How schools, educators, and parents can empower youth to claim agency in their digital lives.

THE NEXT GENERATION OF PRIVACY AND SECURITY
A PERSONAL STORY

LET'S GO BACK TO 2007 FOR A MOMENT

[Images of various online activities and warnings]
At this CA public high school, we had computer labs. We were taught to use Microsoft Office and how to search for research papers.

“Harmful” sites were blocked by an admin at the network level. Kids used VPNs as a workaround.

We weren’t taught at any point about internet safety, data privacy, or computer security in our 4 years at the school.
THERE ARE CONSEQUENCES. FOR EXAMPLE:

**Lifetime Cyberbullying Victimization Rates**

Ten Different Studies 2007-2016

- May 2007: 18.8%
- June 2009: 21.5%
- June 2009: 34.2%
- Nov 2009: 28.7%
- Feb 2010: 20.8%
- Dec 2011: 29.2%
- Oct 2013: 24.1%
- Jan 2014: 34.6%
- Feb 2015: 34.0%
- Aug 2016: 33.8%

*Average: 27.9%*

**Child Identity Fraud**

Minors who are bullied online are **NINE times** more likely to be victims of fraud than minors who were not bullied.

© 2018 Javelin Strategy & Research
One of the biggest takeaways from the study is that everyone, regardless of age, wants the web to be safe and free. However, the ways each generation views safety vary.

All agree that they want to be protected from malware, ID theft, and fraud. The main distinction comes down to privacy. According to the study, older generations are concerned about anonymity online and making sure their data and personal information is kept private.

This is in sharp contrast to Generation Z who is comfortable sharing personal data in order to get a more personalized experience. In fact, millennials and Gen Z are over 25 percent more likely than Gen X and Baby Boomers to opt for a predictive Internet. The study goes farther finding 50% of Gen Z would stop visiting a website if it didn’t anticipate what they needed, liked or wanted.

[Link](https://torquemag.io/2017/12/generation-z-opts-personalization-privacy-means-wordpress/)
THE PROBLEM

PEOPLE ARE GETTING ONLINE EARLIER THAN EVER

“If you’re a millennial mom, there’s a pretty good chance you have a social media account for your baby. No, we’re not talking about posting a ton of baby pics on your personal Facebook or Instagram page—but on a dedicated account with your baby’s own name on it.

According to a new survey conducted by Gerber.com, close to 40 percent of moms aged 18 to 34 created social media accounts for their baby before the child’s first birthday – and another 7 percent made one before their kid’s second birthday.”

https://www.today.com/parents/have-social-media-account-your-baby-40-percent-millennial-moms-1D80224937
SO WHAT CAN WE DO? RECRUIT PARENTS?

82% of parents believe it is their primary responsibility to protect their child's personal information on the Internet.

DIGITAL PARENTING 2014

- How Many Children use the Internet?
  - Age 5-7: 82%
  - Age 8-11: 96%
  - Age 12-15: 99%

- How Much Time Spent Online Weekly?
  - Age 3-7: 6.5 hrs
  - Age 8-11: 9.2 hrs
  - Age 12-15: 17 hrs

- 28% of children aged 11-16 on social networks have experienced something upsetting in the last year.

- 29% of 12-15 year olds admit they have not met 1 of 3 online 'friends'.

- 41% of parents believe their child knows more about the internet than they do.

http://www.nspcc.org.uk/parents/resources/onlinesafety/statistics-online-safety_wldae0075.html
SOLUTIONS

THERE ARE SOLUTIONS THAT CAN BE TAUGHT AT HOME

INTERNET SAFETY TIPS

Hi, I’m Alex! Welcome to my Internet Safety Tips for Kids and Teens. I will show you ways to stay safe online at home and at school.

PERSONAL INFORMATION

Don’t give out personal information without your parent’s permission, including last name, address, school name, or phone number.

PHOTOS AND VIDEOS

Don’t post photos or videos online without getting your parent’s approval.

PASSWORDS

Don’t share your password with anyone but your parents.

DOWNLOADING

Talk to your parents before you open an email attachment or download software.

BULLYING

Don’t send or respond to mean or insulting messages. Tell your parents if you receive one.
There are games that can teach internet safety

“In celebration of Internet safety month, Google has released a classroom curriculum and computer game to teach children about online safety and security.”

Good answer!

Delete it and tell a parent or a teacher.

Computer viruses often come disguised as e-mail attachments. So to be safe like Captain Broadband, delete all e-mails with attachments from people that you do not know. Be careful opening e-mails with attachments from friends, too, and always ask a parent if you are unsure about opening an e-mail.
SOLUTIONS

THERE ARE GUIDES AND RESOURCES TO SHARE

Is the sender familiar to you?
Does the sender’s name correspond to the e-mail address shown?

Is the message addressed to you?

Hover your mouse pointer over the link. Does the text shown correspond?

Does the link look reasonable? Is it too complex or unreadable?

Is the message relevant to you? Does it relate to your work?

Is the message signed?

Is the message correctly phrased, with no obvious typos, in a language you understand?

If you have answered “NO” to any of these questions, be vigilant and careful! Delete the message or check with us at Computer.Security@cern.ch when in doubt.
BUT.. WHY NOT TEACH INTERNET SAFETY/SECURITY/PRIVACY AT SCHOOL?

- Kids typically spend anywhere between 6-8 hours at school on a given day; the vast majority.
- Kids are introduced to computers and technology early, with tech becoming a key part of classroom work and even test-taking.
- Kids wouldn’t have to be dependent on their parents’ skill level or resources to learn.
EXAMPLE: AES LESSON PLAN FOR TEACHING INTERNET SAFETY IN MIDDLE SCHOOL

2. Read the URL Carefully
Online scammers know how easy it is to make an “r” and an “n” look like an “m.”

That may not sound like much — but it makes an enormous difference when you're looking at URLs like:

```
www.bankofamerica.com
www.bankofamerica.com
```

One of those URLs goes to a well-known and long-established bank in the United States.
The other one is an imposter website that could do anything from installing ransomware on your computer to downloading your browser history.
Fortunately, there's a way to help your students avoid this danger altogether.
You can teach them how to identify an online scam.

Step 3. Identifying an Online Scam

```
STOP
```

While scammers upgrade their tactics for every new scheme, they can't beat the one thing that almost everyone feels when they encounter a scam.

https://www.aeseducation.com/blog/how-to-teach-internet-safety-to-middle-school-students
## EXAMPLE: I-SAFE.ORG COMPLETE CURRICULUM K-12

### Cyber Security (Lesson 3)

| Grade K | The i-SAFE character, i-Buddy, is used to introduce the abstract concept of the computer virus, and to reinforce that students should have adult assistance when using the Internet through the following:  
- Review of previous lessons  
- Concept introduction: computers can get "sick"  
- Terminology introduction and discussion: virus  
- Compare descriptions of "sick" people and "sick" computers  
- Concept introduction: computer viruses can be found in e-mails  
- Age-appropriate prevention technique: Do not open emails without permission. |
| Grade 1 | Grade K concepts are introduced and built upon by introducing the following:  
- Terminology introduction and discussion: infected  
- Concept introduction: a computer virus is a computer program. |
| Grade 2 | Grade 1 concepts are introduced and built upon by introducing the following:  
- Terminology introduction and discussion: attachment  
- Concept introduction: there are laws and consequences governing people who invent viruses.  
- Terminology introduction and discussion: prevent, used in conjunction with how to protect the computer from viruses. |
| Grade 3 | Grade 2 concepts are introduced and built upon by introducing expanding explanations, vocabulary, and age-appropriate computer virus prevention techniques. |
| Grade 4 | Grade 3 concepts are introduced and built upon by introducing the following:  
- Terminology introduction and discussion: e-mail forwards.  
- Terminology introduction and discussion: automatically, as it is related to viruses and e-mail.  
- Reinforcement of age-appropriate computer virus prevention techniques. |
| Grade 7 | Review information about e-mail protocol and computer virus prevention and utilize information to construct an educational story or other language arts activity for students in a younger grade.  
- Student activities provide specific focus for grade level:  
  - Construct an educational story on lesson concepts.  
  - Share original Internet safety stories with younger students. |
| Grade 8 | Review and reinforce the necessity of using caution when interacting online, including how to deal with mean or bullying interactions, and utilize information to construct an educational story or other language arts activity for students in a younger grade.  
- Student activities provide specific focus for grade level:  
  - Construct an educational story on lesson concepts.  
  - Share original Internet safety stories with younger students. |

### Homeland Security

Integrate knowledge and concepts previously learned about hacking, steganography, malicious code (i.e. viruses and worms) with information on cyber terrorism, to identify and comprehend the utilization of the Internet in cyber terrorism and cyber warfare.

| Grades 7 - 8 | Students activities:  
- Review previous lesson concepts.  
- Participate in a worksheet for knowledge about homeland security issues.  
- Construct guidelines that can be used to combat cyber terrorism by students and others in the community.  
- Share guidelines through a choice of various media. |

### Cyber Security (Lesson 2)

| Grade 5 | Cyber security issues are addressed, focusing on the following issues:  
- E-mail protocol and etiquette  
- Attributes of viruses  
- Consequences of spam, flaming, and viruses  
- Review and reinforce the necessity of using caution when interacting online, including how to deal with mean or bullying interactions, and utilize information to construct an educational story or other language arts activity for students in a younger grade.  
- Student activities provide specific focus for grade level:  
  - Construct an educational story on lesson concepts.  
  - Share original Internet safety stories with younger students. |
| Grade 6 | An overview of cyber security issues leads into a focus on:  
- Vocabulary associated with e-mail use  
- Attributes of computer viruses  
- Consequences of malicious behavior involved in online communication  
- Develop a ten item list of e-mail rules.  
- Create a slogan to reinforce the necessity of proper e-mail etiquette. |
| Grade 7 | An overview of cyber security leads into a focus on the aspects of cyber bullying:  
- Recognition  
- Consequences  
- Techniques to prevent or discourage  
- Participate in a self-esteem activity.  
- Create a skit or scenario about cyber bullying or computer viruses, which presents a problem and appropriate solution.  
- Use a choice of mediums to share information about cyber security. |
| Grade 8 | Overview of cyber security issues, with details on specific threats and consequences of:  
- Computer viruses  
- Trojan horses  
- Worms  
- Hacking  
- Complete a KEWL chart (KWL-type).  
- Complete a topic review crossword puzzle.  
- Develop a way to share information learned about cyber security. |

[https://www.isafe.org/imgs/pdf/scope_sequence.pdf](https://www.isafe.org/imgs/pdf/scope_sequence.pdf)
Education Service Newsletter:

In August 2017, the Novato Unified School District launched the One to World Initiative. This one-to-one device program provided every student in the fifth, sixth, and ninth grade with a Chromebook to use in school as well as at home. This is the first of a three-year rollout plan where Chromebooks will be placed in the hands of all 3rd through 12th graders by 2020.

As the Chromebook rollout expands, digital citizenship education has become a priority focus both in our classrooms and our community. NUSD has adopted Common Sense Media’s educational curriculum to address online citizenship and safety. These lessons are designed to empower students to think critically, behave safely, and participate responsibly in our digital world. From lesson plans, videos, student interactives, and assessments, to professional learning and family outreach materials, Common Sense Media Curriculum provides a whole-community approach to digital citizenship. (Common Sense, 2018)

In addition to in-class lessons, each monthly Education Services Newsletter will include information to help families and community members support our youth in utilizing technology in a responsible and impactful way. Topics will vary from Privacy and Internet Safety to Screen Time Guidelines. The Common Sense website has a wealth of information and resources for students, educators, guardians, and community members. Click on the video to learn 5 Internet Safety Tips for Kids.

SOLUTIONS

WHAT ELSE CAN WE DO?

- Petition to create and allow Internet Safety/Privacy/Security classes to be taken in place of Cooking/HomeEc/etc.
- Volunteer to teach teachers and share curriculum materials with them because not all are trained in internet safety.
- At universities like USC? Express demand for less-technical Gen Ed. Classes around privacy and security open to all students regardless of major.
SOLUTIONS

AND WHAT ELSE?

▸ If you have the privilege of knowing, share your knowledge. Teach your friends/family/teammates, share articles, talk about social impacts relevant to them.

▸ Look beyond the hype of new technologies (such as facial recognition etc.) and have discussions that encompass both pros and cons.
BECAUSE TECH DOESN’T WAIT FOR ANYONE

- Technologies such as VR and AR and robotics and games are becoming more advanced than ever. This will increase the knowledge gap between being a consumer of a product vs. knowing how it works; making users susceptible to harm.

- The definition of ‘privacy’ in terms of the standards that define it is constantly evolving with technology and the comfort level of users.
THANK YOU! IDEAS? QUESTIONS? ALSO, SEE MY REFERENCES BELOW.

https://www.aeseducation.com/blog/how-to-teach-internet-safety-to-middle-school-students


https://www.isafe.org/educators/curriculum


https://www.today.com/parents/have-social-media-account-your-baby-40-percent-millennial-moms-1D80224937

https://www.comparitech.com/blog/vpn-privacy/protecting-childrens-privacy/

https://www.edweek.org/ew/articles/2018/05/16/teens-are-worried-about-online-privacy-what.html

https://studentprivacy.ed.gov/Apps

https://www.pewinternet.org/fact-sheet/social-media/