



AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

UNIT 2

Introduction to Online Safety





Learning Objectives

- Participants will understand the definition and context of cyberbullying
 - Dealing with cyberbullying
 - Reporting cyberbullying
- Participants will understand what makes certain types of information private or more sensitive than others
- Participants will gain an understanding of how to protect themselves online and appropriately use the Internet
 - Safe browsing
 - Social media tips





AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

SECTION 1

Cyberbullying





Netiquette

Commonly accepted rules of how to behave online

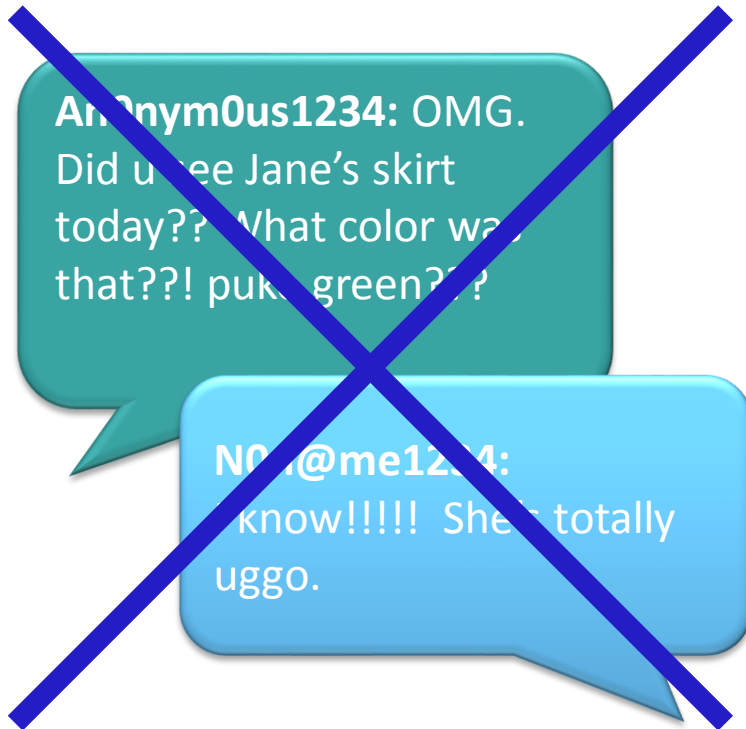
~~L3br0nJ@mes: THE CELTICS SUCK! GO MIAMI!!~~
~~H00psF@N89: Did you guys see the game last night?~~
~~L3br0nJ@mes: THE CELTICS SUCK! GO MIAMI!!~~
~~B@ll3r4Lyfe: I didn't Miami did alright on D, but they have to work on their 3pt game~~
~~L3br0nJ@mes: THE CELTICS SUCK! GO MIAMI!!~~
~~L3br0nJ@mes: THE CELTICS SUCK! GO MIAMI!!~~

- **Do not** spam forums, chat rooms, or social media sites with useless or repeated information
- **Do not** pretend to be someone else
- **Do not** post or distribute illegal material
- **Do not** use abusive or threatening language
- **Do not** try to obtain personal info about someone





Cyberbullying



- Bullying refers to any unwanted, aggressive behavior
- Cyberbullying refers to any bullying that takes place through use of electronic technology
- Forms:
 - Insulting texts or emails
 - Rumors sent via email or social networking sites
 - Fake profiles
 - Embarrassing photos or videos
- Affects 29.2% of students every year and the number is growing
- Why it's harmful:
 - Anonymous
 - Can be done 24/7

Source: <http://www.stopbullying.gov/cyberbullying/>





Cyberbullying: If it Happens to You

- Do not respond to any messages, posts or emails
- Block offenders
- Document and report the behavior so it can be addressed
- Flag the content so other people aren't hurt by it

Hide...
Report Story or Spam

Is this post about you or a friend?

Yes, this post is about me or a friend:

- I don't like this post
- It's harassing me
- It's harassing a friend

No, this post is about something else:

- Violence or harmful behavior
- My friend's account might be compromised or hacked
- Hate speech
- Sexually explicit content
- Spam or scam

Is this your intellectual property?

Continue **Cancel**

Source: <http://www.stopbullying.gov/cyberbullying/>





Reporting Cyberbullying

- To schools:
 - Inform your school 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





AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

SECTION 2

Personally Identifiable Information & Online Safety





Personally Identifiable Information (PII)

- PII is any information specific to an individual
- Examples:
 - Student ID Number
 - Date of Birth
 - Email Address
 - Mailing Address
 - Credit Card Information
 - Social Security Number
- PII can be used by hackers to steal someone's identity, bank funds, etc.
- Hackers also use PII to impersonate victims in order to gain access to a different person or an organizations 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





Risk Sites

- Online Shopping
- Social Media
- Any other website that requires Personally Identifiable Information (PII).
- These sites are enjoyable and useful. Just make sure you are being extra careful when visiting them.





Safe Browsing

- Do not use public Wi-Fi to access risk sites
- Check the address for spoofs

 http://bankOfamerica.com

- Use a secure website, especially when submitting PII
 - Look for an "s" after “http” in the web address
 - Look for a ‘padlock’ in the browser address bar
 - Look for a green background or green text

 https://login.microsoftonline.com/





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
- Internet Explorer is more frequently targeted and has more security flaws than any other browser



Firefox®



chrome



Safari





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



Source: play.google.com

