Design Document: Cybersecurity Basics

Class Description

Learn about common viruses, email and Internet safety, firewalls, and other security features and practices in this class.

Curriculum Track

Software & Apps

Audience

Adults

Course Length

90 minutes

Training Method

Lecture/Demo

Purpose

To inform patrons of basic security concepts and techniques to keep their computer and information safe while using the internet.

Equipment Requirements

Computer, projector, projector screen

Software Requirements

MS PowerPoint

Material Requirements

Pens or pencils, handouts, participant surveys

Learning Objectives

At the end of the session, learners will be able to:

- Explain what a virus is and what it can do
- List common antivirus protection software
- Identify popular web browsers and browser extensions for privacy
- Explain the best strategies for creating and remembering passwords
- Explain the safest web browsing, email and online purchase strategies
- Explain the importance of updates and how it relates to security
- Select the best backup strategy for their needs

Assessment Technique(s)

Question and answer (Lecture/Demo)

Content Outline

Agenda (2 mins)

- What is a Virus
- Antivirus Software
- Web Browsers

- Passwords
- Safe Internet Use
- Buying online
- Updating
- Backup

Topics, Talking Points, and Activities (85 Minutes)

- **What is a virus**
    - Explain that a **Virus** is a malicious set of code meant to harm you and/or your computer. Note that they can come from unsecured websites, spam emails or harmful files.
    - Talk about the types of viruses and what their effects are
        - **Spyware**: Watches what you type to attempt to record your SS#, Credit card info, etc.
        - **Ransomware**: Holds your computer/files hostage and prompts you for payment
        - **Worm**: Uses your computer resources and internet for nefarious means.
        - **Trojan Horse**: Pretends to be a real program to trick you into installing a virus
        - **Malware**: Attacks your computer resulting in malfunction, crash, or being non-responsive

- **Antivirus Software**
    - Explain that you can easily avoid and remove viruses with antivirus software
        - Talk about some of the **free** options. All of these options are about equally as good.
            - ✓ Defender free download for Windows 7 and is included in all newer versions of Windows
            - ✓ Avira
            - ✓ AVG
            - ✓ Avast
        - Talk about some of the **paid** options. The versions are in ranked order.
            - ✓ **Kaspersky**: Has been the best antivirus for many years in a row. It is the best paid security you can get for your computer
            - ✓ **BitDefender Plus**: A newer antivirus company but is highly recommended by PC magazine and in its top rated 2018
            - ✓ **Norton**: Old and trusted program. High quality product that recently had an overhaul.
            - ✓ **McAfee**: Old and trusted program. Like Norton, a high quality product for many years.
    - Discuss secondary programs to target specific types of viruses (free & paid)
        - **Malwarebytes**: specifically targets malware and can be installed alongside an antivirus **Spybot**: specifically targets spyware viruses and can be installed alongside an antivirus
    - Explain what a firewall is and some options
        - **Firewall**: program that monitors and blocks bad traffic trying to get into your computer.
        - **Windows firewall**: Firewall built into Windows. Works well for general computer use.
        - Firewalls that come with paid antiviruses such as Kaspersky and Norton are superior in protection to Windows fire wall

- **Web Browsers**
    - Discuss the safest web browsers for accessing the Internet. Explain that the difference between these browsers is minimal and they should choose one based off of features and preference.
    - **Google Chrome**: Ranked the fastest and safest web browser as of 2016

  - **Firefox**: Comes in a close second to Google Chrome and is also an excellent browser
  - **Windows Edge** (Windows 10 & up)/ **Safari** (Mac users): Explain how Edge is different from Internet Explorer. Explain that internet explorer is very bad for security. Both of these browsers come in 3rd place. They are quick and safe, but not quite as good as Firefox or Chrome.
  - **Opera**: is the weakest of main stream recommended browsers. It is speedy and has built in features other browsers do not have such as a free VPN and adblocker. Note: The free VPN is only in the Opera developer browser.
  - Explain what a browsers extension is and why they may want to install them on their computer. The previously discussed browsers support extensions, but extension availability varies.
  - Browser extensions are small apps that you can add to your browser that do very specific tasks.
    - **Ghostery**: Blocks ads and websites from being able to collect data from you.
    - **Adblocker Plus**: Blocks most ads/videos on webpages. Makes money from donations.
    - **Disconnect**: Blocks malicious trackers who are trying to expose you to malware and steal your identity. Makes money from donations
    - **HTTPS Everywhere:** Automatically switches HTTP websites to HTTPS to keep you secure.

- **Passwords**
  - Explain to the class the best ways to create the strongest possible passwords to protect your accounts. Suggest that they use the following rules when creating a password
    - Use a minimum of 8 characters, but longer is better
    - Use a long string of words
    - Add numbers, symbols, upper case, and lower case letters at the end
    - Never use the same password for multiple accounts
    - Write down your passwords and store them in a file cabinet or other safe easily remembered location (never save passwords on a word file in your computer!)
    - For the highest possible security do not let your web browser save your passwords.
  - You can save Passwords safely on a computer by using a proper program. These programs save and encrypt your passwords. Do your research and choose the product that gives you the best price for the features you need.
    - These programs are compatible with Android, IOS, Chrome, Firefox, and Safari
    - These programs offer more protection than saving passwords in a browser
      - ✓ Do you trust Google/Firefox/Microsoft more than a company who gets paid to keep your information safe?
    - Prices vary depending on the company and the amount of features you need.
      - ✓ Sticky Password is highly rated and has a price of $30 per year or $150 for life
      - ✓ Keeper has a free version or a fee of $30 a year
      - ✓ True Key has a free version or a fee of $20 a year

- **Safe Internet Use**
  - Explain that using common sense when clicking on a link or proceeding to a website will save you from 95% of all the dangers online. Ask yourself questions before proceeding.
  - Explain the safe practices strategies to use when downloading from websites
    - Do not click on popups - Sometimes pop-ups are required (the site will say so)
    - Only give out private information to a trusted site
    - Avoid clicking on strange links or advertisements

  - If it sounds too good to be true it usually is!!!
- Only download from official company websites
  - Make note of the “ad” marker next to the top searches
  - Explain that Google often pulls the company info to the right side of the screen and provides the official website there as well
  - Look at the URL to make sure that it is the correct site.
- Point out pop-ups or screens that may appear on blocked websites. Do not proceed.
  - In very rare occasions a good website could be blocked by your browser, but 99% of the time this will help you avoid danger.
- Use Google transparency report if you are not sure about a website. This site will tell you if there is any known danger from viruses with regards to this webpage
- Explain strategies to use with regards to email
  - Only open emails from trusted email addresses
  - Only download or click on links within emails from trusted email addresses
  - If your friends email does not sound like your friend, they were most likely hacked.
    - ✓ Inform them of this so they can change their password and delete the email
  - If an email asks for personal information and it is not your lawyer, doctor, accountant, etc. delete it and do not send them anything
  - If an email sounds sketchy, copy and paste the text into google to see if it shows up with any known scams
  - Big name companies will not contact you about problems. These companies already have your money and will wait for you to call tech support if you have issues. 99% of these emails or phone calls are scams.
- Explain that they can get email warning them about scams by going to consumer.ftc.gov/scam-alerts to sign up for the email alerts
- Talk about how you can check the security of your account with a website called haveibeenpwned.com.
  - Tell students that if their account has been breached to immediately change the password or even consider making a new account.
- Explain what 2-step Verification is and why it is good to have and increases security
  - Increases security by making you enter a number texted to you when you log into your email
    - ✓ Most major emails have this now such as Google, Yahoo, Outlook, etc.
    - ✓ You can make it so that you do not have to enter a code for specific computer IE your home computers and devices
  - If someone figures out your password and hacks your account, they will not be able to gain access without the verification number
    - ✓ This number will be texted to you so you will know right away if someone is trying to access your account.
- Show how to mark emails as Spam/Junk
  - Select the email you would like to block and click on the Spam/Junk button. Each email providers will display different options.
- Show people how to block email addresses permanently in Google Gmail
  1. Click on the settings in the top right corner
  2. Click on **filters and blocked addresses**
  3. Click on **create a new filter**
  4. Enter the email address or addresses and click on **create filter with this search**

5. Explain that you can block any email domain by filtering the email after the @ sign. Ex: if you type in gailborden.info after the @ sign it will block all emails from the library or staff.

- **Purchasing Online**
  - Explain that it is better to use a secure payment method instead of having your billing information on multiple websites
    - Some of the best options available are Paypal, Apple Pay, and Google Wallet.
  - Only make purchases from legitimate and safe webpages. Check scamadvisor.com.
  - Consider making purchases with a credit card that offers 2 step authentication. The cards will not be charged unless you verify the purchase via text message/other authentication.
- **Updating**
  - Explain that updating your computer keeps you safe from viruses, hacking, and bugs. Note that this can be set to install automatically or you can manually install updates – just stay on track.
    - Windows XP is no longer supported which could result in security issues
- **Privacy**
  - Explain that the following services/products are not required for staying safe while casually browsing the internet but can provide extra privacy measures for those concerned about data.
  - **How to Turn off Google Tracking -** Show students how to turn of Google tracking at the account level instead of on each individual device. (This will not disable apps, but may weaken or turn off some features)
    1. In Google Chrome, go to myaccount.google.com and sign-in.
    2. Click on Data and Personalization in the left-hand sidebar
    3. Select each activity type to toggle tracking on/off
  - Privacy Emails
    - **Proton Mail**: End to End Encryption for truly anonymous email. Which means that all emails you send or receive are encrypted to protect your messages.
    - **Hushmail**: End to End Encryption for truly anonymous email. Which means that all emails you send or receive are encrypted to protect your messages.
    - **Tutanota**: Canadian provider has been providing secure emails since 1999. They are the oldest and most trusted private email provider.
  - Explain and define what a VPN is and how it can benefit you.
    - A **VPN** (Virtual Private Network) service encrypts your browsing experience to prevent hackers, government, and your service provider from having access to your internet habits. This increases privacy, security, and provides access to previously blocked sites and media
  - Explain some VPN options. Suggest that they try Opera developer browser to get started.
    - Easiest is to download Opera developer browser for a free VPN built right into the browser
    - Some highly rated free VPNs are Total VPN, Cyber Ghost VPN, and Tunnel Bear.
    - Some highly rated pay VPNs are Total VPN, Private Internet Access BPN, and Nord VPN
  - Explain that private searching with specific websites offers the following perks:
    - These websites do not track or sell your personal information
    - They do not allow ads to target you
    - No biased search results from companies paying to get higher in the rankings
  - Offer the following sites as private searching options:
    - duckduckgo.com: Completely private experience with their own search engine

        - startpgage.com: Uses Google search and gives your search information to Google, but strips off all of your private information so you are not tracked or identifiable.
    - Talk about the Tor browser. Explain that this is not needed for safe internet browsing and that this is just for extra privacy
        - This browser prevents websites, hackers, and the government from tracking you by creating an anonymous browsing experience
        - How this works: Your computer sends a website request through several other computers/servers randomly. The website request is then sent back through the random order path instead of directly to your computer.

Wrap Up/Closing (3 min)

- Ask if there are any questions and answer any that were “parked” during the session
- Highlight the upcoming technology classes and share the types of topics that will be covered
- Thank participants for coming and ask them to complete the class survey before leaving