

Top 5 Data Security Tips for Educators

It's unfortunate but true – bad actors are hard at work to compromise school districts' data. And one of their most successful strategies is targeting busy educators who have access to student data but may not have adequate security measures or who might fall victim to a clever scam. Here are 5 practical things you can start doing *right now* to protect yourself online and, by extension, protect your school, your students, and your colleagues.

#1: Hover Your Links - Know What You're About to Click

When you visit a website or receive an email, you'll often be presented with several links. While many of these links are harmless or even helpful, some links could lead to fake login pages or downloads of malicious programs. All web browsers and most other programs that display links allow you to "hover" or hold your mouse over the link (without clicking) to see where it goes. This also works on mobile devices by pressing (and not releasing) a link until a preview appears.

Look at the URL that the preview shows you:

- Is it the website you thought you should be going to?
- Is it a weird-but-similar URL designed to trick you like "webs1te.com" when you *should* be going to "website.com"?
- Maybe the link shows "website.com" but when you hover the link you see "hackedwebsite.com".

It's not always obvious, but if the hovered link doesn't look right in any way, do not click on it! Of course, every application and device is different so check the documents on how to hover links on your computer or mobile device. You can always practice hovering links to get the hang of it on a website that you trust already.

OOPS...What if I click on something I shouldn't have?

Let your technology department know IMMEDIATELY! It can happen to anyone, and your best chance of preventing a data disaster is to notify the experts right away, before the hacker has time to infiltrate your system. You will feel embarrassed, but in doing the right thing right away, your tech support will thank you.

#2: Let Automatic Updates Do Their Job

Over and over, attacks are successful **only because the target was running outdated and vulnerable software**. Most operating systems, applications and devices now come with

automatic updates enabled. It's important to keep those settings in place and to allow the updates to apply and, if necessary, reboot. It's the perfect time to take a short walk or get a cup of coffee.

Apply web browser updates the day they become available. It's one of the easiest ways to protect against hackers!

But...what about all my tabs?

In the past, you might have been hesitant to close a browser so updates can be applied, but most browsers today will remember all your tabs and reopen them after restarting your browser. Your web browser is often your interface to the entire Internet, and security updates only work if you allow them to be applied.

#3: Lock AND Encrypt

Many laptops and most mobile devices come with encrypted storage. This is a great thing, but it's important to **make sure your devices are also configured to lock after a short period of inactivity.**

- If a laptop or mobile phone is stolen while it's unlocked, the encryption doesn't matter because the thief not only has your hardware, but also every bit of data you had on your device.
- Replacing a laptop or a mobile phone is much easier and less expensive than containing the damage that might happen if all your data is also lost! Then again, if your device is locked but not encrypted, it's very easy to physically open it and retrieve the data. To be fully protected you need to lock AND encrypt!

#4: Don't Reuse Passwords, Use a Password Vault

You love your password, it's so complicated no one could ever guess it and besides, you spent *so much* time memorizing it. This might work for a while but the reality is...**some website where you used that password five years ago just got hacked and someone is selling the list of usernames and passwords.** Whoever buys the list and starts trying these username/password combinations at popular email or banking websites stands a good chance of getting your data *if you're still using that password!*

- Use a randomly-generated password for *each* website and store them in a secure password vault to mitigate this risk commonly referred to as "credential stuffing."
- Password vaults come in all flavors from paid versions that have a lot of features to free versions that are nearly impossible to crack.

But... I regularly make clever modifications to my favorite password, so I'm good, right?

Nope, making a slight password variation like shifting a “t” to a “+” or adding the 4-digit year at the end is no match for an attacker with your old password and a program specifically designed to try your password with these variations on hundreds or thousands of websites per hour!

#5: Use Multi-Factor Authentication

Unique passwords are great and so is a password vault but they suffer from a fatal flaw. **If someone has your password, they have your access.** This is why anytime it is available, use multi-factor authentication. Just about every financial institution, email provider and many other online services now offer multi-factor authentication. Multi-factor just means “multiple ways to authenticate” or prove you are who you claim to be. Common “factors” include:

- Passwords
- Passkeys
- Security fobs
- Authenticator apps
- SMS or voice codes sent to a mobile device
- A fingerprint
- The shape of your face
- The sound of your voice

They fall into three broad categories:

- Something you know - i.e. a password or passphrase
- Something you have - i.e. an authenticator app or a security fob
- Something you are - i.e. a fingerprint or the shape of your face

While an attacker may be able to find your password through credential stuffing (see #4 above) or some other means, **it's exponentially more difficult for an attacker to capture multiple factors** like a password and a six-digit code that changes every minute provided by your authenticator app. The best part is authenticator apps like Google Authenticator are free and can be downloaded and installed on your mobile device in a few minutes.

Online risks are a fact of life. Every staff member has a role to play in protecting school district data, and these are 5 simple steps we all can take that make a huge difference.

About the Author:



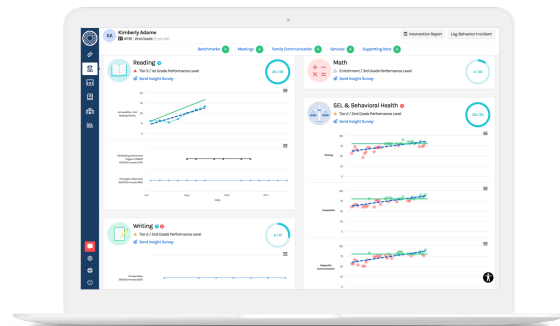
Craig Gooding

Director of Security Operations, Branching Minds


Craig has worked in technology for three decades starting out as a radar technician in the United States Marine Corps, moving on to a career in Information Technology and Information Security in multiple industries. A CISSP since 2007, he is focused on security through user education, surface reduction, enhanced visibility and automation.

It's time to make your MTSS vision a reality.


Protect your data & give your team all the insights and guidance they need to collaboratively achieve best practices so that your students, staff, and schools succeed.




[>>> REQUEST A DEMO TODAY <<](#)




common sense
Privacy Rating
by Common Sense




TrustEd Apps™
CERTIFIED
2023



Data Privacy Certification
by 1EdTech



SOC 2
TYPE 2



SOC 2 Type 2 Certification
by AICPA