Activities for Protecting Your Identity and Computer for Middle and High 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 with contaminated software. The more thoughtful we are about protecting our computer, the less likely that our files and entire operating system can be damaged.*

It's easy and well worth the little effort it takes to protect our files—our work, our music, our photos, our games— everything that we save on our computers—from loss or destruction by malware.

Malware—the short way of referring to all malicious software, including viruses—is destructive software made to purposely harm and destroy a computer. Malware can even steal our personal identity information. And because we are all so connected today, if your computer gets infected or my computer gets infected, the damage spreads very, 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'm sure the link is from a trusted source." (15 minutes)

Ask: *Why is it important to make sure a link is from a trusted source? 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.

Explain: *Experts like to say "When in doubt, always err on the side of caution." Just delete the message and don't click. Simply clicking on links in*

email, tweets, posts, social networking sites, smart phone messages and online advertising can infect your computer.

Probe and Discuss: *What should make you suspicious that a link could cause trouble? A message claiming you've won a big prize or an offer that seems too good to be true is always suspicious. In what other situations should you to stop and* ***not*** *click?*

Guide students in brainstorming to include the possibilities below, while encouraging them to tell stories of suspicious links that they have encountered and what made them stop and think before clicking. Have students explain why the link might be suspicious.

- Links from someone you don't know
- Links that excitedly tell you to take urgent action
- Links in chain letters
- Links in messages that just look "weird"
- Links in a message that is clearly spam (junk mail)
- Links that just seem strange, even if from a good friend.
- Links within messages that use bad grammar or awkward phrasing or misspellings
- Links from a friend or stranger claiming he/she is in trouble and asking that you send money
- Links to a page asking you for any personal information, such as your password
- Links in messages that appear to be from a favorite store, asking you to update your account (Reputable companies never do this.)
- Links on a social networking site that say "watch this funny video of you"
- Links in messages that tell you to open an attachment
- Links in messages that warn you to take urgent action

Probe and Discuss: ***Why do experts tell us that we should be suspicious about a link or email attachment that "looks funny" even if it is from a family member, work colleague or your teacher?***

Guide students to consider that it's very possible a family member's account has been taken over by malware.

Explain: *Today most malware programs are written by sophisticated thieves looking to profit from stealing personal financial information or confidential data. Forged emails that appear to be from people you know and sneaky links that seem to come from friends can include attachments that release malware to steal your passwords and personal information. So if a friend or family member sends an attachment that you were not expecting, text her/him 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 suspicious.*

Using the Poster " I know what I am downloading." (15 minutes)

Display the poster and comment: *Experts say, "When in doubt do not download." Or, as the Greeks said, "Beware of strangers bearing gifts."*

Ask: *What kinds of files do you download?*

Students may name a variety of items from the list below.

Video games and instructions
Movies/Video
Songs
Books
Reports
Slideshow presentations
Photos
Graphics
Free screen savers
Animations
Ringtones
Software

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

Ask: *Stopping before you download is a good first step. Then think, "What should I think about at that moment?"*

Guide students to consider that they should check that their computer is protected and the reputation of a store or any other source before downloading.

Explain: *Start by making certain that the most current version of your browser is installed on your computer. Next, always check for the "lock" icon on the status bar, showing that you are on a secured web site and that the URL begins with "https" in the location bar. You should also consider using a safe searching tool that provides color-coded results showing that a site is safe and secure.*

Optional Online Activity: There are also free tools that can help you avoid unsecure sites. Have students search online for " safe search plug-in." Look at the free options available and explore how the different tools rank the safety and security of a site.

Conclude: *Protecting your private information and 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 and think 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 our files are not corrupted and our computer is not infected with contaminated software.

Explain: *Even when we* try very *conscientiously to stop and think before clicking on a link or download a file, it's still very easy to get tricked. That's because the number of online malware attacks is increasing dramatically as the number of Internet users continues to increase worldwide.*

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

Allow students to share anecdotes.

Optional Online Activities:

McAfee map showing malware threats by country
Extrapolate and infer:

- Which country in the chart shows the greatest amount of detected malware?
- Which country/countries is/are second?
- What inferences might you make from the data relative to population size wealth, or other factors?

McAfee Latest Threat Intelligence
Summarize:
Divide class into small groups with each exploring recent malware threats. Click on the malware name in the left-hand column. There are 50 pages listed.

Allow students to explore for some set time and then summarize and share any observations they make with their classmates.

Research online:

- How are your social network accounts vulnerable to malware?
- Students don't have much money, so why would they be targets of identity theft?
- Do cell phones need to be protected from malware?
- Spyware and viruses are the two best know types of malware. How do they hurt your ability to use your computer effectively?

Explain: *With the increasing sophistication and frequency of malware attacks, it's important to have the most current security software installed on our computers. The most current version of a web browser and operating system are equally important in defending against malware attacks. Many companies sell malware detection software to detect malware and update automatically to protect computers, mobile phones and digital tablets from the latest attacks.*

Conclude: *Protecting your computer and its contents 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 Homework Activity

For students to discuss with the owners of computers they use

- What security software is installed on your computer? Is it current?
- Do you have the most recent version of your browser?
- What setting have you chosen in your browser security preferences?
- Check settings they have on social networks

Go Online: Many computer security vendors offer free computer security checks. Click on the link below to double check your family computer with your parents or guardian at StaySafeOnline.org from the National CyberSecurity Alliance Free Security Check-ups and then share your results in class. Compare the different tools available, or go directly to McAfee's Free Security Checkup.