CyberSecurity Tips For Students

8 WAYS TO KEEP YOUR DATA & IDENTITY SAFE THIS SCHOOL YEAR

BEWARE OF PUBLIC WIFI

Hackers are pretty sneaky and can create fake copies of known WIFI connection points. (Think McDonalds/Dunkin) Be sure of the WIFI network you're trying to connect to and always be cautious. Just because it's free, doesn't mean it's safe!

WATCH OUT FOR PHISHING EMAILS IMPERSONATING TRUSTED BRANDS

There has been a significant rise in phishing attacks: over 600% since the beginning of 2020. Microsoft being the top impersonated brand. If you are asked to log into an account to verify any data, don't click on any links in the email. Go directly to the website to access your info.

LOCK YOUR MOBILE DEVICES WHEN NOT IN USE

The first line of defense to keep someone from browsing through your data is having the Screen Lock enabled. Keep this locked with a strong password or your fingerprint. Ensure that the device Auto-locks after a short period of time.

PASSWORD SAFETY

Limit using the same password for multiple sites. Using long, nonsense phrases such as "I<3myblueBMXbike" or "Brady12sitheBomb" are going to be much stronger than "Mark1082" or easier to remember than "je*30B#Y+owRB0". Never use paper to store your passwords, use a program like LastPass or 1Password to keep them secure.

DON'T PLUG IN UNKNOWN USB DEVICES

USB devices can contain malware and viruses that are activated to auto-run as soon as they are plugged in. Only connect trusted devices. Be careful swapping USB drives with friends in case they have been unknowingly contaminated.

USE MULTI-FACTOR AUTHENTICATION

Especially for teens/college students - Set up and use Multi-Factor Authentication through SMS or apps like Authy or Google Authenticator. In the off-chance your password is compromised, hackers won't be able to access your accounts.

BE CAUTIOUS WITH APPS

Be mindful of what apps you are downloading and using on your devices. Many have very loose privacy policies on what information they collect and share with outside partners. If downloading financial apps, always visit the institution's website first and follow links to download their app directly rather than searching in the app store. That way you'll know for sure you are getting the legitimate application and not a copycat app out to steal your credentials.

PROVIDED BY:

ClearCom
IT Solutions

For more tips and information, visit:
https://www.clearcomit.com/blog