CAN WE LEARN TO BE SAFE ONLINE?

EVERY TIME WE LOG IN TO OUR EMAIL ACCOUNT, POST A PICTURE ON INSTAGRAM OR DOWNLOAD A NEW GAME, WE ARE PUTTING OUR PERSONAL INFORMATION AT RISK. KNOWING THAT STUDENTS CAN BE AN EASY TARGET, **PROF DOUG JACOBSON**, FROM **IOWA STATE UNIVERSITY**, USA, HAS DEVELOPED A COURSE TO TEACH COLLEGE AND HIGH SCHOOL STUDENTS ABOUT CYBERSECURITY

TALK LIKE A CYBERSECURITY SPECIALIST

Cyber attacker
The person responsible for the cyber attack, looking to make money or disrupt computing services.

Cyber attack
Intentional and malicious attempts to damage or gain access to computer systems, networks or even single devices.

Breach
Unauthorised access to private information.

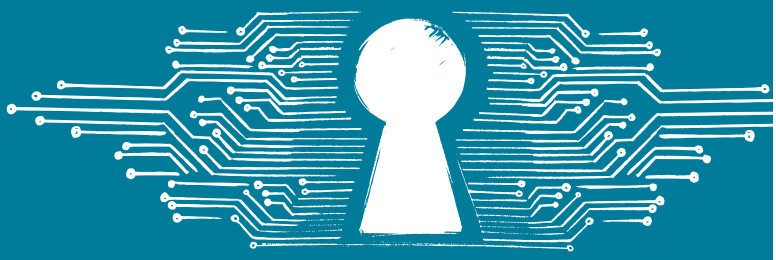
Cyber incident
A breach of security, which may include:

- Unauthorised access to a device or account
- Unauthorised use of computers to steal personal data
- Changes to software or hardware without the owner's consent.

Hacker
The person responsible for breaking into computers and networks.

Internet of Things (IoT)
In broad terms, IoT refers to everything that can connect to the internet. In everyday language, it's often used to describe items that can 'talk' to each other. The IoT is made up of all devices - such as smartphones, TVs, watches, cars and even some household appliances - connected together.

Phishing
Emails designed to trick users into giving up sensitive personal information or clicking on links to a fake website.



With the help of technology, we are becoming more connected than ever before. Undoubtedly, this progress is making our lives more comfortable, but it is also bringing a new set of challenges. Every time we log in to our email account, post a picture on Instagram or download a new game, we are putting our personal information at risk.

With so much time spent online, students are the perfect target for hackers. Because of this, Professor Doug Jacobson, from Iowa State University, knows that it is now more critical than ever before to discuss cybersecurity awareness in a school environment. However, old-fashioned methods of collecting top-ten lists of security threats or poorly organised awareness campaigns are not relevant anymore. What these students need is formal computer security education to give them the knowledge to recognise and fight these threats. Doug believes that it should be required that students learn about cybersecurity before they leave school – just as it is with subjects such as science and maths. "While technology can help keep us secure, attackers are always adapting, and we need to be vigilant," he says. "The more we know about how they attack, the better we are at defending ourselves".

DOUG JACOBSON

University Professor
Director Information Assurance Center
Iowa State University, USA

FIELD OF RESEARCH

Cybersecurity

RESEARCH PROJECT

To design courses for college and high school students that teach cyber security literacy.

FUNDERS

National Science Foundation
Iowa State University

HOW CAN WE TEACH CYBERSECURITY TO STUDENTS?

Doug and his colleagues developed a module-based course to teach cybersecurity awareness to college students. The 8-week 'Introduction to Computer Literacy' course is suitable for all students, including those studying computer science and other related courses. It is natural to assume that IT students would have an advantage, but the reality is that at the beginning of the course all students demonstrated low cybersecurity literacy.

Classes are taught by a member of the Department of Computer and Electrical Engineering, who conducts demonstrations and provides real-life examples. Analysing phishing emails or guessing bad passwords are always popular activities with the students. Crucially, this allows students to experience real situations of cyber incidents in a safe and controlled manner. By the end of the course, students can recognise security threats and make sound decisions when it comes to protecting their personal information.

Interestingly, in their initial runs of the course, Doug and his team found it hard to engage with some of the students, especially when they were not from a computer background. The scientists are now developing a further section to the course, aimed specifically at these students, to help them think about how cybersecurity can be applied to their particular situation and how to avoid potential traps in the future.

"IT CAN'T HAPPEN TO ME, CAN IT?"

College students are not the only target audience that needs to learn about cybersecurity. High school pupils spend just as much time online as older students and, therefore, also need to be aware of cybersecurity issues.

It is not easy to reach these students, however. Most have an 'it can't happen to me' attitude, which teachers have trouble breaking through. For Doug, the best way to change this mentality is to present examples that are meaningful for this age group. "It is about making cybersecurity relevant to their lives," he says. For example, discussing how to keep bank account details safe will feel very alien, but the possibility of losing their Twitter or Snapchat account will quickly grab their attention.

With this in mind, the team has adapted the course material to make cybersecurity issues relevant to high school students, too. The modules are supported by detailed lesson plans, as well as videos and possible discussion topics. The new version has generally been well received by students, who seem to enjoy learning how hackers operate.

If you cannot gain access to these courses, Doug and his team are also developing a web-based version (www.security-literacy.org). The idea is to enable both teachers and students to learn about cybersecurity by themselves. Modules can be used sequentially throughout the term/semester or through a pick-and-mix approach to suit each class. Importantly, all materials are available free of charge.

For students interested in studying cybersecurity as a possible major, Doug's team has devised a project called IT-Adventures (www.it-adventures.org), which has been developed to attract more high school students to an IT field.

If you are a high school student, this may be a good way to venture into robotics and cyber defence. Form a club with your friends - it can be in school, through another group like Scouts or even home school - and register online at http://www.it-adventures.org/clubs/. Once your club is registered, you will have access to all the resources developed by Doug's team.

Unfortunately, the frequency of cyber attacks is likely to increase in the future, but this means professionals with knowledge and experience in cybersecurity will be greatly needed. In fact, the US Bureau of Labour Statistics predicts the demand for these professionals will be very high in the next few years, so it will be a good career option for students with an IT background.

ABOUT CYBERSECURITY

In the last few years, there have been several high-profile cyber attacks on multiple national and international companies. These include the attack on Twitter that affected accounts of many famous personalities like Bill Gates, Elon Musk and Barack Obama; and when a hacker known as ShinyHunters released 386 million usernames and passwords stolen from 18 different companies. Through their malicious actions, cyber criminals have accessed billions of personal records, such as emails, passwords and credit card details. With new threats appearing almost daily, there is an increasing need not only for tighter security measures but also for experienced cybersecurity specialists.

WHAT EXACTLY IS CYBERSECURITY?

Cybersecurity can be described as a way to protect information shared online from being stolen or shared without the owner's permission. With all the new devices that make up the Internet of Things, like phones and smart TVs, cybersecurity is fast becoming one of the main challenges in the modern world.

WHAT ARE THE LATEST TRENDS IN CYBERSECURITY?

Hackers commonly use automated systems to mount their attacks, which makes them very difficult to catch. But now, cybersecurity specialists are starting to use similar technologies to predict attacks and stop them before they happen.

WHAT ARE THE ESSENTIAL SKILLS TO FOLLOW A CAREER IN CYBERSECURITY?

This is a rapidly changing field, so professionals need to be able to adapt quickly to evolving threats and even anticipate them before they breach security systems. Cybersecurity specialists also need core skills like computer programming and coding, as well as risk analysis and problem solving.

HOW TO BECOME A CYBERSECURITY SPECIALIST

Maths and computer programming are the best subjects to study at school to follow a career in cybersecurity. With the increasing need for cybersecurity specialists, many universities and colleges now offer programmes in cybersecurity education. To find out more, visit: www.cyberdegrees.org/listings/top-schools.

There are also several security certifications available, such as the Certified Information Systems Security Professional (CISSP): https://www.isc2.org/Certifications/CISSP#.

According to the US Bureau of Labour Statistics, experienced cybersecurity analysts can earn up to $99,000.

PATHWAY FROM SCHOOL TO CYBERSECURITY

There are many different pathways you can take to become a cybersecurity specialist:

- Get a degree in maths, computer science or any related subject. Some employers ask for post-graduate studies, such as a Masters of Business Administration (MBA) in information systems. This two-year programme covers both business and computer courses.
- There are also several cybersecurity apprenticeships that allow participants to earn while they learn. This PDF from the National Institute of Standards and Technology, US Department of Commerce, offers some great advice: (https://www.nist.gov/system/files/documents/2018/01/09/nice_apprenticeship_one_pager_oct_31_2017.pdf)
- The final option is to work your way up with an IT security firm, gaining experience while studying for further qualifications.

DOUG'S TOP TIPS FOR STUDENTS

1. Get involved in activities that you're passionate about.
2. Explore your curiosity, learn how things work and play with computers.
3. Don't be afraid of trying things!

HOW DID PROF DOUG JACOBSON BECOME A CYBERSECURITY EXPERT?

WHAT WERE YOUR INTERESTS AS A CHILD?

I was interested in building things, whether it was building forts, playing with electronics or helping my dad with construction projects.

WHO HAS INSPIRED YOU IN YOUR CAREER?

My 9th-grade teacher got me interested in electronics when we built an electric motor. In high school, my physics teacher taught us more electronics and also arranged for a few us to get together at a local college on a few Saturdays and play on a computer. This was long before computers were in general use!

WHAT HAVE BEEN YOUR PROUDEST CAREER ACHIEVEMENTS SO FAR?

Building a new degree in cybersecurity engineering at Iowa State and launching it.

WHAT AMBITIONS DO YOU STILL HAVE TO ACHIEVE?

Getting wide-spread adoption of the cybersecurity literacy and essential materials we produce.

WHAT DO YOU FIND MOST REWARDING/CHALLENGING ABOUT YOUR WORK ON COMPUTER AND NETWORK SECURITY?

This is a field that changes every day. If cybersecurity were a game, it would be unfair since the good people can only play defence and always have to get it right. The attackers play offence. So, the best we can hope for is a draw. Working in cybersecurity helps people directly, and cyber literacy has the potential to reach a large number of people from different backgrounds and with other interests.

WHAT DO YOU FIND MOST EXCITING ABOUT THE IOT? WHAT DO YOU FIND MOST CONCERNING?

IoT can make our lives so much better by making the world more efficient and reducing time wasted. The concerning part is that these devices are often built without security in mind, and they are harder to protect since we do not directly interact with them.

WHAT WOULD MOST PEOPLE BE SURPRISED TO KNOW ABOUT CYBERSECURITY?

Most attacks target people and not computers. Attackers want information on you, rather than information on your computer.

DOUG'S SECURITY LITERACY PROJECT USES A FICTITIOUS VILLAGE, HACKERVILLE, THAT ALLOWS STUDENTS TO EXPLORE CYBERSECURITY. MEET TWO STUDENTS WHO WERE INVOLVED IN WORKING ON IT:

MELISSA HERNANDEZ

I built the CityBank site (both the real one and the 'fake' one), and I designed my own plugin for the site, which would let it act as a real banking website. It was challenging, but it was also a lot of fun.

I gained an entirely new set of technical skills from the Hackerville project. Before this summer, I had no experience with WordPress, the WordPress API, or with the Personal Home Page language (PHP). Now, I've built my plugin from scratch in PHP that allows our team to enhance the capabilities of WordPress. I feel like I've grown as a person and as a developer.

My key advice is that it is better to be safe than sorry! Taking extra security precautions online can slow you down occasionally, but it is much better to take the extra minute to answer a security question than to realise your account has been hacked.

From my experience in school, I think I may eventually end up being a mentor or a project manager. That's not something I ever planned for myself, but I'm fond of leadership and good teamwork, and I often find myself leading the team projects I'm a part of.

CHRIS HORVATICH

My role on the Hackerville project was to replicate common websites that people use every day, such as social media sites, to be used for training.

I gained a lot of cybersecurity knowledge as well as practical cybersecurity experience. Our project was submitted to the 2020 Summer Virtual Undergraduate Research Symposium at Iowa State University, which was a good learning experience for me as well.

I would tell young people to never forget the human element when dealing with cybersecurity issues. Your security is only as strong as your weakest link. You can throw a lot of money into technology to secure your systems, which would make people your weakest link. Malicious hackers will use phishing and social engineering to target people's laziness and fallibility. Trying to train people to be on the lookout for these attacks is the best way to prevent them.

I see myself graduating with a Major in Cybersecurity Engineering and a Minor in Computer Science. One day I hope to own a business that does cybersecurity contracting.