

Staying Safe Online

Lesson Plan

Students will learn how to protect themselves from scams, dangers, and misinformation in the online environment.

Lesson Objectives

At the end of the class, the student will:

* Be able to create strong passwords.
* Be able to identify and avoid harm caused by phishing emails, fraudulent job offers, and fake social network posts.
* Be able to identify and avoid pop-ups
* Be able to identify and avoid scams in the form of coupons and “something for nothing” offers.
* Understand how to evaluate websites for safety and reliability

Lesson Prep Work

(30 min, at a minimum, prior to student arrival)

* get in early to test for technology failure, because it will happen :-)
* Sign into email account.
* Load www.passwordmeter.com
* Open PowerPoint presentation
* Load Commoncraft Phishing video http://www.commoncraft.com/video/phishing-scams
* print handouts

Lesson Prerequisites

* Student must have completed lessons 1-3 of Computer Basics series

Lesson Outline

The lesson is completed in one (90) minute class session.

*(5)* Introduction

* Introduce instructor, students.
  + Ask students at introduction: What are you hoping to get from this class?
* Let students know it is okay to take phone calls, but ask them to put their phone on vibrate and answer calls outside the classroom.
* Inform students that they can sit back and watch if the class is too advanced.
* Inform students they can go to the bathroom, they don’t need permission.
* Show order in which class will happen. Explain scope of class.

*(5)* General Overview of Safety Online

* Just like the real world, the internet is both a dangerous and also a completely safe environment. And, just like the real world, it’s up to you to know how to protect yourself from the bad staff so you can enjoy the good stuff. This class is designed to give you those skills so you can use internet with confidence.

*(20)* Passwords

* Why do we need passwords?
  + *Explanation*
    - Usernames and Passwords help identify us as the owner of an account. Passwords are the secret code that allows us entrance to the tree house, or the membership card that lets us get into the bowling alley.
  + *Metaphor*
    - Like a lock and a key, the username and password must fit exactly to work.
  + *Discussion: What types of sites require passwords?*
    - Email
    - Business – buying and selling online
    - Banking
    - Paying bills
    - Social networks
    - Job applications
  + *Discussion: Should you write down your usernames and passwords?*
    - Pros:
      * Can help organize account information, especially as you accrue more and more.
    - Cons:
      * If you lose it or if it gets stolen, your online persona and account information is compromised.
    - Take precautions if you decide to write your passwords down. Store them in a safe location (like… a safe).
  + *Teachers Tip: If you have a high skill level class, you may want to recommend a password manager (like keepass).*
* How to make a strong password
  + *Explanation*
    - The stronger your password is, the more likely you are to keep prying eyes from your accounts. It’s important to make a password that is both difficult to guess/hack, but also memorable.
  + *PowerPoint slide: Characteristics of a good password*
    - At least 10 characters (the more the merrier)
    - Substitute letters for numbers
      * *Activity: Write letters on the board and have class transform them into numbers (for instance, E becomes 3, A becomes 4, I becomes 1 (or !)).*
    - Mix symbols, letters, and numbers.
    - Exclude all personal (identifying) information
      * *Discussion: What are examples of identifying info?*
        + Names of kids
        + Pets
        + Addresses
    - Hint: Use your favorite food, music, book, poem, lyrics, teacher or celebrity name. It’ll be easy to remember but hard to guess.
  + *Activity: Create a strong password and test it at www.passwordmeter.com*
    - Have class navigate open up Firefox browser and navigate to passwordmeter.com
    - Turn off hide characters on instructor PC for demo purposes. Also explain that “hide characters” merely masks what you’re typing.
    - Type in “elvis”
      * Point out how weak that password is.
    - Type in “Elvisrocks”
    - Type in “Elvis rocks!?”
    - Finally type “3lvisRocks!?” (it should show that the password is very strong)
  + *Activity: Students create a strong password at passwordmeter.com (indicate that they don’t need to use their current password, they can make a new one!).*
  + *Activity: Demo how to change password on email account.*
    - Navigate to Gmail (or another email account).
    - Click on the down arrow next to profile picture (in Gmail).
      * Make a special note to point out the importance of the down arrow.
    - Click on “Account”
    - Click on “Security”
    - Select “Change password”
    - If necessary, demo the same thing in Facebook (or Yahoo mail). Remember to point out similarities in the steps to change your password.

*(20)* Safety in Email

* What is phishing?
  + *Explanation*
    - Phishing is literally people “fishing” for your personal information. It’s an email fraud scam conducted for the purposes of information or identity theft.
  + *Activity: Watch Commoncraft phishing video (*[*http://commoncraft.com/video/phishing-scams*](http://commoncraft.com/video/phishing-scams)*)*
  + *PowerPoint Slide: How to recognize phishing emails*
    - Don’t address you by name
    - Will ask for personal information.
      * *Discussion: What is personal information?*
        + Name
        + Social security Number
        + Birth date
    - It may contain a threat or warning (for example, “Your account will be suspended if…”)
    - There may be spelling or grammar errors.
    - Will appear to be from a reliable organization (like a bank or government agency).
  + *PowerPoint Slide: Look at examples 1 and 2 of Phishing scams*
    - *Activity: Have a student read the emails out loud and then ask students to identify the “phishy” parts.*
    - Note: Phishing emails can also appear to come from personal friends. “Hi Simone! I’m stranded in Paris and my wallet was stolen! I don’t know what to do – could you please wire me $$$.” This is also phishing – your friend’s email has been taken over by phishers who are sending this same message to everyone in your friend’s address book.
* What should you do with a phishing email?
  + Don’t click on any links or attachments if you open the email
  + Delete the email
  + Do not respond to the email
  + Throw it back out to sea… (get it?)

*(20)* Other online Scams

* Safety while Job Searching
  + *Explanation*
    - Be aware of fake job offers.
    - Fake job offers will have the same trademarks as phishing emails
      * *Discuss: Ask class to name the characteristics of phishing emails*
    - Be extra careful on Craigslist – a good site, but still full of scams.
  + *PowerPoint slide: Job Phishing*
    - *Activity: Have a student read the email out loud and then ask the students to identify the “phishy” parts.*
* Deals/Coupons
  + *Explanation*
    - Bottom line: If it seems too good to be true, it is!
    - Will offer a great gift certificate or prize, like a laptop or an iPhone, but will ask for all your personal information.
    - Don’t enter your personal information
    - Deals/Coupons often appear as pop-ups
  + *PowerPoint slide: Fake deal/coupon examples*
* Pop-ups
  + *Explanation*
    - A pop-up is an online advertisement or message from your computer that opens in a separate window without you have clicked anything to open it.
    - Some pop-ups are necessary, others are not.
  + *PowerPoint slide: Necessary pop-up examples*
    - Typically a message from your operating system or a piece of legitimate software.
    - Remember to read it – oftentimes, you should just click “ok”.
  + *PowerPoint slide: Nefarious pop-up examples*
    - Why are they bad? At best they’re stealing personal information and at worst they could infect your computer.
  + *Discussion: How can you recognize an illegitimate pop-up?*
    - What can you do about bad pop-ups?
      * Don’t click any part of it (occasionally the X to close the window could be a link to a nasty website).
      * Hold down ALT+F4 on the keyboard (this will close whatever window is currently selected or most recently opened).
* Warning about Social Networks
  + *Explanation*
    - Posts and messages on Facebook will look like deal but they aren’t! They’ll have the same characteristics as phishing emails.

*(15)* Website Reliability

* Website evaluation
  + *Discuss: Why is it important to be able to evaluate a website for reliability?*
    - We look for important information online:
      * Government forms
      * Jobs
      * Medical information (among all kinds of other information)
    - It’s good to make sure the information we’re getting is accurate.
  + *Explanation*
    - Some searches are more important than others, if you’re looking up cat videos, website reliability isn’t that relevant. If you’re going to download a government form for a legal proceeding, it’s incredibly important that you are getting the form from a legitimate source.
  + *PowerPoint slide: 4 questions to determine website reliability*
    - Who – created it?
    - When – was it last updated?
    - Why – was it created?
    - What – does it say? What is the purpose of this website (look for bias)?
  + *PowerPoint slide: Domain name review*
    - *Activity: Students go to – irs.gov then irs.com. Students work with the person next to them to answer the 4 reliability questions about each website and determine which one’s the real deal.*
      * *Teachers Tip: You may want to point out the site map at the bottom of each page (specifically the “about us” section for irs.com). Also, time permitting; you can do a Google search about the legitimacy of irs.com.*
  + *PowerPoint slide: HTTP v. HTTPS*
    - Insecure vs. secure browsing. Look for it when entering private info like username, password, and/or financial information.
  + *Activity: Navigate to sign in page at yahoo.com.*
    - Point out the https in the address bar
    - Also point out the “lock” symbol at the far left of the address bar.

**(5)** **Conclusion**

* Go over handout, review material, and emphasize contact info & further resources on handout.
* Any questions? Final comments?
* Remind patrons to practice; assign take-home-practice - remind them they can ask for help
* Remind to take survey.

Appendix

What This Lesson Does Not Cover

* Anti-virus software – it is covered in protecting your computer. And staying safe online is more about preventative care.

Key Decisions

1. We teach passwordmeter.com rather than howsecureismypassword.net because you can unhide the characters you type in.
2. We do not teach how to report phishing emails because we’ve yet to see evidence of that being an effective strategy.

Links

<http://www.staysafeonline.org/stay-safe-online/>

<http://www.commoncraft.com/video/phishing-scams>

School of hard knocks