Surfing the Digital Wave: Cyber Security Basics

Image "Social Media Information Overload" by Mark Smiciklas is licensed under CC BY-NC 2.0
Be a cyber secure digital lifeguard as you lead your students in surfing the sometimes turbulent and murky waters of the digital world.
My Experiences with Cyber Security

My biggest take away from the first camp was that my password security was nonexistent.

I chose a password manager and changed my passwords for everything to something different for each site. I change my passwords frequently.

My email password is the one that I keep the most secure--because it is the key to the kingdom.

Do you know why?

Suggested Password rules:

1. Make the password/passphrase at least 12 characters long---the longer the better.
2. Use seemingly random words strung together
3. Mix in numbers, symbols, upper, and lower-case letters.
4. Use something that you can remember but others could not guess.
5. Do not use famous quotations that might be easy to guess.

HOW SECURE IS YOUR PASSWORD? Try a password like one that you use at this site.

LastPass  https://lastpass.com/howsecure.php

Other password test sites:
• Dashlane [https://howsecureismypassword.net](https://howsecureismypassword.net)


3 - Image “Cyber Security-Cyber Crime” by Blue Coat Photos, is licensed under [CC BY-SA 2.0](https://creativecommons.org/licenses/by-sa/2.0/)
Essential Questions

- What is cyber security?
- What are the principles of cyber security?
- Why is cyber security a meaningful topic for this conference?
- What are some of the resources useful for educating your students about safely and ethically treading digital waters?

What Is Cyber Security?

“Computer security, also known as cyber security or IT security, is the protection of computer systems from the theft or damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide.”

What are the principles of Cyber Security?

CIA Triad

![Image of CIA Triad]

Definition - What does CIA Triad of Information Security mean?

The CIA (Confidentiality, Integrity, and Availability) triad of information security is an information security benchmark model used to evaluate the information security of an organization. The CIA triad of information security implements security using three key areas related to information systems including confidentiality, integrity and availability.

Techopedia explains CIA Triad of Information Security

The CIA triad of information security was created to provide a baseline standard for evaluating and implementing information security regardless of the underlying system and/or organization. The three core goals have distinct requirements and processes within each other.

- **Confidentiality**: Ensures that data or an information system is accessed by only an authorized person. User ID’s and passwords, access control lists (ACL) and policy-based security are some of the methods through which confidentiality is achieved.

- **Integrity**: Integrity assures that the data or information system can be trusted. Ensures that it is edited by only authorized persons and remains in its original state when at rest. Data encryption and hashing algorithms are key processes in providing integrity.

- **Availability**: Data and information systems are available when required. Hardware maintenance, software patching/upgrading and network optimization ensures availability.


Types of Attacks (Big Picture)

Physical Security Attacks
Software-Based Attacks
Web App-Based Attacks
Social Engineering Attacks
Network-Based Attacks

Why is cyber security a meaningful topic for this conference?

Image "Cyber Security-Hacker" by Blue Coat Photos is licensed under CC BY-SA 2.0
5 - Cyber Security in the News

Image Headline by Illuminated Living is licensed under CC BY-NC-ND 3.0


Digital Leadership

Among the refreshed Technology Standards for Instructional Personnel drafted by VSTE is the standard of Digital Leadership.

Teachers positively contribute to and responsibly participate in the digital world.

In this standard teachers:

- Cultivate and manage their digital identities and reputations and are aware of the permanence of their actions in the digital world.

- Promote and model safe, legal and ethical behaviors with students by embedding digital citizenship skills in online lessons and activities.

- Select and correctly attribute appropriate digital content, tools and resources that meet local, state and/or federal policies.

- Understand the rights and obligations of student privacy and security when collecting and using student data, communicating with stakeholders, reviewing user agreements, and selecting digital content, tools, and resources.
These standards are all related to topics that fall under the umbrella of cyber security.

Meeting these standards positively supports the cyber security principles of confidentiality, integrity and availability.

A lack of attention to these standards can contribute to the compromise of any of these three principles.

Cyber Security and Education
Cyberattacks on Educational Institutions Have Soared in 2017 - Web...
https://www.spamton.com/web.../cyberattacks-on-educational-institutions-2017/  
Mar 15, 2017 - The list of educational institutions that have reported cyberattacks in... There are many reasons why the attacks have soared in recent months.

Common Types of Cyberattacks in Education and What We Can Learn...
https://www.fortinet.com.../common-types-of-cyberattacks-in-education-and-what-we...  
Oct 6, 2017 - Common Types of Cyberattacks in Education and What We Can Learn from... attacks, with a recent study finding that 13 percent of educational...

Cyberattacks Increasingly Target Student Data
www.govtech.com/security/Cyberattacks-Increasingly-Target-Student-Data.html  
Dec 28, 2017 - Schools in DeKalb County, Ga., see as many as 3000 cyberattacks a day, ... parents' names, and contacts — cyber criminals have targeted them. ... In recent months, three metro Atlanta school districts reported email phishing attacks. ... In October, the U.S. Department of Education warned schools of...

Dept. of Ed. Alerts Schools of 'New Type of Cyber Attacks' - Campus...
https://www.campussafetymagazine.com.../department-education-schools-new-type-c...  
Oct 26, 2017 - The Department of Education alerted schools of a cyber extortion threat and provided guidance in an announcement by the Federal Student...

10 biggest hacks of 2017 - Business
Dec 18, 2017 - The cyberattacks highlighted the alarming vulnerability of our personal information... it scanned the network for shared folders with common names and attempted... It was the latest in a string of major breaches stemming from... Related: Hackers are targeting schools, U.S. Department of Education warns.

Cyber attacks are one of the biggest threats that schools face, experts...
https://www.telegraph.co.uk > Education  
Mar 17, 2018 - Malware and phishing are the most popular types of attacks, ... Faith Parish, the education director at Ecclesiastical, said: "Schools hold...

What Cyberthreats Do Higher Education Institutions Face? - Forbes
https://www.forbes.com.../what-cyberthreats-do-higher-education-institutions-face/  
Aug 21, 2017 - Nevertheless, a typical higher education institution stores just as... There are myriad cyberattacks a university may face. ... To begin addressing these problems, it's vital that universities create a list of potential vulnerabilities.

Cybersecurity In K-12 education: Schools face increased risk of cyber...
https://www.fedscop.com/cybersecurity-in-k-12-education-schools-around-the-count...  
Jul 17, 2015 - ... millions of people (in the recent Office of Personnel Management case, 21.5.... But experts say K-12 schools are also at risk — from outside threats and... data, including school ID numbers and the names of those receiving free or ... the statement, saying the agency does not track school cyber attacks.

Google Search for"list of recent education cyber attacks"

Understand the rights and obligations of student privacy and security when collecting and using student data, communicating with stakeholders, reviewing user agreements, and selecting digital content, tools, and resources.

**Protecting Student Privacy and Data**

*Digital Leadership: Teachers positively contribute to and responsibly participate in the digital world.*

- Cultivate and manage their digital identities and reputations and are aware of the permanence of their actions in the digital world
- Promote and model safe, legal and ethical behaviors with students by embedding digital citizenship skills in online lessons and activities
- Select and correctly attribute appropriate digital content, tools and resources that meet local, state and/or federal policies
- **Understand the rights and obligations of student privacy and security when collecting and using student data, communicating with stakeholders, reviewing user agreements, and selecting digital content, tools, and resources.**


• “Protecting Students’ Online Privacy.” Common Sense Education, 2018. PDF Protecting Students’ Online Privacy


Teachers positively contribute to and responsibly participate in the digital world. In this standard teachers:

Promote and model safe, legal and ethical behaviors with students by embedding digital citizenship skills in online lessons and activities.

What are some of the resources useful for educating your students about safely and ethically treading digital waters?

Image Art Academy - Tidal Wave by Frank RT is licensed under CC BY-NC-ND 3.0
"It is not about the **Tools**...It's **about the Skills**.

---

**Image**: "Wikis - It is not about the Tools...It's about the Skills" by langwitches is licensed under [CC BY-NC-SA 2.0](https://creativecommons.org/licenses/by-nc-sa/2.0/).


---

**Image**: Educational Postcard about good digital practices for students by Ken Whytock is licensed under [CC BY-NC 2.0](https://creativecommons.org/licenses/by-nc/2.0/).

"Closely linked with being digitally literate is the necessity to help students develop the skills of safe, responsible digital citizenship.

Students need an understanding of human, cultural, and societal issues related to technology, and practice legal and ethical behaviour.

We need to help our students to learn how to ensure that the ‘digital footprint’ they leave behind serves to reinforce positive relationships and helps them to be aware of how they can make the world a better place.”

---

[What Research Tells Us...](http://21cvlearning.com/)


• “Teacher's Portal.” Teaching Privacy, Is Supported by the National Science Foundation under Grant #1636590, 19 Apr. 2017, https://teachingprivacy.org/teachers-portal/.

• “Teach Cyber.” Teach Cyber, Supported by a Grant from the National Security Agency CAE Grant# H98230-17-1-0314, https://teachcyber.org/.


• “Resources for Teachers and Parents.” Teach Cyber, Supported by a Grant from the National Security Agency CAE Grant# H98230-17-1-0314, 6 June 2018, https://teachcyber.org/about/resources-for-teachers-parents/.


• Log In https://nicerc.instructure.com/
Be a cyber secure digital lifeguard as you lead your students in surfing the sometimes turbulent and murky waters of the digital world.

In the increasingly digital world we live in, cyber security is relevant to everyone.

Educators have an especially crucial role in promoting cyber security:

- The refreshed TSIP standards address cyber security-related digital leadership standards for educators.

- As digital leaders, educators promote and model safe, legal and ethical behaviors and include digital citizenship in their lessons.
Wrapping It Up

My hope for this session is that you walk away:

- Aware of the definition and importance of cyber security.
- Informed of the refreshed TSIP standards under the category of digital leadership.
- Armed with references that will inform you as a digital leader.
- Armed with references useful for educating your students about safely and ethically treading digital waters.
A final word about a digital leadership standard modeled in this presentation:

- Select and correctly attribute appropriate digital content, tools and resources that meet local, state and/or federal policies.

Digital Leadership: Teachers positively contribute to and responsibly participate in the digital world.

- Cultivate and manage their digital identities and reputations and are aware of the permanence of their actions in the digital world
- Promote and model safe, legal and ethical behaviors with students by embedding digital citizenship skills in online lessons and activities
- Select and correctly attribute appropriate digital content, tools and resources that meet local, state and/or federal policies
- Understand the rights and obligations of student privacy and security when collecting and using student data, communicating with stakeholders, reviewing user agreements, and selecting digital content, tools, and resources.

Tools to Assist with Attribution of Images and Source Citations


Other references used in the creation of this presentation:


Presenter VSTE 2018:

June M. Jones, Educational Technology Facilitator
York County School Division

jjones2@ycsd.york.va.us