Activities for Protecting Your Identity and Computer for Elementary and Middle School Students

Overview

There are three posters about protecting your computer for this grade span. We recommend that these be hung together, either vertically or horizontally, in the order noted below and in a location you can easily point to. The bite-sized activities associated with each poster require 10-15 minutes offline and are structured to encourage discussion among students. They can easily be reused yearly.

Goal

To provide students with a simple checklist reminding them how to protect their identities and computer, while engaging them in creative and critical thinking to explore the concepts behind each tip.

Introduce: *It's important that we protect our computer from being infected or sick with bad software. The more thoughtful we are about protecting our computer, the less likely that everything we keep on our computer can be damaged.*

It's easy to protect our files—our school work, our music, our photos, our games—everything that we save on our computers—from loss by malware.

Malware is a short name for all software that is made to attack and hurt computers and all the stuff on our computers. Malware can even steal our personal identity information. Because we are all so connected today, if your computer gets infected or sick with malware, then my computer gets sick and infected too. Malware can attack a lot of computers very quickly.

Each of these three posters reminds us of one way to check if we have protected our computer and all of our stuff on our computer. Let's look at one way today and explore why experts say it is important.

Using the Poster "I think before I click." (15 minutes)

Ask: *Why is it important to make sure a link is OK before we click? Can't we just click and if it's not what we want or thought it would be, just go back?*

Encourage students to critically consider this question. If appropriate, introduce an analogy by asking them to consider if they can "go back"

after saying something. Point out that once they speak, the words are already "out" there and cannot be taken back.

Explain: *If we click a link that gets our computer sick with a malware infection, we cannot go back. Just clicking on links in email, instant messages, and online advertising can infect your computer.*

Probe and Discuss: *So how do you know if it is OK to click on a link? What might make you stop and think that there is something bad about a link that could cause trouble?*

Guide students in considering the possibilities below, while encouraging them to share stories of any strange links that they have encountered and what make them stop and think before clicking.

Read list below and discuss with students. In each situation, the student should be reminded to STOP and THINK why this link might be cause trouble.

- Links that tell you won a big prize or a lot of money
- Links from someone you don't know
- Links saying we won a contest
- Links from letters that were passed along to many people (chain letters)
- Links from messages that just look "weird"
- Links in that contain sill works or easy words are misspelled
- Links in that use bad grammar like maybe a small child might say
- Links from a friend saying he/she is in trouble and asking that you send money.
- Links to a page asking you for any personal information like your password

Probe and Discuss: *Sometimes we should even be careful about a link or an email attachment that "looks funny" even if it is from someone in our family, like our grandmother or grandfather or cousin or a really good friend. Can you think why we need to be careful of these links from people we know really well and love?*

Guide students to consider that it's very possible that a family member's account has been taken over by malware and they don't know it.

Explain: *Today most malware programs are written by thieves looking to make money from stealing personal financial information and passwords. So it's possible to receive an email that looks like it came*

from your grandma or a friend but really was made by a thieve. Sneaky link that look like it came from friends and includes an attachment can release malware and steal your passwords and personal information. So if a friend or family member sends an attachment you were not expecting, stop and ask your parent or call and ask about the attachment before you click.

Conclude: *Protecting your computer requires not just one check, but all three checks shown on the posters. Today we learned that to get this first check (point to poster) we need to stop before we click and think about a link or an email attachment that looks "weird" or strange to us.*

Using the Poster " I stop before I download." (15 minutes)

Display the poster and comment*: Stop before you download.*

Ask: What kinds of files do you download?
Students may name a variety of items from the list below.

Video games and instructions
Movies
Songs
Books
Photos
Free screen savers
Animations
Ringtones
Software

Guide students to realize that downloading may be something they routinely do.

Explain: *Stopping before you download is important because if your computer isn't protected, you can make your computer sick with infected software and ruin all of your stuff —including your games—on your computer.*

Probe: What should you do after you stop?

Guide students to consider that the safest strategy is to wait and ask an adult before they download something, especially if it is a computer at a friend's house or it is a computer that they share with their family. It would also be a good idea to ask if the family computer is protected from malware. There are companies that sell special software that can protect a computer from being attacked.

Conclude: *Protecting all of the important stuff on your computer requires not just one check, but all three checks shown on the posters. Today we learned that to get this second check (point to poster) we need to stop before downloading.*

Using the Poster, "My computer is a clean machine." (15 minutes)

Display the poster and ask: *What does it mean when experts say a computer is "clean"?*

Guide students to realize this isn't about wiping cookie crumbs off keyboards, but something much more serious—making certain that our computer doesn't become "dirty" with **malware**, software that attacks our computer and sometimes tries to steal personal identity information.

Explain: *Even when we* try very *hard to stop and think before clicking on a link or downloading something, it's still very easy to get tricked. Why? Because even though we are smart, so are the criminals and thieves that want to attack our computer.*

Probe: *Do you know anyone who has experienced problems with a computer because of a malware attack?*

Allow students to share anecdotes.

Explain: *Everyday more people everywhere are using computers and going online. And everyday there are more malware attacks infecting computers everywhere. Many companies sell special software that automatically protect computers, mobile phones and digital tablets from the latest malware attacks.*

Conclude: *Protecting your computer requires not just one check, but all three checks shown on the posters. Today we learned that to get the third check (point to poster) we need to make sure that the computers we use have the latest security software.*

Optional Class Activity

Invite the School or District Technology Director
Arrange a classroom discussion or a computer video conference. Have students prepare questions, which might include:

- What does our school do to protect our computers?
- What malware problems can school computers have?

- Has anything bad ever happened to our school computers?
- Do you know about a school that has had malware?
- Can we bring malware from our home computers to the school?