Microsoft

K-12 cybersecurity conversation guide

Helps parents, teachers, school administrators, and guardians have conversations teaching K-12 students about safe cyber practices.

Why does it matter?

Students are especially vulnerable to identity theft, as some may not discover it for years until they apply for a credit card or car loan! Additionally, hackers often view students as pathways into school networks, allowing them to steal information on teachers, staff, and parents.

Key points to discuss

Why you shouldn't click on unknown links

- Hackers have bad intentions, and they use phishing links to infiltrate your life!
- Unknown links come in all forms, including text messages, emails, search engines, websites, social media posts, direct messages, and more
- Sometimes hackers will try to create a friendship with you under false pretenses, or impersonate a family member, friend, teacher, or authority figure to get you to share information with them (this is called social engineering)
- Clicking on these links can have consequences that directly affect your life by ruining the device you love or even damaging your friendships if you are hacked and impersonated

Some red flags of phishing messages

- SMS phishing (or SMSishing) is a big problem for students in K-12
- Legitimate sources can misspell words or have errors sometimes, but be cautious when you see any errors in the messages that are sent to you
- Always hover over a link (including emails) before you click on it on your computer to see where it will go
- Threat and urgency are often conveyed in the message to scare you into acting before you can verify if the link is safe
- Always be suspicious of messages or calls that ask you for sensitive information (like login credentials)
- To trick you, sometimes hackers will offer you fake rewards to get you to turn over your information

A phishing message can have any mix of these issues

Why you should avoid scam ads

- Ads are paid to be put in front of you, and sometimes hackers pay to create scam ads that harvest your personal data and invade your privacy
- Watch out for the common phishing red flags in these scam advertisements, and pay extra attention to the link

It's important to speak up and get help if they click on a bad link

- Emphasize that asking for your help will not be punished or reprimanded. (We recommend a no-consequences self-reporting environment, when possible)
- If you click on a bad link, your life isn't over! You just need to tell an adult
- Once adults are involved, they can take the necessary steps to fix it
- But it can be hard to fix, so please be careful and be cautious when clicking!

Microsoft

Examples of when to be extra vigilant!

These are common scenarios when a student may be targeted with a phishing attempt. These examples are separated by age group, but you can pick and choose the most relevant scenarios for your students.

Elementary

- Researching information for a class report
- Looking for online math tutoring courses
- Searching for online videos & citing unverified information in schoolwork
- Messaging a teacher with a question

Secondary

- Searching for a customer support number
- Differentiating between ads and organic posts on social media
- Getting a message asking you to input your password or threatening that you'll be locked out of your account
- Being DM-ed with an unknown link and the other person urging you to click the link
- Searching for a summer job and applying for a scam company
- Researching and applying for college or trade school
- Looking for a doctor nearby
- Getting a friend request from a duplicated profile of someone you know

Links & Resources

- aka.ms/edu-cybersecurity-guide
- aka.ms/edu-cybersecurity
- aka.ms/what-is-phishing
- aka.ms/what-is-malware
- aka.ms/parental-control-apps