Bits N' Bytes Cybersecurity Education

Classroom + BNBCE Collaboration

Time: approx. 2 hours: 25 minutes per station

Ages: 6th - 8th grade

Materials: Whiteboards or blank paper, pens or markers, computers, images and tables found in this instruction guide, worksheets found in the shared folder.

Goal: Students will learn the basics of securing their devices from outside interference and cyber-criminals, in order to protect their data and identity online. The ultimate idea of this lesson is for students to understand the state of current cyber-threats occurring in our world and leave knowing how to manage their own risk to help reduce this global loss.

Background: The dictionary definition of cybersecurity is any and all measures taken to protect a computer or computer system from unauthorized access or attack. Cybersecurity has always existed, but in the last ten years, paralleled with the revolutionary transition of corporations going completely digital, this idea of cybersecurity has become more of a priority for companies, governments, and citizens. The reason why the importance of this issue has progressively increased is because companies like Amazon, Google, and Uber, continue to grow their massive “data banks,” storing valuable information about the consumer, including names of consumers, email addresses, Social Security numbers, credit scores, and valuable information about the company itself, including classified details and financial information. If the “bad guys”, or cyber-criminals, were to gain access to this digital data, it would cause great disruption for both our citizens and the internal systems of the company. While we are seeing over 1 million cyber-attacks on corporations daily, we are also now seeing a rise in state-to-state interference, as states build larger criminal cyber-armies to take down national infrastructure and attack global networks, since they know it would cause chaos in cities. However, in every well-organized nation and corporation, big and small, high-powered, well-equipped teams are put in place to wear their “white-hats,” intercept threats dynamically, and stand as defence. While these teams are highly-trained, the users on the consumer end, using these devices and services, also need to be aware and equipped to handle the threats that cyber-criminals direct to us. In the future, every citizen will have to deal with these problems. That is why if we can learn the basic principles of cybersecurity, we can help protect our own devices and our community stay safe and secure online.

Bits N' Bytes Cybersecurity Education

Instructor Procedure: Be sure you have filled out the BNBCE data collection survey here: https://goo.gl/forms/ncM7xLjLrb41O5iB3. You are ready! Note that this curriculum need not be used in station format as it is organized: educators may take creative freedom in organizing each station as a class discussion!

Number each table 1-5. Seat one volunteer at each table. Split the whole group so that there are an even number of students in each group. The groups will be rotating through 5 stations, spending about **25 minutes at each station**: Exploring Encryption, Phishing for Scams, Understanding Your Online Privacy, What's Your Password?, and Understanding World Crises. Before you begin, please take a minute to have the students fill out the pre/post surveys,

- ★ Pre-survey: LINK FROM DRIVE
- ★ Post-survey: LINK FROM DRIVE

Station instructions are as follows (can be used separately):

Instructions Station 1: Exploring Encryption

Have the students discuss what they believe encryption is. After about 5 minutes of discussion, reveal the definition of encryption: In cryptography, **encryption** is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Explain how over time, different ciphers have been developed to help encode/decode messages confidential information, and how companies still use some of the more complex ciphers for secure communication. Share that today, we will be exploring

- ➔ **Caesar Cipher**
  - ◆ Write this example of an encrypted word on a piece of paper/whiteboard using the Caesar Cipher and have the students brainstorm what they believe the pattern is in the encryption:

Plaintext: Encryption is fun!	**Ciphertext:** Fodszqujpo jt gvo!

  - ◆ Explain that a **caesar cipher** shifts all the letters in the plaintext by a certain predetermined amount to create the ciphertext, using the typical alphabet below. In the example above, the key was **1.**
  - ◆ Have the students practice this with each other. Have one student write down a word and another chose a key number. The students should work together to encrypt the message.
  - ◆ Have the students decrypt this message without knowing the key:

Bits N' Bytes Cybersecurity Education

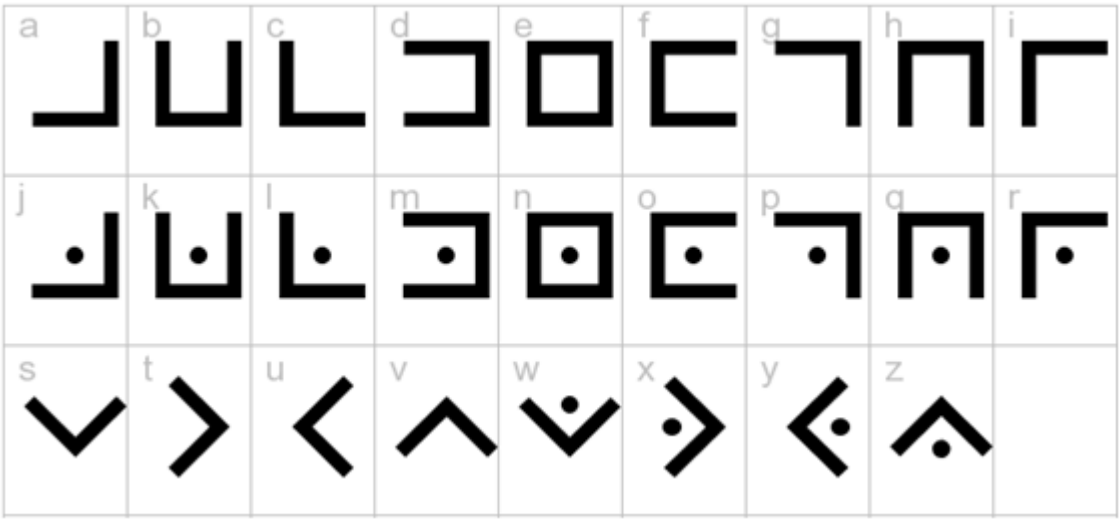
Ciphertext: bj fwj hdgjwxyfwx!	**Plaintext?** ___ _____ _____!

Key: 5, Answer: we are cyberstars!

a	b	c	d	e	f	g
h	i	j	k	l	m	n
o	p	q	r	s	t	u
v	w	x	y	z		

➔ **Rosicrucian Cipher:**

- Explain that a Rosicrucian Cipher, or a Pigpen Cipher, uses symbols to represent letters and was first published in 1531. Using the key below, have the students encrypt and decrypt the following words on their whiteboards:



-

Bits N' Bytes Cybersecurity Education

Plaintext	Ciphertext
Encoding	
Software	
Algorithm	
	
Clue: they used to be the population that used this type of cipher the most!	

- Review the meaning of encryption and decryption with the group.

PLUGGED CORNER

Have them explore these sites on their laptop device:

- https://cryptii.com/pipes/caesar-cipher: Have the kids challenge each other to decode and encode

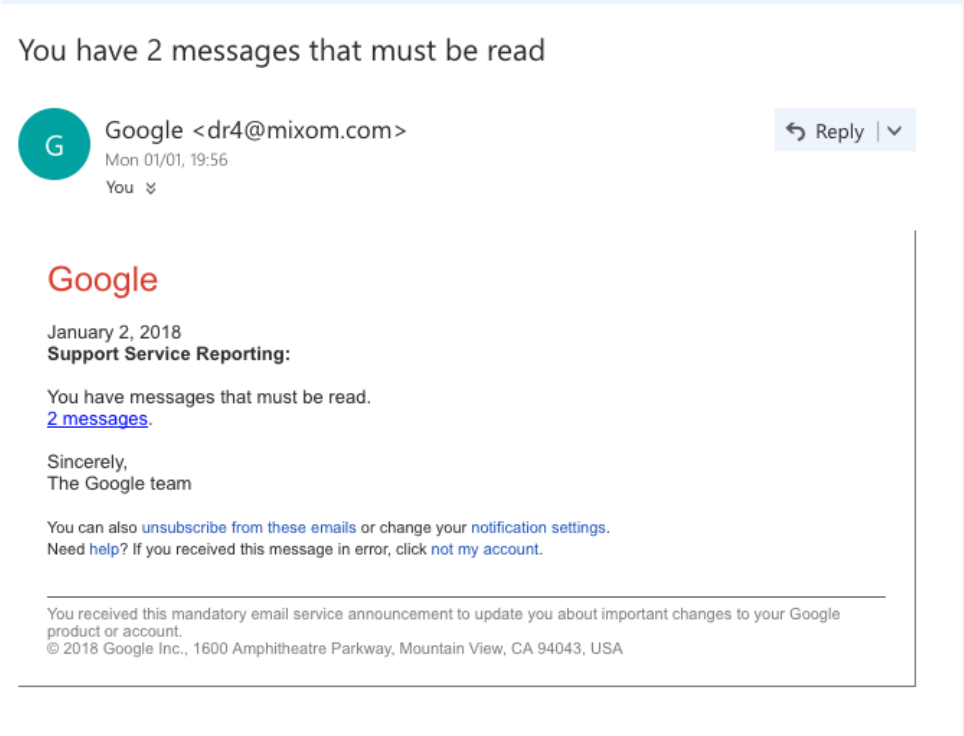
Instructions Station 2: Phishing for Scams Chromebook

- **Explain** to the students that cybercriminals can send malicious links over email, messaging, or social media, to try and get the consumer to press the link out of worry, urgency, or "socially engineering" to link to fit their interests.
- Work through the "Phishing" portion of this web app: https://studio.code.org/projects/applab/kg5-pnhm0eghHU5-RfLABw. The game is challenging. If the students are spending more that 5-6 minutes trying, you can review the main points of game, which is the tips of a safe password.
- **Brainstorm** with the group some clues for telling if an email is a "phishing scam." Ideas will include:
    - The introduction line is very **generic**
    - There is a **link** that seems **suspicious**
    - There is a sense of **urgency**

- It offers you something for **free**
- It's telling you about something you **never did**
  - Some emails will say something like, "Your last order with us has been double charged." In this case, remember if you actually did order from that company.
- **Typos** and **grammar** errors are common in these emails to, as many of these emails come from foreign parties who do not speak English as a first language.
- The person **doesn't regularly** send you emails like this
- The email address is **spoofed.** Explain that spoofing is defined as slightly changing a real name or brand name by making minute changes in order to trick the consumer's eye. *Examples: Google to Go0gle, Amazon to Amazon, facebook.com to facebook.com.*

Here is an example you can show the students:

Bits N' Bytes Cybersecurity Education



- *Common Phishing Emails: Learn the signs* https://www.edts.com/edts-blog/15-examples-of-phishing-emails-from-2016-2017

- **Explain** to the students that clicking the link in the email may compromise your username and password for the account, giving it to the hacker.
    - Explain: If you realize that you have compromised yourself afterwards, make sure to change your password and username accordingly.
- ***Activity***: Using blank paper, have each student "draft" a phishing email, based on the discussion you had. Once everyone is done, have the student pass their paper to the person to the right and using a different colored pen, underline and explain each "clue" that leads them to believe that they should ignore the message.

    - After the activity, explain to them that since these emails are getting more and more realistic, it is better to install an **anti-malware software**, or a software to protect their device from **malware** (code that can allow for the cybercriminals to take control over a device). In case you do click on a link, the anti-malware should warn you that the site is **spurious** (contains harmful material).

Bits N' Bytes Cybersecurity Education

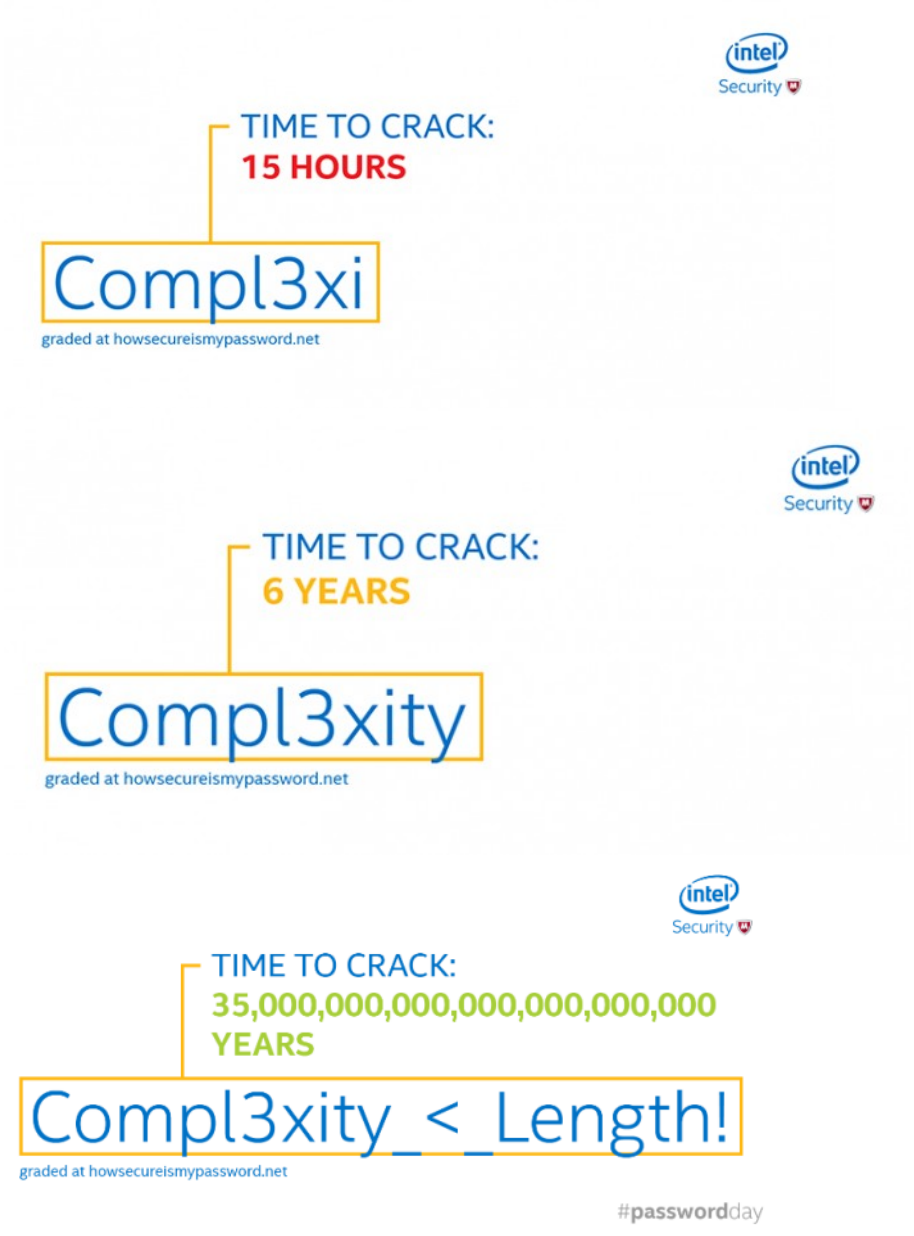
INSTRUCTIONS Station 3: What's Your Password? Chromebook

- **Brianstorm** with the group where they have used **passwords** (long strings used for authentication) before. Ideas may include:
    - Email
    - Bank accounts
    - Voicemail
    - Unlocking your phone
    - Social media accounts
    - To access your grades
    - Amazon: to online shop
    - Health accounts: doctor data
- Work through the "Password Management" portion of this: https://studio.code.org/projects/applab/kg5-pnhm0eghHU5-RfLABw. The game is challenging. If the students are spending more that 5-6 minutes trying, you can review the main points of game, which is the tips of a safe password.
- Now, **explain** how hackers try and crack passwords. In today's day, hackers program computers to run algorithms to crack passwords for them. Thus, the longer the password is (the more characters it has), the longer it will take for a computer to crack it. Although you may have previously heard that "the more complex the password is, the better!", it will actually put you at a greater advantage if your password is **longer**. It can still have some level of complexity, but you should still be able to remember it.
    - Share this helpful tip:
        - Try meshing together a couple words that you remember when you think of the website or words that are significant in your life. For instance, if your favorite food is chocolate, and you eat chocolate a lot during dinner, and you eat dinner with your family, and your family goes to Miami every summer, you may come up with something like: **Ch0colate Dinner Fami1 Miami!**
        - That way, it is long and you will be able to remember it better.

- Go on to: https://howsecureismypassword.net
- With the group, **write** at least ***5 different ideas*** for solid passwords, similar to the Chocolate example above.
- **Brainstorm** good password hygiene habits with the students. Ideas may be:
    - Do not repeat passwords for websites
        - Once a hacker gains access to one account, they will try that password with other accounts.

- Change your passwords after major data breaches or cyberattacks that you hear on the news. You should be changing them regularly: once in 6 months!
- Do not share passwords with anyone, except maybe your parent/guardians. Even then, tell them to be careful with the information.
- To remember all your passwords

Remember:



Bits N' Bytes Cybersecurity Education

INSTRUCTIONS Station 4: Understanding Your Online Privacy Chromebook

- Have the students open the worksheet titled **"Station 4 Activity Guide: Google Yourself":** The students will be completing this worksheet.: **https://tinyurl.com/ycnqd79y**
- To understand just how much data is collected during your daily life, have the students explore this online lab: https://www.cbc.ca/news2/interactives/digitalsurveillance/
- **If there is time left,** move on to the privacy policy activity below.
- **Explain** to the group that each and every company that handles consumer data, in any way, shape, or form, has a written **"Privacy Policy"** that they share with the public. This outlines how they use your data, what data they collect/store that is yours, and who they give their data to to help enhance their services. Google, Amazon, Fitbit, Uber, Yahoo, Facebook, Instagram, Snapchat….all of these companies have a Privacy Policy. And it's a great thing that they do! This allows us to know **exactly** what data the company has control over, and how we can alter that data or erase that data if we wish.
- Skim through **ONE privacy policy** online: Google this
- ***Activity***: **privacy policies** are typically written by an attorney and have a lot of legal wording to protect the company, but today, with your group, you are going to be pretending that we are the executives at a company called ***STAR Buddies***, who has a free web application that pairs tutors with students based on the subject the student wants help in. The app runs ads to gain profit. The rest of details of the web application is for your team to decide!
    - On a piece of paper, have on person write down answers to these questions:
        - What information about the user does the web app collect?
        - How does the web app use the information collected?
        - How is the information inputted in the web app shared?
        - What kind of information do your **cookies** collect? **Cookies** are pieces of data (text files) stored on the user's computer while they are browsing. They allow the company to keep track of a user's preferences and recognize you, in order to market their products better.
        - How can the user change their personal information if they wish?
        - How do you secure communication between the server and the user?
            - Think about the "https" and the idea of **Transport Layer Security**, or TLS. TLS, or SSL, encrypts communication between web browsers and web servers. Allows people to send personal information like credit card information with the promise that it is going to the intended destination. When you see a lock next to the

URL when you are surfing the web, this assures you that TLS is being utilized and the company has an **SSL** certificate.

- Help the teams **understand** how important it is to familiarize themselves with a privacy policy before they agree to using a device or service, because you may never know what you agreed to in the terms and conditions (yes, the thing you scroll through just to check off).
- Have the teams **share** what their team brainstormed and put it on the wall at the end of the entire session, next to all the other team's **privacy policy** drafts.

INSTRUCTIONS Station 5: Understanding World Crises Chromebook

- **Explain**: Every day, our world's corporations and governments see loads of attacks on their infrastructure from the bad guys. Most of the time, the "white-hat" teams can stop attacks before they escalate. However, when an attack is unforseen and either the corporation does not see it coming, or a user on the consumer end has caused it, it can lead to large scale, pervasive consequences to customer data and internal systems. If only we learn from our past mistakes, we can prevent the same problems from arising in the future.
- Pass out the worksheet for the students to participate in the matching exercise.
- Using everyone's current knowledge, put heads together and try and match each major cyber attack/data breach with the correct fact that corresponds with it.

Answers: C, D, A, F, G, E, B, H

- **Explain** how companies have to be vigilant at all times against cyber attack, but on the user end, if we protect ourselves and our communities, we can become **resilient** against cybercriminals.
- **Urge** the students to keep up with the news everyday on cybersecurity in order to hear about these hacks right when they happen. **Tell** them to pass on the information as soon as they read what happened and change passwords and take action as soon as possible, to prevent any fraudulent usage of your data.
- **Have** the students check if their or their parents email account details have ever been breached in the past: Have I Been Pwned

Bits N' Bytes Cybersecurity Education

- As always, **share** with them that proactive action **(strong passwords, knowing phishing scams, using/understanding encryption, and maintaining your privacy)** can only help prevent these data breaches!

This curriculum was produced by Kyla Guru, Founder/CEO of Bits N' Bytes Cybersecurity Education. Check out www.bitsnbytes.us.com to keep up with relevant tips on becoming more cybersecure, learn about the latest cyber-threats, and gain resources to help you manage your online safety seamlessly. Please don't hesitate to direct any questions to the contact page on Kyla's website, and be sure to follow @GuruDetective on Twitter to stay in touch!