Introduction to Online Safety

Unit 2

A STEM Program of the Air & Space Forces Association

Learning Objectives

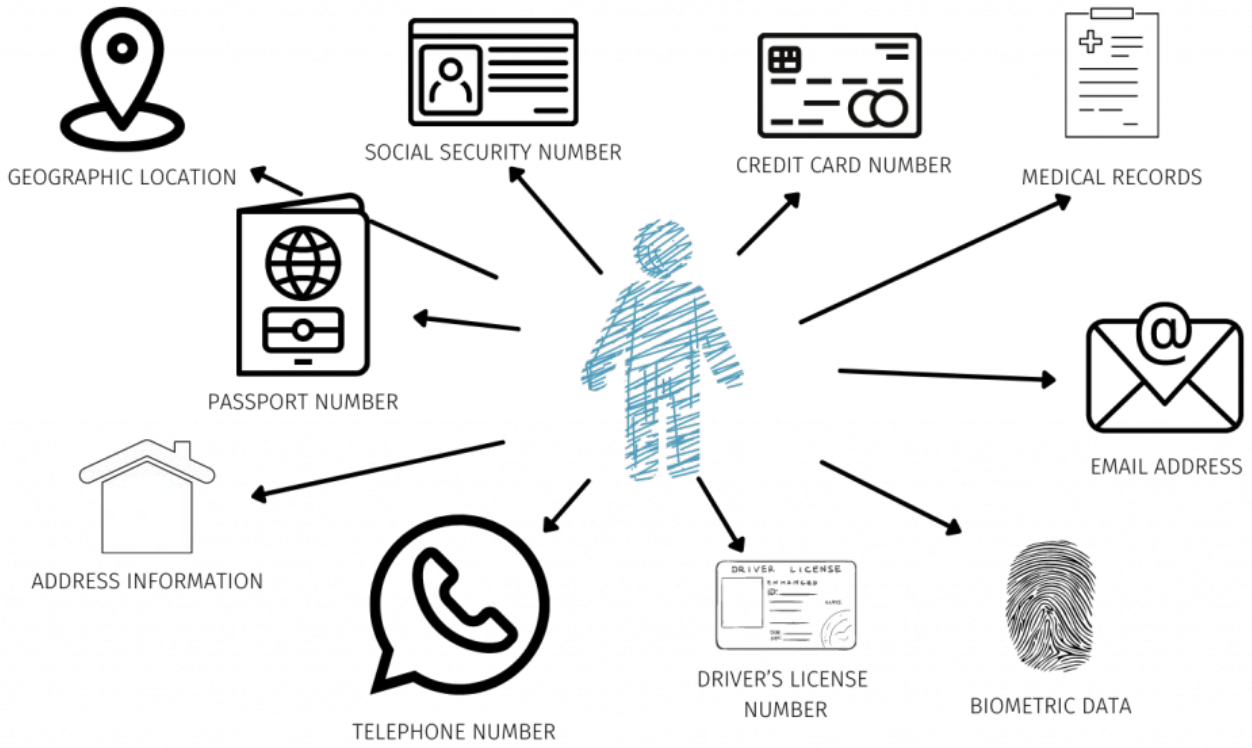
- PII Protection
  - Understand what makes certain information more sensitive and how to keep it secure
- Cyber ethics
  - Understand responsible and respectful use of internet resources
- Cyberbullying
  - Define Cyberbullying and discuss strategies to help yourself or others in this type of situation
- Real world scenarios
  - Analyze and discuss real world example(s) and use what they've learned to determine a course of action for each scenario

PII Protection

Section 1

Personally Identifiable Information (PII)

- PII is any information specific to an individual (see examples).
- PII can be used by hackers to steal someone's identity, bank funds, etc.
- Hackers also use PII to impersonate victims and gain access to a different person or an organization's network.
- This type of information should only be shared with trusted, verified individuals.



Online Safety: The Basics

- Never share your password.
- Only share PII when *absolutely* necessary.
- Do not download any suspicious or unknown software.
- Always log out when you are done.
- Never post anything you do not want public.
  - You might think you're being safe and limiting your posts to only friends, but anything you post can be easily copied and pasted and sent to someone else.
- If you're unsure about anything you do online, ask your parent or guardian if it is OK.

Safe Browsing

- Use a trustworthy web browser.
- Check that your connection is secure.
  - Do not use public Wi-Fi to access sites with sensitive information.
- Check the address for spoofs.
- Use a secure website, especially when submitting PII.
  - Look for an "s" after “http” in the web address .
  - Caution sign is an alert.
  - Look for a ‘padlock’ in the browser address bar.

- Do not directly click on any unknown URL.

Browser Tools

- Use automatic updates
- Use and regularly update built-in safety features
  - Pop-up blockers
  - Anti-spyware
  - Anti-virus
  - Anti-phishing
- Do not use “Save Password” or “Remember Me” functions

Social Media Tips

- Be picky
  - Only accept or follow friends you know in real life
- Do not post your location
- Be careful with apps
  - Games and geo-tracking apps may give away your location or other PII
- Assume everything you post online is permanent
  - Colleges and employers check social media accounts
- Don’t over-share
  - Just because a site asks for information doesn’t mean it’s required to set up an account
- Customize and update your security settings
  - Default settings are weak

Cyber Ethics

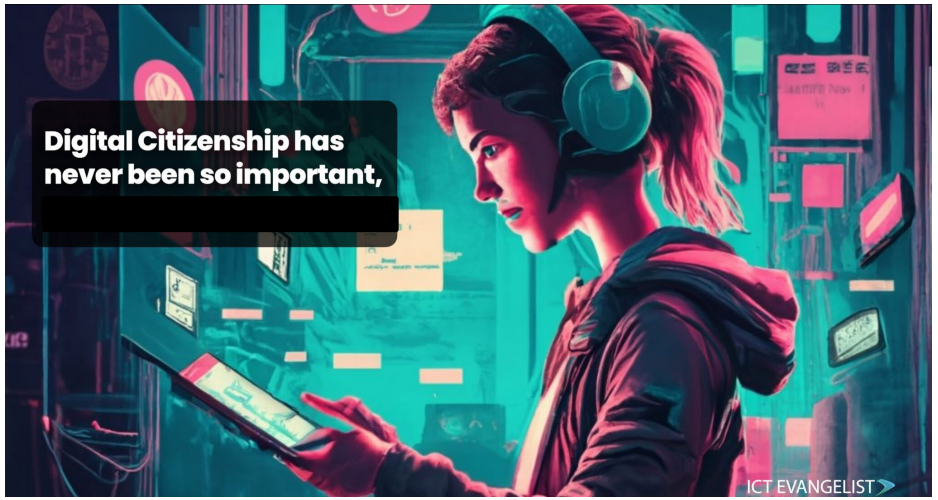
Section 2

Digital Citizenship & Cyber Ethics

Digital Citizenship is the responsible, ethical, and safe use of technology and the internet, encompassing the rights and responsibilities of users in the digital world. Cyber ethics establishes a moral code of conduct for online interactions.

Generally, computers improve our lives, but they can also cause serious harm. The basic idea of cyber ethics is that you should never do something in cyberspace that would be considered wrong or illegal to do in everyday life.

Always be responsible and respectful when using technology.



Principles of Cyber Ethics

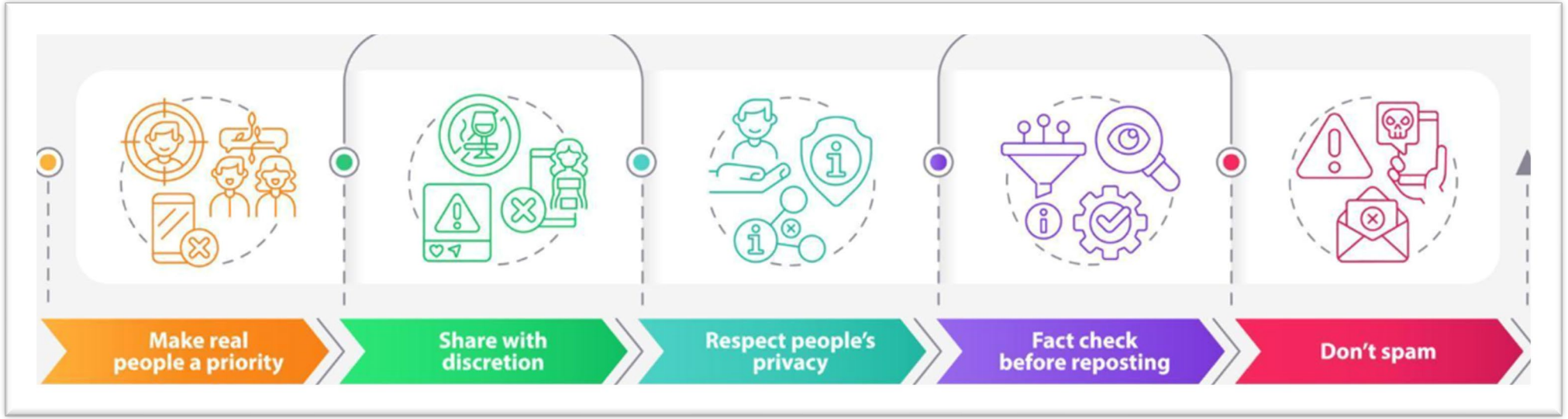
The principles listed below have been adapted and adopted by CyberPatriot as the ethical guidelines for the program. Use this code of conduct to help you navigate the choices you make.

- ❑ Do not use a computer to harm other people.
- ❑ Do not interfere with other people's computer work.
- ❑ Do not snoop around in other people's computer files.
- ❑ Do not use a computer to steal.
- ❑ Do not copy or use proprietary software for which you have not paid.
- ❑ Do not use other people's computer resources without authorization or proper compensation.
- ❑ Do not appropriate other people's intellectual output.
- ❑ **Do think about the social consequences of the program you are writing or the system you are designing.**
- ❑ **Do always use a computer in ways that ensure consideration and respect for your fellow humans.**

Netiquette

(Network Etiquette) is the polite or acceptable way of communicating online. Think manners, but for digital spaces.

Here are some examples:



Cyberbullying

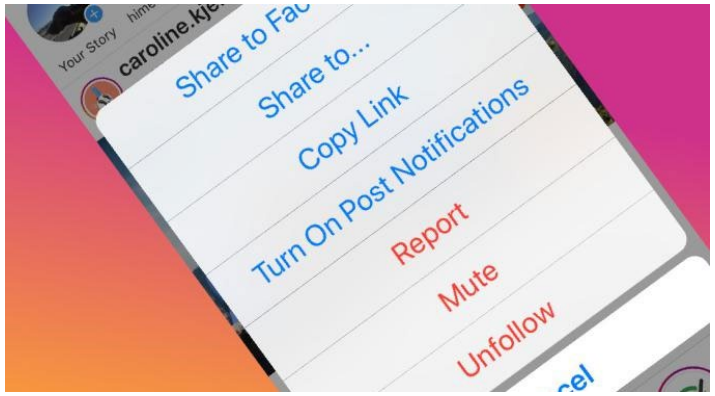
Section 3

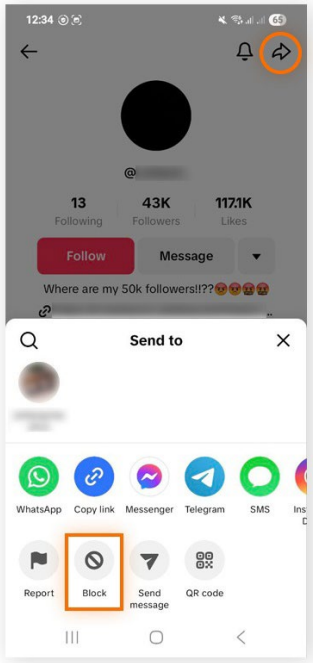
Cyberbullying

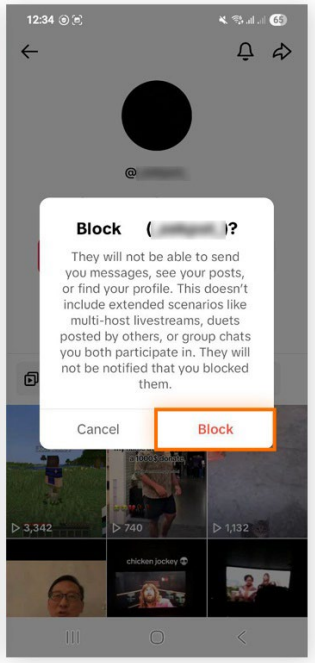
- Bullying refers to any unwanted, aggressive behavior.
- Cyberbullying refers to any bullying that takes place through use of electronic technology.
- Forms:
  - Hurtful comments, texts or emails
  - Rumors through virtual platforms
  - Fake profiles
  - Embarrassing photos or videos
- Studies suggest 46%-55% of teens have experienced a form cyberbullying.

Cyberbullying: If it Happens to You

- Make your accounts private.
- Do not respond to any messages, posts or emails
- Block offenders.
- Document or screenshot and report the behavior so it can be addressed.
- Report the content so other people aren't hurt by it as well.







Reporting Cyberbullying

- To schools:
  - Inform your school administration of any cyberbullying as you would with other types of bullying
  - Provide screenshots or records of bullying

- To your parents and law enforcement, *especially* if it involves any of the following:
  - Threats of violence
  - Explicit messages or photos
  - Taking a photo or video of someone in a place where he or she would expect privacy
  - Stalking and hate crimes

Application

Section 4

To Hack, or Not to Hack?

Scenario A

Scenario A: To Hack, or Not to Hack?

Emily posted a picture of your friend Jayden on Instagram. The picture makes it look as if Jayden is consuming alcohol, but you know that he wasn't. Your friend Jayden is very upset and Emily refuses to take the picture down. Jayden asks for your help in getting into Emily's Instagram account to remove the picture.

What should she do?

Scenario A: To Hack, or Not to Hack?

1. You don't want Jayden to get into trouble, so you tell him that you're only going to help this once. Then you use a tool that you found on the Internet to help Jayden get into Emily's Instagram account and remove the picture.
2. You let Jayden know that Instagram allows people to report images that violate their rules. You help Jayden contact Instagram to have them remove the picture. You let him know that it may take a few days to get an answer.
3. You don't want to be a bad friend, so you help Jayden remove the picture. Then, you change Emily's password so she can't repost the picture. Later, you borrow Emily's phone and delete the picture so that this situation will be over.
4. You explain to Jayden that it's his fault for being in the picture in the first place and Emily shouldn't have to take down the picture. You also explain how things can stay on the Internet forever and that you don't want to be friends with people who don't make good decisions.

Scenario A: To Hack, or Not to Hack?

Discussion

Privileged Information

Scenario B

Scenario B: Privileged Information

Jessica has a group project due tomorrow. She and her friends have been working diligently and are very proud of their final product. Yesterday, her group gave the final copy to Derek so that he could print it out and turn it in. Unfortunately, Derek is out sick today and not answering his phone. The group is at risk of getting a lower grade if the project is turned in late. Jessica has seen Derek type in his password multiple times and knows that she can get into his email account where their project is stored.

What should she do?

Scenario B: Privileged Information

1. She should use the password just this once to retrieve and print the assignment so that the group doesn't get a bad grade. It would be unfair if the group were punished because one person was sick. Derek certainly wouldn't want them to get a bad grade.
2. She should use the password to print the assignment. When Derek gets back, she should tell him what happened and help him choose a new password. This way it won’t be a big deal because she told him what happened, and she and her friends won't get a bad grade.
3. She should tell the teacher the situation and ask the teacher to allow the group to turn in the project late. In the future, she should always make sure that multiple people in the group have access to the final project to avoid this type of situation.
4. She should log into Derek's account to print the assignment. Then she should immediately change the password and let Derek know the new password when he gets back. She should also show him how to avoid other people learning his password by watching him type.

Scenario B: Privileged Information

Discussion

Responsible Actions

Scenario C

Scenario C: Responsible Actions

Joel is a competitor in the CyberPatriot National Finals Competition. During the competition you can overhear a member of another team talking from across another partition. You're not actively trying to hear his conversation, but he is a little louder than the others, and his voice projects rather well.

You overhear him suggest checking a port number that you didn't think about, and it inspires you to check the same port for vulnerability. The CyberPatriot Rules Book states that you should receive no outside assistance which includes direct and indirect advice.

What should he do?

Scenario C: Responsible Actions

1. Is Joel obligated to report what he has overheard? Why or why not?
2. What if Joel tells the participant to quiet down and that he can hear him talking? Does that excuse Joel from using what he overheard?

Scenario C: Responsible Actions

Discussion