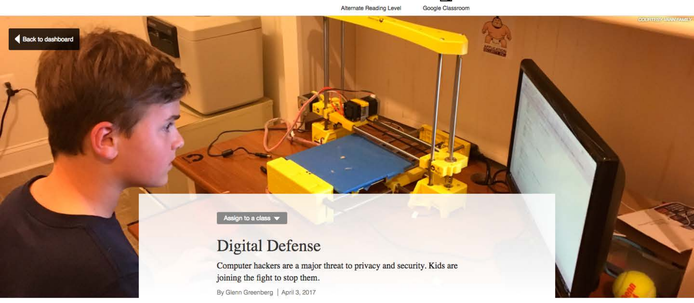

Assign to a class

Digital Defense

Computer hackers are a major threat to privacy and security. Kids are joining the fight to stop them.

By Glenn Greenberg | April 3, 2017

Teacher's Guide

Lexile
- Main article (current view): 1120L
- Alternate reading level: 970L

Focus on Online Safety
Cyber attacks are becoming more frequent and putting personal information at risk. As this

Expand Teaching Notes

February was a tough month for owners and makers of Internet-connected toys.

First, Germany banned the sale of the popular talking doll My Friend Cayla. Parents who had already bought the smart toy were advised to destroy it. The doll asks children personal questions, such as what their favorite TV shows and songs are, and records the answers. The German government determined that hackers could use the doll as a way to spy on kids.

Days later, American consumers learned that CloudPets also posed a risk. The line of stuffed smart toys is produced by Spiral Toys, a U.S.-based company. Through the toy's mobile app, parents and kids can record and send voice messages to each other. But security experts discovered that the CloudPets database was compromised in December 2016. It exposed users' private information, including audio recordings and profile pictures. Experts estimate that more than 820,000 user accounts were affected and about 2 million voice recordings were leaked.

These recent issues with smart toys are part of a growing list of cyber attacks that have infiltrated governments and businesses. U.S. government agencies and corporations, including Yahoo, Sony, Target, and Home Depot, have been hacked. The hits exposed emails, credit-card numbers, fingerprints, and other private information.

Cybercrime is a growing threat, and experts are focused on developing new ways to combat it. Some top specialists are kids.

LEON NEAL—AFP/GETTY IMAGES

The 18-inch talking doll My Friend Cayla allows real-time, two-way conversations through speech-recognition software. Users need a Bluetooth-enabled Apple or Android smart device to take advantage of all of the doll's technological capabilities. But Germany has banned the toy as a threat to children's privacy.

Help Against Hackers

Paul Vann, 14, of Fredericksburg, Virginia, has been immersed in the world of cybersecurity since he was 9. His father works in the industry, and over the years, he brought home books on the subject that Paul read avidly. Paul also watched YouTube videos and attended conferences, where he learned about the tools used against hackers and other Internet-based criminals. "I wanted to take what I learned and use it for security purposes, not for malicious purposes," Paul told TIME Edge.

Paul designed a system to look like an online portal used by National Security Agency employees. He wanted to see if the site would attract hackers. Sure enough, there were about 12,000 attempts to break into what seemed to be a U.S. government network. Paul was then able to determine where the intruders were located. "There were a ton of different countries," he says. "But I saw Russia and China the most."

Paul, a high school sophomore, recently formed his own company, Vann Tech Cyber. He is developing a product for both home and business computer systems that will run weekly security tests. It will scan systems for vulnerabilities, block individuals who have been identified as a threat, and prevent new threats from gaining access.

Paul says there are some key advantages to getting started in the cybersecurity world at such a young age. "I have more time to build my knowledge and partake in cybersecurity internships, conferences, talks, etc.," he notes. "I'm able to constantly learn new information and new techniques that longtime experts may not have had the chance to learn."

Young Minds, Fresh Ideas

Like Paul, the organizers of CyberPatriot, the National Youth Cyber Education Program, see the benefits of an early start in cybersecurity. CyberPatriot is designed to inspire kids nationwide to pursue careers in cybersecurity and STEM fields. The Air Force Association, a nonprofit Air Force and aerospace education group, and Northrop Grumman Foundation developed the program. It offers education resources to elementary school students and summer workshops that teach middle and high school students cybersafety and cybersecurity skills.

COURTESY VANN FAMILY

Paul Vann works on his computer. The 14-year-old cybersecurity expert has launched his own company to develop and sell products designed to protect computer systems from hacking.

CyberPatriot's central project is its annual National Youth Cyber Defense Competition. It consists of a series of rounds that take place online over several months, beginning in October. Student teams are tasked with managing the computer network at a fictitious small company. The teams must identify and repair security weaknesses in the company's operating system. In April, the top teams go to Baltimore, Maryland, to compete in the finals round. Winners receive scholarships.

"It can be stressful, but it's gratifying when you find vulnerabilities and fix them," says Keenan Curp, 13. He is on the team from Summit Lakes Middle School, in Lee's Summit, Missouri. The team will compete in this year's finals from April 3 to 5.

Planning for Tomorrow

CyberPatriot began in 2009 as an effort to address a shortage in the U.S. of young people interested in the areas of science, technology, engineering, and mathematics. Bernard Skoch, the program's national commissioner, says the program also emphasizes the importance of proper online social behavior.

Since its launch, CyberPatriot has seen a steady increase in participation. "We're growing at a rate of about 30-plus percent a year," Skoch says. In 2016, 69,000 students nationwide took part in the program.

"It has helped me understand how to secure computers and how Internet security works," says Arjun Pratap Ghoshal, 13. He is the captain of one of two teams from Oak Valley Middle School, in San Diego, California, competing in this year's finals. "I am fascinated enough to want to pursue a career in cybersecurity," he says. "We have to teach our generation about it, so that we can prevent harmful hacking in this new age of technology."

Keenan agrees. "All businesses need cybersecurity, and anyone can be a victim of hacking," he says. "It's important for kids to have a basic knowledge of cybersecurity. There will be a lot of jobs in the future that require it."

View Classes

PAIRED TEXT

U.S.

Apple Battles the FBI

Apple continues to fight the Federal Bureau of Investigation over a privacy issue.

Assign to a class

MICHELE ASSELIN FOR TIME

U.S.

The Tech Giant and the FBI

Apple CEO Tim Cook talks to TIME about the tension between privacy and security when it comes to high-tech devices.

Assign to a class