have a role in cybersecurity too.

Cybercriminals target students as they return to school in the fall, travel on school breaks, and as they use online applications to complete class work or post on social media. Starting in K-12 and continuing into college, we all have a part in protecting student data and privacy.

10 Steps to Cybersecurity Safety for Students:

Set up 2 factor authentication everywhere!

Two Factor authentication, often called "multi-factor authentication", is one of the most effective ways to protect your accounts and applications. Two factor authentication is a must on any app that contains personal data, including all social media accounts, streaming accounts, banking apps, school email accounts, and education applications!

Don't save passwords in your browser.

Saving passwords in the browser may seem like an easy way to quickly log into applications and websites, but it is also one the most common ways for cybercriminals to steal your passwords. Use unique passwords for all of your apps, and never save them in your browser. It may seem like a good idea, but it is actually very dangerous.

Use cellular data or VPN when using sensitive apps.

Free and insecure Wi-Fi networks are not safe to use when interacting with sensitive data such as banking applications, tuition accounts, or healthcare apps. If you routinely use free Wi-Fi at your favorite coffee shops or in public areas, remember to turn your Wi-Fi off and use your cellular data when using sensitive apps. If you must use public Wi-Fi we recommend using a VPN application to encrypt your data. They are inexpensive and easy to use!

Keep your phone and all apps up-to-date.

Many students don't update their phones and mobile devices when software patches are made available from Apple, Google, or other manufacturers. Remember to update your software often. These updates contain security enhancements that stop attackers from gaining access to your devices and data.

Backup all of your data!

We recommend you utilize a cloud backup solution for your mobile devices and laptop. In the event of a device failure, a theft, or a security event that causes you to lose data, you won't lose your school work, pictures, contacts, or emails. Most backup solutions work automatically once installed.

Don't click on links sent in text messages.

Cybercriminals often send links in text, SMS, iMessage, or social media messaging applications. These links will direct unsuspecting users to websites that steal data or give access to files on your phone and other devices. We recommend never clicking on a link sent in a message unless you know and trust the sender.

Don't share your current location on social media.

Posting on social media can be a fun way to connect with your friends and family. In order to stay safe, we recommend posting your pictures and stories after you have left a location, not while you are there! Providing cybercriminals with your exact ocation can put you at risk.

Don't scan random QR codes!

QR codes are used for many legitimate reasons, such as accessing menus in restaurants. But stickers with fake QR codes are often put in public places or over legitimate QR codes that direct students to fake copies of familiar websites and applications like Amazon, Instagram or Doordash. These fake websites are built to steal credentials or install malware on devices. Only scan QR codes from reputable sources that you trust.

Do not plug into public USB Charging ports.

Public and free USB charging ports are widely considered to be dangerous. These ports can often give an attacker access to the data on your device. Carry a charger with you and plug into an outlet to keep your devices safe at school and when traveling.

Never leave devices unattended.

Unattended devices are a target for data theft. Keep devices with you or store them in a secure location at all times. When traveling, never leave them in a hotel room or unattended in luggage.

How to Report a Cyber Incident

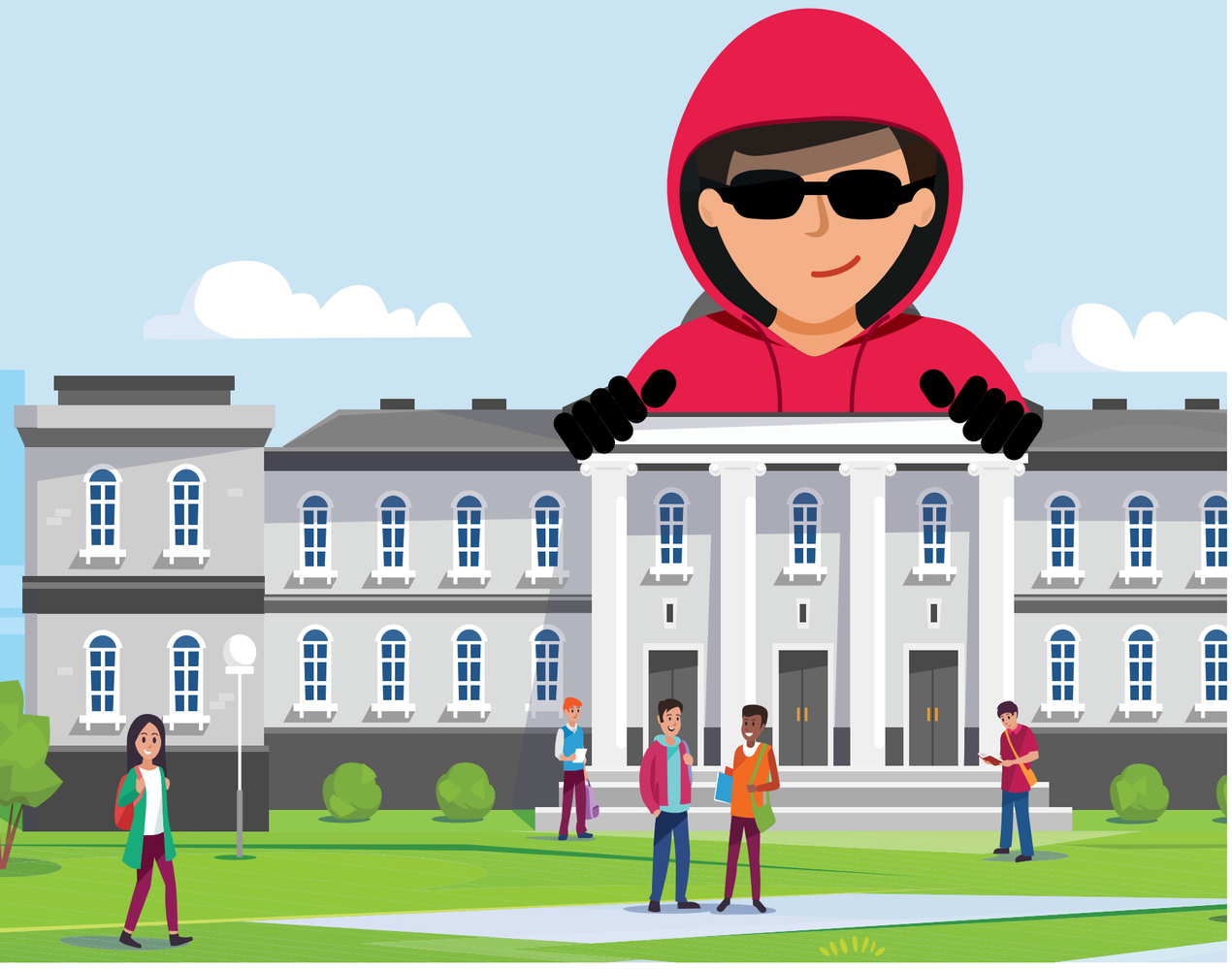
Cyber incidents often go unreported in New Hampshire. Reporting is a critical part of safeguarding our state. It allows incident responders, law enforcement, and policymakers to see the types of cyber events happening in our state.

Please consider doing your part to report any cyber incident, no matter how small it may seem at:

www.nh.gov

Click on this icon at the bottom of the page

Report a CYBER Incident



The Municipal Cyber Defense Grant is a collaboration between The ATOM Group, LLC. and the The New Hampshire Department of Information Technology. It is managed in coordination with the New Hampshire Public Risk Management Exchange and serves all New Hampshire based municipal governments, schools, and public sector organizations. For more information about the MCDG Program and the free services we provide, please visit us at https://www.theatomgroup.com/mcdp