TEACHER GUIDE

LEARNING UNDEFEATED
Educate | Elevate | Empower

Who Are Your Friends: A Cybersecurity Mystery

Topic(s): Password safety, social engineering, phishing, ciphers

Grade level(s): 5th-10th grades

Time: 45-60 minutes

CSTA Standards: 1B-NI-05, 2-NI-05, 2-NI-06, 2-IC-23

Maryland Computer Science Standards: 7.NI.C.01, 7.IC.SLE.01, 8.NI.C.01, 10.NI.C.05, 12.NI.C.01

Virginia Computer Science Standards of Learning: 5.9, 5.10, 6.6, 7.6, 7.7, 8.6, 8.7, 8.9, 8.13, CSF.7

ACTIVITY OVERVIEW

Who Are Your Friends? is an activity developed by Northrop Grumman and Learning Undefeated to help students understand safe internet use through the lens of cybersecurity. From social engineering to simple phishing emails, every internet user can be targeted for personal information. Most often, the targeted information is credit card and banking information, followed by social security numbers, usernames and passwords. This information can allow someone to masquerade as a legitimate trusted source.

In this lab, students will act as members of the school's cyber-defense team to help a student clear his name of accusations and walk the stage at graduation. Students will investigate the victim's social media account and email for clues. Then provided objects found in the victim's locker, students will break codes to determine who broke into the victim's social account.

ALIGNMENT TO STANDARDS

CSTA Standards

1B-NI-05. Discuss real-world cybersecurity problems and how personal information can be protected.

2-NI-05. Explain how physical and digital security measures protect electronic information.

2-NI-06. Apply multiple methods of encryption to model the secure transmission of information.

2-IC-23. Describe tradeoffs between allowing information to be public and keeping information private and secure.

Maryland Computer Science Standards

5.NI.C.01. Define personal identifiable information (e.g., digital footprint) and why it should be protected as related to real-world cybersecurity problems.

5.NI.C.02. Discuss real-world cybersecurity problems and explain how personal information can be protected (e.g., antivirus software, backing up data, strong passwords).

7.NI.C.01. Explain how to protect electronic information using both physical (hard drive) and digital measures; explain existing cybersecurity concerns with the internet and the systems it uses.

7.IC.SLE.01. Explain the connection between the longevity of data on the internet, personal online identity, and personal privacy.

8.NI.C.01. Evaluate physical and digital security measures that have been developed and implemented to protect electronic information; discuss the impacts of hacking, ransomware, scams, fake scams, and ethical/legal concerns.

12.NI.C.01. Compare and refine ways software developers protect devices and information from unauthorized access including complex encryption algorithms such as public key encryption.

10.NI.C.05. Recognize and prevent social engineering attacks. Differentiate between legitimate and fraudulent information.

Virginia Computer Science Standards of Learning

5.9. The student will evaluate and solve problems that relate to inappropriate use of computing devices and networks.

5.10. The student will determine whether passwords are strong, explain why strong passwords should be used, and demonstrate proper use and protection of personal passwords.

6.6. The student will identify physical and digital security measures used to protect electronic information.

7.6. The student will describe how physical and digital security measures protect electronic information.

7.7. The student will identify existing cybersecurity concerns associated with Internet use and Internet-based systems and potential options to address these issues.

8.6. The student will evaluate physical and digital security measures used to protect electronic information.

8.7. The student will identify impacts of hacking, ransomware, scams, fake vulnerability scans, and the ethical and legal concerns involved. Exclusion: Students do not need to implement solutions.

8.9. The student will describe tradeoffs between allowing information to be public and keeping information private

8.13. The student will identify existing cybersecurity concerns associated with Internet use and Internet-based systems and potential options to address these issues.

CSF.7. The student will explain typical tradeoffs between usability and security and recommend security measures in a given scenario based on these (or other) tradeoffs.

LEARNING OUTCOMES

Students will know:

- Examples of password security check questions.
- Signs of a phishing attack.
- How to decipher a Caesar shift cipher.
- What social engineering is.

Students will understand:

- The importance of strong passwords.
- The ways shared personal information can be used maliciously

Students will be able to:

- Analyze social media and email usage for suspicious content.
- Use inferences to solve ciphers, including a Caesar shift cipher.
- Identify social engineering techniques and phishing attacks.

BACKGROUND INFORMATION

Social Engineering

Social Engineering is a technique used to deceive a targeted end user into giving up sensitive information that can be used in infrastructure recognizance, criminal activity or to gain access to sensitive institutional data containing personally-identifiable information commonly referred to as PII. Most often, the targeted information is credit card and banking information, followed by social security numbers, usernames and passwords. The social engineer may use e-mails, voice messages, phone calls or even in-person visits masquerading as a legitimate trusted source such as a parent, end user, vendor or student.

The language used when contacted by the social engineer is often persuasively urgent in context such as: "please enter your password before your account expires" or "to increase your quota, please log into your account now" The social engineer may also use "verification of configuration" language during a phone call or in-person visit to the targeted location or individual that appears legitimate and official in nature.

https://pace.edu/its/it-security/social-engineering

Phishing Attacks

Phishing attacks are a subset of social engineering strategy that imitate a trusted source and concoct a seemingly logical scenario for handing over login credentials or other sensitive personal data. According to Webroot data, financial institutions represent the vast majority of impersonated companies and, according to Verizon's annual Data Breach Investigations Report, social engineering attacks including phishing and pretexting (see below) are responsible for 93% of successful data breaches.

- Using a compelling story or pretext, these messages may:
    - Urgently ask for your help. Your 'friend' is stuck in country X, has been robbed, beaten, and is in the hospital. They need you to send money so they can get home and they tell you how to send the money to the criminal.
- Use phishing attempts with a legitimate-seeming background.
    - Typically, a phisher sends an e-mail, IM, comment, or text message that appears to come from a legitimate, popular company, bank, school, or institution.
- Ask you to donate to their charitable fundraiser, or some other cause.
    - Likely with instructions on how to send the money to the criminal. Preying on kindness and generosity, these phishers ask for aid or support for whatever disaster, political campaign, or charity is momentarily top-of-mind.
- Present a problem that requires you to "verify" your information by clicking on the displayed link and providing information in their form.
    - The link location may look very legitimate with all the right logos, and content (in fact, the criminals may have copied the exact format and content of the legitimate site). Because everything looks legitimate, you trust the email and the phony site and provide whatever information the crook is asking for. These types of phishing scams often include a warning of what will happen if you fail to act soon because criminals know that if they can get you to act before you think, you're more likely to fall for their phishing attempt.

- Notify you that you're a 'winner.'
    - Maybe the email claims to be from a lottery, or a dead relative, or the millionth person to click on their site, etc. In order to give you your 'winnings' you have to provide information about your bank routing so they know how to send it to you or give your address and phone number so they can send the prize, and you may also be asked to prove who you are often including your social security number. These are the 'greed phishes' where even if the story pretext is thin, people want what is offered and fall for it by giving away their information, then having their bank account emptied, and identity stolen.
- Pose as a boss or coworker.
    - It may ask for an update on an important, proprietary project your company is currently working on, for payment information pertaining to a company credit card, or some other inquiry masquerading as day-to-day business.

https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering

Inference

Inference is simply guessing passwords from information you know about users — such as their date of birth, favorite television show, or phone numbers. It sounds silly, but criminals often determine their victims' passwords simply by guessing them!

The best defense against an inference attack is to educate users about creating secure passwords that don't include information that can be associated with them. Outside of certain password complexity filters, it's often not easy to enforce this practice with technical controls. So, you need a sound security policy and ongoing security awareness and training to remind users of the importance of secure password creation.

https://www.dummies.com/programming/networking/how-hackers-crack-passwords/

Password Strength

The strength of passwords as an authentication control is more important than ever before. Cyber-criminals are increasingly using automated password cracking tools to identify passwords in a matter of seconds. Our 2015 Trustwave Global Security Report revealed that out of a password sample size of 499,556 hashed passwords, our experts cracked 51 percent of them within 24 hours and 88 percent within two weeks.

Our 2015 Trustwave Global Security Report reveals that it can only take one day to crack an eight-character password in most instances, whereas it takes an average of 591 days to crack a 10 character password. With this in mind, it is recommended that policies should be put in place that require employees to change their passwords on a regular basis, for example every 60 days. Furthermore, administrators should enforce character complexity rules and length requirements of 10 characters or more for all password policies.

Despite the fact that weak passwords can lead to a data breach, they are expected to remain as an authentication control for the foreseeable future. In order to make passwords stronger and increase the security of businesses' sensitive information, employees must be educated as to what represents a strong password.

Beyond using strong passwords, implementing two-factor authentication also helps strengthen security. Two-factor authentication combines “something you possess”, like a code sent via text message, with “something you know”, a password. This makes it more difficult for attackers to gain control of an account because they would need to compromise both modes of authentication. Moreover, should a single account become compromised by an attacker, two-factor authentication would thwart attempts to progress the compromised networks, a password reuse would become a negated (or at least mitigated) attack vector due to the second factor requirement.

https://www.informationsecuritybuzz.com/articles/the-importance-of-strong-passwords/

By granting anyone else your user credentials, you are seriously compromising the security of your account, because from the moment they have access, you don’t know what they are going to do with your access details.

They may write them down and store in an insecure location, they may store it on an insecure or compromised device (Or a device that is later compromised). Or you may have emailed it to them, which is an inherently insecure messaging system.

Most likely the person you have trusted with your account details didn’t mean to compromise your account, but they likely haven’t thought through the wider implications of the account getting compromised and thus will not take necessary steps to secure the information.

https://swgfl.org.uk/magazine/why-sharing-passwords-is-a-bad-idea/

PRE-LABORATORY ACTIVITY

Discuss with students how passwords can be strengthened: character length, letter case (upper and lowercase), symbols, numbers, and nonwords.

Have students compete to determine who can create the strongest password (i.e. the password that would take the longest to crack via brute strength).

https://www.passwordmonster.com/

POST-LABORATORY ACTIVITY

Use NOVA Lab’s Cybersecurity Lab to have students explore more about passwords, coding and how to defeat malicious hackers.

https://www.pbs.org/wgbh/nova/labs/lab/cyber/

ACTIVITY PREPARATIONS

This activity can be run a couple different ways depending on the equipment available.

1. On MXLab (computers and tablets)
    a. Computers at each station will be used for the email portion and a USB drive will be in each cryptex. The USB can be connected to the computer and analyzed once the password is cracked.
2. Shortened version (no cryptex, tablets only)
    a. There will be two sets of tablets, one set that contains the email and social media portions and another set password locked that acts as the USB portion.
    b. Instead of information being stored in the cryptex, students are provided the locked tablet, hint/note, and notebook as clues after the email portion of the activity.

Day Before Activity
Ensure tablets are charged for activity

Day of Activity

- Turn on tablets and computers, if using them.
- Set Up Adobe XD:
    - The social media app "TheBook" is stored in the Adobe XD app. This is accessible from the home screen
    - It should be logged in to the appropriate account, but if it asks to sign in use the following info:
        - Select sign in with Adobe Account
            - Username: riley.bread02@gmail.com
            - Password: Notsecurepassword123
    - Once logged in, press the cloud symbol in the bottom left.
    - A list of three files should appear. The top file is the one that is already downloaded to the device and the one that should be used for this activity. Click this file to open it.
- If using computers, open the Thunderbird application to show the email files.
- Set up the Cryptex
    - Open the cryptex by lining up the rings at the triangles to spell the word "CIPHER".
        - The cryptex should pull apart if the rings are aligned properly
    - Inside the cryptex should be the following:
        - hint/note and USB drive.
    - Close and relock (shuffle letters) the cipher.

Student Station Set Up

1. On MXLab
    a. One table of six will need a computer keyboard and mouse to share.
    b. Each pair at the table will have a tablet opened to TheBook
2. Shortened Version
    a. Each pair will have a tablet opened to TheBook

To be distributed throughout the activity

1. On MXLab
    a. Cryptex (to be shared with everyone at a table)
    b. Journal
2. Shortened version
    a. Journal with hint/note
    b. Locked tablet (Password: qwertyuiop)

LESSON PLAN

Introduction (5 minutes)

- Explain that today they will be learning about cybersecurity in the context of an account hacking.
- Ask students if they have ever had a social media account hacked or know someone who has. If they are comfortable sharing, they can elaborate on what was hacked and how it was hacked (if they know).
- Explain that accounts ranging from social media to email to bank accounts are hacked everyday. Explain that there are some practices we can use to spot suspicious offenders who might be trying to gain access to your account and ways to keep your account secure.
- Introduce the narrative for today's activity:
    - Shaun Penner, a student at Gaines High School in Baltimore, was looking forward to graduation and all the fun activities that come with the end of senior year. Shaun and his close friends, Kaitlin and Brandon, are inseparable. They spend every day after school together and even share their social media accounts with each other. They love playing games and sharing jokes on their social media until one day, a joke about school trespassing is posted on Shaun's profile. In the photo it looks like Shaun was a part of the school prank, filling the hallway floor with cups of water. Shaun claims he didn't do it but the school learned of this post and banned him from walking the stage at graduation. Shaun is devastated and calls on you, a member of the cyber-defense team, to help clear his name and keep his graduation plans intact.
- Explain that some of those closest to Shaun are the primary suspects. Information about each suspect can be found on the first page of the handout.

Part 1: Social Media Investigation (10-15 minutes)

- Explain that because the social media account was hacked, looking through that account is the best place to start.
- Instruct students to use the provided tablet to access Shaun's social media account on TheBook.
    - Review how to navigate the app.
        - To see a person's profile page, tap their profile picture.
        - To go back to the home page, tape the house image or back arrow in the top left.
        - Remind students that they are logged into Shaun's account and therefore have access to his direct messages (DMs) as well. To get to these, go to Shaun's profile and select messages.
- Allow students 10-15 minutes to look through the app and record any suspicious activity for each suspect on page 2 of their handout.
- Regroup to discuss what was found. Ask students if they found anything suspicious or odd.
    - Some might notice that Kaitlin has some odd messages in her DM with Shaun and Brandon. She says "I don't know what to do", then quickly says "Sorry wrong person/chat". It makes it seem like she might feel guilty about the hacking but accidently sent the message to Shaun instead of another friend.

- Some might notice that in the messages with Breana, Breana asks some odd questions (favorite movie, do you have pets, pet names). Though this could be benign, many of these questions could also be security questions.
    - Explain to students that one of the ways software developers can keep our information safe is the number of hurdles they place in the way of a hacker. For example, if an account is accessed from a new device or new location, after a username and password are input, they may ask you to answer security questions that you set up when the account was made. They may also utilize two factor authentication, where they send a code to the email or phone number attached to the account to verify that you are the true owner of the account.

Part 2: Email Investigation (10-15 minutes)

- **If on MXLab,** direct student attention to the computer screens and the email inbox visible. Explain to students that all of the emails shown in the inbox are the emails Shaun received in the weeks leading up to the hacking.
- **If doing the shortened version,** have students navigate to the tablet's home screen.
    - Press the button at the bottom of the screen (if present) or swipe up from the bottom to then select the square symbol in the middle bottom of the screen.
- Direct students attention to the folder of PDFs on the home screen labeled "Shaun's Inbox". Explain that in this folder are PDFs of the emails Shaun received in the few weeks leading up to the time of the hacking.
- Allow students 10-15 minutes to look through the emails and record any suspicious activity for each suspect on page 3 of their handout.
- Regroup to discuss what was found. Ask students if they found anything suspicious or odd.
    - The most suspicious email that is linked to this case is the "Security Alert". This contains a link to update the password for "TheBook" in addition to a pet charity at the bottom. You can speak to the content that should be in password change emails, but it is not common for other advertisements to be there. Students might recognize the dog in the photo in that email from the dog Breana posted on TheBook.
    - There are a few phishing email examples in this set, including "Hello my friendo", the Taco Bell Scholarship email, and Security Alert.
    - You can discuss some of the ways to identify phishing attacks using the acronym RUIN:
        - R: Random- the email comes from someone you've never talked to or in general just seems to come out of the blue
        - U: Urgent- the email indicates that something has to be done quickly or else something bad might happen
        - I: Impersonal- the email does not include any information specific to you, meaning that it could have been sent out to a long list of people
        - N: Non-specific- the email might say you've won a prize but not what the prize is, who it's associated with, or how you qualified
- Ask students who they think the primary suspect is at this point in our investigation.
    - Answers will vary, but Breana's connection to the security questions and the security alert email may bring her to the top of the list.

Part 3: Cryptex Challenge/Caesar Cipher (15-20 minutes)

- **If on MXLab,** explain that in the week following Shaun's hacking, he found a cryptex and a notebook in his locker that did not belong to him. He thinks that the items are somehow related to the hacking investigation and brings them to us for further analysis.
    - Pass out these materials to the tables.
- Instruct students to try to open the cryptex. If we think this ties back to our suspect, what six letter words might relate to them.
    - Hints you can give students: what types of topics or themes are commonly used for passwords: birthdates, anniversaries, family member names, pet names
    - If students need more guidance, tell them that we think this might belong to Breana. Ask students if we know any personal information about her. (They can reference back to TheBook.)
        - Password: CIPHER
- Once students have opened the cryptex, they will find the hint/note and USB inside.
- Direct students to the USB ports next to each display and instruct students to plug in the USB drive. This will automatically open a file explorer window.
- Instruct students to select the application (.exe file). This will open a window and require a password for entry.
- Using the notebook, hint/note and the provided journal, students will work to determine the password for the the USB.
    - The journal gives an example of a Caesar shift cipher.
    - In the note provided, all of the "K" are underlined and on the back indicates that the number of Ks is important.
    - The number of Ks is the key for their shift cipher telling them how many spaces to shift the alphabet.
    - There are 10 Ks, so the alphabet shifts to have A start at letter K. Once they have the plaintext alphabet written out, they can decrypt the encoded password
        - Password is qwertyuiop (all lowercase)
- **If doing the shortened version,** explain that in the week following Shaun's hacking, he found a hint/note, notebook, and tablet in his locker that did not belong to him. He thinks that the items are somehow related to the hacking investigation and brings them to us for further analysis.
    - Pass out these materials to the tables.
- Instruct students to try to access the tablet.
    - They can't it's locked with a password
- Using the hint/note and the provided journal, students will work to determine the password for the tablet.
    - The journal gives an example of a Caesar shift cipher.
    - In the note provided, all of the "K" are underlined and on the back indicates that the number of Ks is important.
    - The number of Ks is the key for their shift caepher telling them how many spaces to shift the alphabet.
    - There are 10 Ks, so the alphabet shifts to have A start at letter K. Once they have the plaintext alphabet written out, they can decrypt the encoded password
        - Password is qwertyuiop (all lowercase)
- Once students have accessed the USB/tablet, instruct them to look through the files to determine its owner and if it helps determine who hacked into Shaun's account.

Part 4: Wrap Up (5-10 minutes)

- Have students share their ideas and theories about who they think hacked into Shaun's account, how they did it, and why.
    - The intended answer: Kaitlin posted the picture as she was part of the prank, but thought it would be funny to post it on Shaun's account. She used the Security Alert email to get Shaun to "change his password" but it actually just gave her his current password. She wasn't being malicious and didn't think the school admin would get involved.