SECURITY-MINDED

Practical security wisdom for daily life.

BACK-TO-SCHOOL CYBERSECURITY

Easy lessons for parents, students, and teachers at the start of the school year

The start of the school year brings changes for everyone, whether you're a student, a parent, or an educator. You may need to navigate new physical and digital environments, create new online accounts, and safely share data, documents, and personal details.

The following security tips can help you—and any students in your care—start the year strong.

Keep Devices Close

Whether it's the local middle school or a university campus, thieves are drawn to unattended smartphones, tablets, or laptops. And asking a stranger to "watch your stuff" at the library or coffee shop is never a good idea. Instead, **keep devices with you whenever possible**. Otherwise, lock them in a secure location, such as a desk drawer or locker.

Make sure you're locking your device with a **strong password or PIN** (Personal Identification Number) in case it goes missing. This simple step helps keep strangers out of your private messages, photos, data, and accounts. Some devices also have features that (if enabled) can help you locate the device or erase its contents remotely.

Secure Your Accounts

Educational institutions of all types rely heavily on mobile and online applications. That means students, parents, teachers, and administrators must set up new accounts and login credentials. These credentials may be necessary to keep track of assignments, grades, and school calendars. You may also need them for university email accounts, tuition payment systems, and other campus computing resources.

In the rush to start the new year, it's easy to overlook important security measures. For example, you might be tempted to use the same password to create multiple new accounts—but that's a serious mistake. Instead, always **create a strong, unique password for each account**, and consider using a password manager to keep track of them. For more security, **enable multi-factor authentication** whenever possible.

Prepare for New Networks

Using a school's official network is usually much safer than free, unsecured Wi-Fi. But joining these networks can have unintended consequences. For example, if you've been sharing your computer's library of music or videos on your home network, you could accidentally share it with the entire school network.

Whether it's the local middle school or a university campus, thieves are drawn to unattended smartphones, tablets, or laptops.

SOCIAL MEDIA FOR SMART STUDENTS

Share these tips with the students in your life:

- **Think before you share –** What could you gain from posting this comment, photo, or link? What could it cost you, today and in the future? Many colleges and employers say that they consider a person's social media when making decisions about applicants.
- **Take a breath –** It's tempting to vent negative emotions on social media, whether they're directed at others, yourself, or your school. But it pays to cool off before you post. If you wouldn't say it to or share it with a stranger, it probably shouldn't be posted on social media.
- **Privacy settings aren't foolproof –** You may intend to only share your thoughts with a small circle of online friends and followers, but there's always a risk that others could see what you post. An online comment about a teacher or classmate, for example, can quickly make its way back to that person.

Before you join the school's network, **check your device's settings and disable file sharing**. It's also a good idea to check the sharing settings on any cloud storage services you may be using.

Get Smart About Sharing

The start of the year is also a good time to review your social media. Even if the photos, activities, and opinions you've posted seemed fine in your personal life, they may not make the grade. **Teachers, especially, should expect scrutiny** of their social media activities, both past and present. But students and their parents can also face consequences for online behavior that others find inappropriate.

Take some time to **go through your social accounts** and remove anything that could reflect badly on you, your school, or your friends and colleagues. If you're the parent of a student, consider doing this essential chore together.

Unfortunately, even if you delete a post or photo, someone could have already taken a screenshot or downloaded the image. Going forward, assume that everything posted on social networks is not only *public*, but also *permanent*.

Activity Corner // Word Scramble

Unscramble these ten things you should double-check before school starts:

1. **wrspaossd**
2. **acviypr estgtins**
3. **rtsewkno**
4. **aislco cncaotsu**
5. **fiwi**
6. **phmtsrenoa**
7. **rctilmuafto inetitcnahatuo**
8. **mouptecr**
9. **trsaofew sutedap**
10. **ouldc civseser**

Answers:

1. passwords
2. privacy settings
3. networks
4. social accounts
5. Wi-Fi
6. smartphone
7. multi-factor authentication
8. computer
9. software updates
10. cloud services