Student Cyber Security Best Practices

Cyber security is a crucial skill for students in the digital age. By understanding and applying best practices, students can defend not only their personal information but also contribute to the security of everyone in the district. It's a collective effort where each individual's actions can make a significant difference. Staying informed and vigilant helps maintain the integrity and safety of our increasingly connected world. Let's all commit to being cyber-smart and protect our digital future together!

Use strong passwords or passphrases and MFA

Create unique, complex passwords *or a passphrase* of three or more words with special characters and numbers separating them. Use a password manager to generate and store different passwords for all your accounts, **and don't share them with anyone!** When available, enable multi-factor authentication (MFA) for an extra layer of security. It keeps your accounts safe if the passwords are breached or leaked, by combining something you know, with something you have. This can be done with an authenticator app, using passkeys, or a physical security key.

Read More →

Update everything!

Developers can make mistakes in their code, so regularly check, and apply updates for your apps and devices to patch security vulnerabilities. You can make this easier by enabling auto updates and regularly rebooting your device. This helps protect against cyber threats by patching vulnerabilities in the code. **Check in your settings app for updates, and don't ignore notifications to update your device!**

Watch out for phishy stuff

If a message seems weird, makes you uncomfortable, or is asking for too much information, don't take the bait! Avoid clicking on strange links or downloading mystery files especially if it's from someone you don't know. Messages may try to impersonate a friend or teacher, ask for personal information, have misspellings or poor grammar, or has an offer that seems too good to be true, **it probably is**.

Read More →

Lock Your Device

You wouldn't walk away with your locker open and unlocked, don't do the same with your device! On Windows, you can quickly lock your PC by pressing ⊞ Win + L on your keyboard, this will help keep unauthorized people out!

Be careful what you share

Review and adjust privacy settings on apps and websites. Only share what's necessary—don't overshare permissions that could put you at risk if the data were leaked! Hackers can't steal information if it doesn't exist.

Don't bypass the protections on your device

The protection tools that come built in or installed by the district like web filters, malware scanners, and firewalls are there to protect you from harm. Attempting to bypass these are not only a violation of district board policy and the Technology Acceptable Use and Internet Safety Agreement, but could also put your personal privacy and safety at risk.

Read More →

Report and take action

If you suspect your school account has been compromised, or you have other concerns. Report it to your teacher or school administration as quickly as possible, so they can begin the appropriate action steps toward remediation.

Take action by resetting your password yourself, by either pressing **CTRL+ALT+DEL** and pressing **change a password** or by going to mysignins.microsoft.com/security-info and changing your password from there. Then look for a link to **sign out everywhere**, that will kick the threat actors out of your account.

Securing your account with strong passphrases and MFA

- **Complexity matters**:
  - A strong password is like a magical spell—hard to crack! Use a mix of uppercase and lowercase letters, numbers, and special characters.
  - Consider using a passphrase—a series of random words or a sentence. For example: “GreenDragon$42@Sky!”
  - Avoid using common words like “password” or your school’s name, and personal details like your birthday.
- **Unique for each Account**:
  - Imagine if your castle had the same key for every door – convenient but if someone stole that one key they could get into your castle **and worse,** your secret dungeon where you store your loot! **Don’t reuse passwords.**
  - Each account (like your email, school, social media, or gaming) deserves its own special key.
- **Length is power**:
  - Longer passwords are like thicker castle walls. Aim for at least 12 characters.
  - Passphrases can be even longer—like epic poems of security.

Storing these passwords and passphrases with a password manager

- **What’s a password manager?**
  - It’s like a magical chest where you store all your keys (passwords).
  - You only need to remember **one master password** and a MFA method to unlock it.
- **Why use a password manager?**
  - **Organization**: Keeps all your passwords in one place.
  - **Randomization**: Generates strong, unique passwords for each site.
  - **Security**: Encrypts your info so only you can access it.
- **Which password manager should I use?**
  - **We recommend using Bitwarden**, as it’s free and open source.
  - **There are other managers that we already have allow-listed in our browser extensions:** Keeper, Dashlane, Norton Pass, Proton Pass, etc.
  - Alternatively, you can use your browser’s built-in password manager, but please note these are often tied to your district Microsoft account and you will lose access to them if you lose access to your district account.

Multi-Factor Authentication (MFA)

- **What’s MFA?**
  - It’s like having a key and a secret knock. It mixes something you have (eg: your phone) with something you know.
  - Prevents account breaches if your password is leaked online.
  - There are multiple flavors of MFA: phishing-resistant MFA with the Microsoft authenticator app, using passkeys, or a physical security key or Legacy *non-phishing resistant* MFA like one-time passcodes & SMS.
  - Most password manager apps will also do MFA, but often they only support legacy MFA methods.
  - When available, we recommend using phishing-resistant MFA as it protects you from Attacker-In-The-Middle attacks. Legacy MFA is still better than no MFA.
  - Most apps and services offer or enforce MFA—There really isn’t a reason not to use it!

How to spot & avoid phishing

What is Phishing? Phishing is a type of scam where attackers try to trick you into giving them your personal information, like passwords, credit card numbers, addresses, etc. They often do this by sending fake emails or messages that look like they're from a trusted source, such as your school, financial institution, or a popular website.

- **Be skeptical of unfamiliar messages:**
  - If you receive an email from someone you don't know, be cautious. Don't open any links or attachments unless you trust the source.
  - Report the message as phishing if you believe it's a scam, better to be safe than sorry.
- **Look for red flags:** 🚩
  - Check for spelling mistakes, strange email addresses or phone numbers, or if the message is creating a false sense of urgency while asking for personal information. These are common signs of phishing.
- **Verify the source:**
  - If a message claims to be from your school, bank, or another trusted source, double-check by contacting them directly using a known phone number or website. They could be impersonated and not know about it.
  - If the message is an email from a trusted source, verify the sender's address is coming from the trusted source's domain and not a third party. You can view message details to verify this.
- **Don't share personal Information:**
  - Never give out your passwords, social security number, or other personal details through email or text messages.

Security and web protections on devices

What protections are on school devices? We deploy security and web filters that help protect you and your device from harmful content and cyber threats. They block access to inappropriate websites, prevent malware infections, and keep your personal information safe.

Why you shouldn't attempt to bypass these protections:

- **Increased Risk of Cyber Threats:**
  - Bypassing security measures can expose your device to viruses, malware, and hackers. These threats can steal your personal information or damage your device.
- **Access to Inappropriate Content:**
  - Web filters are in place to block harmful or inappropriate content. Bypassing these filters can lead you to websites that are not safe or suitable for your age.
- **Violation of District Policies:**
  - Using Virtual Private Networks (VPNs), proxy / unblocking sites, or other methods to bypass security measures is against district policies. This can result in disciplinary actions, such as losing device privileges or other consequences.
- **Compromised Personal Information:**
  - Using a VPN or proxy can sometimes be unreliable or even malicious. If you use one, all your internet traffic and data will pass through those services and can put your personal data at risk, as it may be collected and misused by third parties.
- **Disruption of Learning:**
  - Security and web filters help create a safe and focused learning environment. Bypassing these protections can lead to distractions and hinder your educational experience.