Cyber Safety: Seven Security Steps Teachers, Students & Families Can Protect Themselves

Remote learning and remote work bring an increased range of online activity into the home. Teachers, students, and their families are at increased risk for cybersecurity attacks and exploits. These six basic cyber safety practices can help remote learners protect themselves online anytime, anywhere.

1. Think before you click.

Avoid clicking on strange looking links or opening unexpected files. Not sure if a link looks strange? Hover over it with your mouse to see the content of the link. If the link looks at all suspicious or the information is too good to be true, do not click.

2. When in doubt, throw it out.

Avoid opening email from strangers. Opening an email from strangers is like opening the door of your house for a stranger. Even email that appears to be official, may not be. If you do not recognize the sender or the organization, don't open the message.

3. Passphrase it.

Create and use strong passphrases. A passphrase is a long password (14+ characters) that is easy to remember. "May the 4th be with you!" is an example of a passphrase that has letters, numbers and special characters. Tip: Use password management tools when they are available to you.

4. Confirm you are you.

Use any additional confirmation tools available to protect your accounts - for example, if you have the option to confirm login with a message to your cell phone, use it. If you have access to a multifactor authentication (MFA) option, such as using a specially generated PIN or one-time code, use it. MFA, sometimes referred to as two-factor authentication or 2FA, is a security enhancement that allows you to present two pieces of evidence – your credentials – when logging in to an account.

5. Secure your home WiFi

Make sure you have a strong password or passphrase on your home WiFi router. Make a list of all the devices connected to your home network, including computers, tablets, baby monitors, gaming consoles, TVs, security systems, and smart appliances. Check to make sure all those devices are protected by a strong password. Change the default passwords that come with these devices.

6. Update your tech.

Make sure devices, software and web browsers are up to date by turning on automatic updates. Using automatic updates ensures that critical security fixes are installed timely and automatically.

7. Know what you've got and where it is.

Do you know where your physical equipment is? Avoid leaving laptops, phones, etc. unattended. Make sure you know how to "untrust' lost equipment.