**Protecting The Elderly From Cybercrime:**

**A Community Education Approach**

**Curriculum Packet**

**Sydney Brazeau**

**2020**

**Sample Lesson Plan**

**Target Audience:**

Senior citizens age 65 and over

Content is also relevant to caregivers and family members of senior citizens

**Learning Objectives:**

Students will understand current cybercrime trends and how it relates to them as senior citizens.

Students will know how to access resources to prevent, mitigate, and report cybercrime.

Students will gain skills and techniques with which to avoid cybercrime.

**Materials/Supplies/Handouts Needed:**

Pens/pencils

Cybercrime handout

Assisted notes handout

**Technology Requirements:**

Projector and screen **or** large TV for displaying slide show presentation

Slide show viewer software

**Preparation:**

Advertise class in relevant areas

Obtain a sufficient space for the class

Partner with applicable local agencies or tech companies

Print off handouts and quiz

Sharpen pencils if necessary

Obtain snacks for class to increase attendance

**Activities:**

Quiz

Discussion

|  |  |  |
| --- | --- | --- |
| Time (minutes) | Activity | Purpose |
| 10 | Introduction | -Develops a rapport with students |
| 10 | Quiz | -Develops an understanding of the baseline cybersecurity knowledge of class |
| 10 | Quiz Review | -Starts students thinking about their role in cybersecurity |
| 5 | Handouts | -Assists students with vision or hearing difficulties during PowerPoint presentation  -Provides reference and note-taking materials |
| 20-30 | Slide Show Presentation | -Delivers core of cybersecurity information |
| 10-20 | Questions/Discussion | -Address student questions and revisit unclear terms  -Discuss cybercrimes and cybercrimes that students have encountered if they feel comfortable sharing  -Analyze actions the student took and how those actions would change after being presented with class information |
| 10 | Wrap-up | -Provide short overview of topics covered in class  -Direct students to further research and resources available in their community |
| 10-30 | Cookies/Coffee | -Food and drink are a way to increase attendance |

**Cybercrime Handout**

**Cybercrime Types**

* Ransomware
* Phishing
* Tech Support Scams
* Romance Scams
* Clickbait

**Avoiding Cybercrime**

Don’t interact with scammers

* Don’t respond to phishing e-mails
* Don’t open attachments
* Don’t click on links in e-mails

Set-up online banking

* Monitor regularly

Monitor current scams and cybercrime trends

* AARP Fraud Watch
* FTC Scam Alerts
* IC3 Consumer Alerts

**Mitigating Cybercrime**

Run updates regularly

* Operating system (OS) updates
* Application updates like Microsoft Word
* Anti-virus updates

Backup essential files

* Photos
* Important documents
* Use a disconnected external hard drive for backups

**If You are a Victim of a Cybercrime**

File a police report

* Obtain a copy

File IC3 and FTC reports

Initiate fraud alert on credit

Close accounts that the criminal has access to and change pins/passwords

* Bank accounts
* Online accounts

Update computer and anti-virus software

**How to…**

**Update your computer**

* Apple
  + Click on the Apple icon in the top left corner
  + Select “About This Mac”
  + A window should pop up with a button that says “Software update…”
  + Click the “Software update…” button to run updates
* Windows
  + Click on the “Start” button in the lower left corner
  + Type in “Update”
  + Select “Check for updates”
  + If updates are available, click “Install updates”
* Chromebook
  + Click on the clock in the lower right corner
  + Select the settings icon in the pop-up menu
  + Select “About Chrome OS” below the menu bar on the left side of the screen
  + Click “Check for updates” on the right side of the screen
  + Click “Restart” once updates have finished installing

**Update your anti-virus**

**Note:** Use trusted anti-virus software. Some malware can look like anti-virus software.

**Trusted anti-virus software examples:** Windows Defender, Norton, Avast, Bitdefender, Kaspersky, McAfee, Trend Micro, F-Secure, Intego, AVG Technologies, Webroot, ESET, Malwarebytes

* Windows Defender
  + - Click on the “Start” button in the lower left corner
    - Type in “Defender”
    - Select “Windows Defender Security Center”
    - Click “Virus & threat protection”
    - Click “Protection updates”
    - Click “Check for updates”
    - Install updates if available
* Malwarebytes for Windows
  + Click on the “Start” button in the lower left corner
  + Type in “Malwarebytes”
  + Select “Malwarebytes”
  + In the lower right corner of the dashboard, look for the word “Updates”
  + Click on the blue word next to the word “Updates” to check for updates
  + Install updates if available

**Set-up online banking**

* Navigate to your bank’s website
* On the home page under the sign-in, there should be a button labeled “Enroll in Online Banking” that leads to a form
* Fill out the form
* Choose a password at least 12 characters long
* Check your accounts regularly to detect unauthorized purchases and stop fraud early

**Set-up a credit freeze**

**Note:** Setting up a credit freeze does not affect your credit score. You have to set up a credit freeze individually with each of the three credit bureaus. Placing and lifting a credit freeze is free.

* Equifax
  + Visit <https://www.equifax.com/personal/credit-report-services/>
  + Select “Place A Freeze”
  + Fill out the form
  + Store your password in a secure place
    - You’ll need your password in order to unfreeze your account
  + Or call: 800-685-1111
* Experian
  + Visit <https://www.experian.com/help/>
  + Select “Security Freeze”
  + Select “Add a Security Freeze”
  + Select “Freeze my own credit file”
  + Fill out the form
  + Store your pin in a secure place
    - You’ll need your pin in order to unfreeze your account
  + Or call: 888-397-3742
* TransUnion
  + Visit <https://www.transunion.com/credit-help>
  + Select “Freeze Credit”
  + Select the “Add Freeze” button under “Freeze My Credit” heading
  + Fill out the form
  + Store your password in a secure place
    - You’ll need your password in order to unfreeze your account
  + Or call: 888-909-8872

**Set-up a fraud alert on your credit**

* General Information:
  + Setting up a fraud alert on your credit is free of charge
  + You should set up a fraud alert if your personal information has been stolen, lost, or involved in a breech
  + When you set up a fraud alert with one credit bureau, it issues a fraud alert to the other credit bureaus
* Equifax
  + Visit <https://www.equifax.com/personal/credit-report-services/>
  + Click on “Place an Alert” under the “Add a fraud or active duty alert” heading
  + Fill out the form
  + Store your password in a secure place
  + Renew fraud alert yearly
* Experian
  + Visit <https://www.experian.com/help/>
  + Click on “Fraud Alert”
  + Click on “Add a Fraud Alert”
  + Click on “Temporary fraud alert”
  + Scroll down to “Add a fraud alert using your personal information”
  + Fill out the form
  + Renew fraud alert yearly
* TransUnion
  + Visit <https://www.transunion.com/credit-help>
  + Click on “Fraud Alerts”
  + Click on “Add Fraud Alert” under the “Initial Fraud Alert – 1 Year” heading
  + Click on “Register” under the “Create an account” heading
  + Fill out the form
  + Renew fraud alert yearly
  + Or call: 800-680-7289

**Report a scam or identity theft to the FTC**

* FTC Complaint Assistant to report **fraud or scams**:
  + FTCComplaintAssistant.gov **or** ftc.gov/complaint
* For FTC complaints regarding **identity theft** visit:
  + IdentityTheft.gov
* Or call:
  + 1-877-FTC-HELP (1-877-382-4357)

**Report a cybercrime to the FBI**

* The FBI’s Internet Crime Complaints Center (IC3) handles cybercrimes
  + Visit ic3.gov
  + Click “File a Complaint”
  + Click “IC3.gov”
  + Click “I accept” after reading the FAQs (Frequently Asked Questions)
  + Fill out the form

**Report a scam to AARP**

* Visit AARP’s website to report a scam or search existing scams
  + Type AARP.org/money/scams-fraud/tracking-map in your search bar
  + Fill out the “Report a Scam” form
  + AARP scam reports are public, so don’t include personally identifiable information
* Or call AARP’s Fraud Watch Network Helpline:
  + 1-877-908-3360
  + Hours: Monday – Friday 7 am to 10 pm Eastern Time

Quiz

Answer with “True” or “False”

1. Setting up online banking increases your chances of cybercrime victimization.
2. Shaming scammers is an effective way to make them stop.
3. You should update your computer and your anti-virus software regularly.
4. Short passwords are better because they are easier to remember.
5. If you don’t use a computer, your personal information cannot be exploited by cybercriminals.
6. A person’s full name, social security number, driver’s license number, passport number, and e-mail address can be purchased for around $4 on the dark web.
7. Senior citizens are commonly targeted by scammers because of their good credit scores.
8. You should not click links in unsolicited or suspicious e-mails.
9. Wire transfers can be reversed.
10. If a person you meet online asks for your bank account information saying that they will give you money, they are most likely a scammer.

**Quiz Answer Key**

1. Setting up online banking increases your chances of cybercrime victimization.
   1. **False**. Online banking decreases the risk of identity theft and fraud victimization (Pak, et al., 2018).
2. Shaming scammers is an effective way to make them stop.
   1. **False**. Scammers are often highly trained individuals with lots of experience in social engineering (Cross, 2016).
3. You should update your computer and your anti-virus software regularly.
   1. **True.** Computers and anti-virus software require regular updates to stay current and protected against the latest threats (Christensson, 2010).
4. Short passwords are better because they are easier to remember.
   1. **False.** Long, unique passwords are recommended because they are harder for hackers to crack. NIST recommends a minimum password length of eight characters (Grassi, Fenton, Newton, Perlner, Regensheid, Burr, & Richer, 2017).
5. If you don’t use a computer, your personal information cannot be exploited by cybercriminals.
   1. **False**. Even if you don’t use a computer, your personal information is most likely available online through public records, genealogy websites, and donation recognitions in newsletters, and more (Cross, 2016).
6. A person’s full name, social security number, driver’s license number, passport number, and e-mail address can be purchased for around $4 on the dark web.
   1. **True**. The exact purchase amount varies based on a victim’s credit score and other factors, but a packet of information with person’s full name, SSN, driver’s license number, passport number and e-mail sells for around $4 on the dark web as of 2020 (Damiani, 2020).
7. Senior citizens are commonly targeted by scammers because of their good credit scores.
   1. **True**. The stereotype of senior citizens having good credit scores and the ability to create long lines of credit makes them a target for scammers (Cross, 2016).
8. You should not click links in unsolicited or suspicious e-mails.
   1. **True.** These links can lead a user to malware, or a website designed to steal their personal information (AFA, 2020).
9. Wire transfers can be reversed.
   1. **False.** Wire transfers cannot be reversed once the recipient’s bank has accepted the payment order (Baylor, 2019). There is no exception for fraud victims.
10. If a person you meet online asks for your bank account information saying that they will give you money, they are most likely a scammer.
    1. **True.** The FBI reports that if someone offers to deposit money in your bank account in exchange for your banking details, it is most likely a scammer trying to carry out fraud or theft (FBI, n.d.). This is a common tactic used in romance scams (FBI, n.d.)

**Framework**

**Communication**

* Provide written information to supplement orally presented information
* Adapt for cultural and geographic communication differences
  + Rate of speech, length of class, resources available
* Be mindful of communication difficulties such as hearing or vision loss
  + Large-print font, microphones, handouts

**Class topics**

* Password/Authentication management
  + Retrieved latest recommendations from NIST
* Top cybercrime and fraud trends
  + Retrieve top 5 or top 10 cybercrime trends by frequency and by financial impact from IC3 yearly report
  + Retrieve fraud data from FTC yearly report
* Skills and tools
  + Social engineering prevention
  + How to run and/or automate operating system and application updates
  + Analyze top cybercrime trends
  + Social media literacy

**Trusted Sources**

* AARP
* IC3/FBI
* FTC
* NIS