AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

UNIT TWO

Cyber Ethics and Online Safety

www.uscyberpatriot.org

SECTION ONE

Cyber Ethics

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!!!

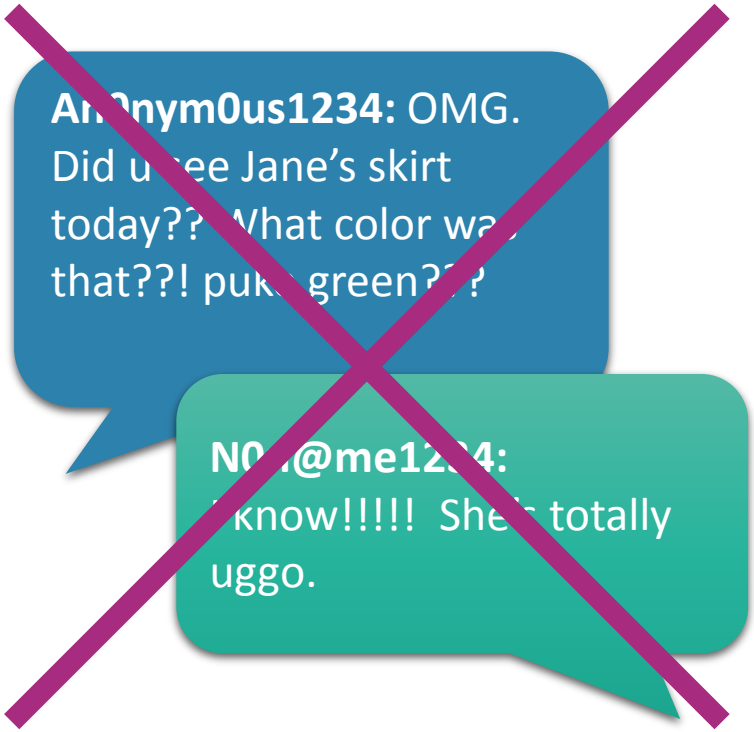
B@ll3r4Lyfe: I did! Miami did alright on D, but they have to work on their 3pt game

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

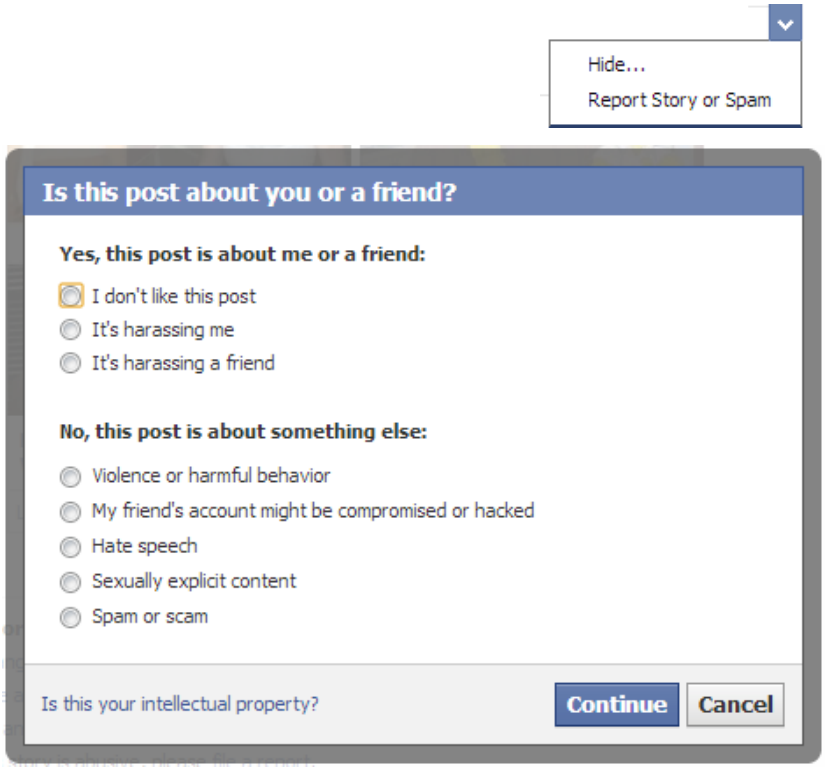


- Affects 29.2% of students every year and the number is growing
- Forms:
  - Insulting texts or emails
  - Rumors sent via email or social networking sites
  - Fake profiles
  - Embarrassing photos or videos
- Why it's harmful:
  - Anonymous
  - Can be done 24/7

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



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

Cyberbullying: Report It

- 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

The 10 Commandments of Computer Ethics

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

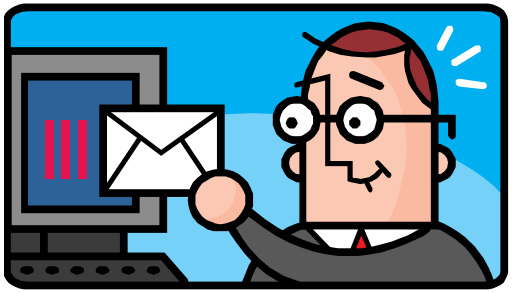
Source: The Computer Ethics Institute, http://computerethicsinstitute.org/

SECTION TWO

Online Safety

Safety Online: The Basics

- Chat only with trusted, verified individuals
- Never publically share these things online:
  - Passwords
  - Social Security number
  - Student ID number
  - Other Personally Identifiable Information (PII)
- Never share your password
- 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



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

- 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

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

Social Media Tips

- Be picky
  - Only accept or follow friends you know if 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