Expert Opinions and Academic Research: CyberCrime in Education

by Nicole Ponsford, Digital Education Specialist, Achievement for All.

To understand why schools need to be more engaged with cybercrime and cybersecurity, leaders in the field were asked for their views. Here are their responses.

Why should schools educate students in cybercrime as a safeguarding topic?

Expert Opinions 1#

Chris Blackwell, Freelance IT Consultant, begins by saying the main issue is an innocent ignorance by the general public:

"Computer Security (as it was once known before the marketing folks invented the term 'Cyber') used to be something that the general public could put to the back of their minds, so long as they had some antivirus software installed. Going back only as far as the millennium, "compromising computer security was something of a game for the attackers, who would create 'viruses' and 'hack' computers primarily for interest and kudos from their peers.

In the past 10-15 years, with the huge growth in financial transactions being possible online, and with the help of tools such as TOR and BitCoin to remain anonymous, it is now possible to steal, coerce, or demand (through a ransom) a person to part with their money.

It is not necessary for everybody to understand the methods and techniques that are used in modern cybercrime, but there is an argument to say that **the** more that is understood by the masses, the better a person, a family member, a school, a company or even law enforcement can defend themselves and others against cybercrime. Trying to keep up with the various techniques in use at any time is probably not realistic for most people, because they are varied. However, by teaching the basic principles of security and risk in schools, it should help to create a healthy respect and inform everybody that the internet has become a pretty hostile place.

So, what are the best things to teach students? Blackwell says, "The best thing they (schools) can do is to reinforce the message of TNO. This is a term used by some security professionals and means **Trust No One!** It sounds overly dramatic, but if this attitude is adopted when working online, it will lead people to be at least a little suspicious of everything and everyone.

As mentioned above, it is not realistic for everybody to understand all the techniques in a cybercriminal's armoury. However, an understanding of the purpose of an attack is probably a good idea. If we assume a modern cybercriminal is primarily motivated by money, that will

© Achievement for All 2017

cover most scenarios. The outcomes he/she is then looking for are to either covertly steal sensitive information, which will allow them to obtain money or goods in the victim's name, or to overtly demand money directly from a person in the form of a ransom.

From these points you can work backwards, and any techniques used by the criminal are always with these outcomes in mind.

The two primary methods to achieve these goals will be:

1. Stealing a person's passwords. This can be done in a variety of ways, but the key message for everybody should be to use complex passwords and not to reuse passwords on different sites. The idea being to make it as difficult as possible to obtain the first password and if that is successful it does not give the attacker access to numerous online services belonging to the victim. The use of 'two factor' authentication is also a good idea and is a very strong protection.

A person's passwords or credit card details can also be stolen from third party websites who are holding them. This is very difficult to defend against because the victim has no control over the website which holds the data. Avoiding password reuse helps here as mentioned above. I also avoid entering credit card details into websites whenever possible and opt for retailers who I already have accounts for such as Amazon or anything Paypal connected (sometimes even if it costs more!)

2. Installing malware onto a computer. This is often the first step and will give the attacker the ability to run crypto-code as part of a ransomware attack, or run some other software covertly (such as a key logger) to steal information (such as passwords). The key defence against malware is to install security updates (and to a lesser extent install antivirus software) and to avoid clicking on malicious links.

Further Security Tricks: Probably the simplest thing that everybody should be doing is applying the security patches to their computers/phones/tablets as soon as they are available. This is so simple, but it is amazing how many people (and large organisation who employ security professionals and dedicated IT staff) do not do this quickly enough.

A quick background in how much of the malware or attacks work; the vast majority of attacks rely on some kind of security hole in some commonly-used software. Somebody somewhere finds the security hole - could be a good guy researcher, a bad guy hacker or even a government. There is now a period of time when the vulnerability can be used by those who know about it to cause trouble before the vendor of the software learns about the problem and issues a security patch - during this period the vulnerability is referred to a a 'zero day' vulnerability. This time period can vary depending on who discovered the vulnerability and if it has been disclosed to the vendor. However, the irony here is that attacks during the 'zero day' period are often relatively small compared with those after the patch has been released. The bad guys will very often build their malware to attack

© Achievement for All 2017

vulnerabilities discovered by others and that have already been patched by the vendors (e.g. wanna cry). They then simply rely on the fact that many people and companies have not installed the patch to fix the issue quickly enough. If everybody patched as soon as the updates were available, the number of successful attacks would be hugely reduced.

With regard to avoiding clicking on links, this is nothing new and seems to be widely known regarding links in emails, but attackers will post links hosting malware to anywhere they can. This includes links in email, on social media sites, forums, chat sites and anywhere where a link could be placed to tempt a user into clicking. Many links will have their true addresses masked and what appears to be a trusted site (bbc.co.uk for e.g.) may actually point somewhere else. It is often possible to see the true address of a link by hovering over it but not clicking.

Padlock Your Browser. A further useful defensive technique, but one which can begin to get a little technical, is to look for the padlock in the browser. This indicates that the site they are connected to is using Transport Layer Security (or SSL, or HTTPS) and that the connection from their browser through to the end web server is encrypted. This technology uses Public Key Infrastructure Certificates to provide Domain Validation and, with a little knowledge, can be used to validate that the site is in fact genuine and not a spoof. it should be noted that a site without the padlock (TLS) is vulnerable to a man in the middle (MITM) attack. This means the connection to the website is in 'clear text' and could be read by a third party at an upstream point in the network.

Public Networks. Whilst this is low risk, I generally avoid using public wifi networks because I have no knowledge of how secure they are or how trustworthy they are. As mentioned above, it is possible to capture some network traffic if you are participating on the same network as your victim and without the correct security. This could include passwords or other sensitive info. If I absolutely have to use the wifi in Starbucks, I use a Virtual Private Network, which creates a secure connection from where I am to a trusted point on the internet".

© Achievement for All 2017

Expert Opinions 2#

Robert Schifreen, Founder and Editor of SecuritySmart, believes that there are lots of reasons that schools need to educate learners in cybercrime. In fact, he says there are "All sorts of reasons". These include:

1. "Because kids who know this stuff will find it useful when they get a job".

2. Because they need to know how far they can go if they want to do a bit of hacking for fun.

3. Because kids of this age don't understand what it was like NOT to have permanent internet access in the palm of their hand, all the time.

4. Because knowing how to behave online is part of modern day citizenship".
Schifreen suggests the place to start educating staff, students and parents about CyberCrime is begin with a blank sheet. "The most important point is to define what they mean by cybercrime". He suggests asking what do they think are cybercrimes: "Fraud? Hacking? Hacking someone's files and altering their coursework? Guessing someone's password for fun? Stealing their phone? Impersonating them on email or on social media? Libelling someone online? Planting a camera in the toilets? Downloading pirated apps? Bypassing the lock screen on a tablet? Then, for teachers, it's all about a) being able to recognise it, and b) knowing how to handle it. Getting the right ratio of carrot:stick is really hard". Schifreen also knows that the messages are complicated. He suggests it isn't always about the "technical stuff" or "the legal ramifications" or "whether they'll get punished, or how they'll feel if they get caught/affected". He advises schools instead to, "Make it about how it will affect their relationship with their peers. That's what they care about".

© Achievement for All 2017

Expert Opinions 3#

Professor Richard Mills, Honorary Research Fellow of the Centre for Applied Autism Research (CAAR), Dept. Psychology at The University of Bath also believes passionately that cybercrime is a necessary topic for UK schools. He describes cybercrime as falling into two areas:

- **Cyber-enabled offending:** "These are crimes involving bullying, trolling, porn, theft, exploitation etc. Young people are vulnerable as perpetrators and victims . These offences that can be committed with or without a computer"
- **Cyber dependent offending:** "Crimes involving coding, malware, DDoS, hacking etc (Computer Misuse Act 1990). Young people are vulnerable as perpetrators and victims. These can be serious offences that can only be committed with a computer and may be unknowingly committed in non-UK jurisdictions. Offenders can be extradited"

He continues, "It is to a degree a generational issue - our research shows cyber interest includes offending is getting younger and younger". Interestingly, it is also male dominant. Mills says that " few girls are involved in cyber-dependent crime as perpetrators - although may be involved in cyber-enabled- probably social media (trolling and bullying) etc - but many more will be victims".

The reasons that young people can turn to cybercrime as a means of showing off their tech-savvy skills can be to gain kudos - albeit from a chat room or forum, or from their friends (real or in cyberspace). Mills' research supports this, "Recognition is key, rather than financial gain. "Offenders have a 'non criminal' background and profile. Teachers and parents are often out of the loop when it comes to understanding". This is why it is crucial that schools use experts for this safe-guarding issue, just as they would with issues in the real world (like sexual abuse or domestic violence). "Some young people are contemptuous of older people's lack of computer nous and it is important the cyber education is undertaken by people who really know their stuff or they will have no credibility". One barrier is that many teachers are new to the topic of online safety beyond phot-sharing and are not aware of the issues/solutions when it comes to online safeguarding and law. "Teachers are sometime slow to admit that they don't know." Mills is currently working on research to explore the links between cybercrime and users with autism.

© Achievement for All 2017

Expert Opinions 4#

Dr Tim Summers is a Hacker, Professor and Comsulted Expert. He is CEO of Summers & Company, Founder of WikiBreach, and the Director of Innovation, Entrepreneurship & Engagement in the iSchool at the University of Maryland, College Park. Dr. Tim Summers says, "My research on HowHackersThink proposes a framework for developing the cognitive skills necessary for cybersecurity effectiveness. There is much literature that outlines the various methods of cognitive and psycho-social aspects of learning technology; however, there is a dearth of literature that specifically addresses cybersecurity. To effectively teach cybersecurity to the youth, we must understand how to build the correct mental models necessary for dynamic thinking required for security research and analysis.

I call this **the hacker mindset**. **The hacker mindset** refers to the cognitive skills and traits necessary that must be developed in order for one to be effective at security research and analysis.

You may find value in reviewing the following literature. Personally, I found value in the perspective that Ramalingam (2004) takes with regard to understanding the role of self-efficacy in learning how to write code. Voiskunsky (2003) outlines a model for hacker motivations, which could be helpful in identifying specific elements of the black hat mindset. Van Beveren (2000) provides a conceptual model of hacker development and motivation which could also lend itself well to your module. All of my research uses engaged scholarship by Van de Ven (2007) which you might also find useful.

Why is cybercrime a necessary topic for schools to educate learners in?

Piaget (1973) suggested that the child's mind builds cognitive structures, such as mental "maps", schemes, and networked concepts for understanding and responding to experiences within his or her environment. We have seen revolutionary changes in our society, particularly widespread proliferation of technology, especially in education. With these changes has come a rotten fruit of the times, cybercrime. But this fruit has brought about, as suggested by Pea (1984), an abundance of new opportunities for addressing questions regarding the design of educational activities that integrate aspects of cybersecurity, and interconnectedly cybercrime. If we were to refer back to Piaget's theory regarding child development and learning, we would need to ask questions about the mental activities engaged by cybersecurity and cybercrime.

In the security community, we make a strong case that one must understand elements of cybercrime in order to combat it within cybersecurity. Gercke (2012) states that "cybercrime and cybersecurity are issues that can hardly be separated". And as cybercrime has become a prominent element within today's society, we must develop and engage the mental capacity of our future thinkers. It would be a disservice not to do so. Additionally, there has been much research on using education as a means to deter youngsters with an interest in cybersecurity away from a life of cybercrime.

What are the top things that educators should know about cybercrime and cybersecurity?

© Achievement for All 2017

I believe it to be important for teachers to understand the relationship between the two. As suggested by Gercke (2012), cybersecurity is important to the development of information technology and the evolution of Internet services by enhancing our infrastructure, national security, and economic well-being.

It's about *making the Internet safer for all*. It's a common mistake to believe that cybersecurity and cybercrime education are all about the technical and procedural measures. This couldn't be further from the truth.

Developmental theorists such as Piaget and Inhelder (1969), Werner (1957) and Vygotsky (1978) provided profound research regarding the development processes addressing technologies in education.

Following this line of thought, Pea (1984) proposed that cognitive development consists of a "series of progressive reorganizations of knowledge driven by the child's active engagements with physical and social environments". This is especially try in cybersecurity and cybercrime. Effective education in these areas much engage the physical and social environments. And we are now beginning to ask questions about the socio-technical implications of cybersecurity, which I believe will also be a huge point of debate for child cognitive development in the near future.

What organisation or links would you suggest educators refer to when educating themselves and others about this?

Unfortunately, there is a huge need for resources for educators. For too long, we have relied on the professional credentialing industry to provide the majority of educational opportunities in cybersecurity. But this represents a massive opportunity for educators, researchers, and practitioners to collaborate and create a new model for cybersecurity and cybercrime education. In my opinion, resources like this are non-existent.

One of the best resources that I've seen currently is from PBS Nova Labs: http://www.pbs.org/wgbh/nova/labs/about-cyber-lab/educator-guide/

© Achievement for All 2017

Expert Opinions 5#

Dr. Jamie Saunders (Director of the UK National CyberCrime Unit) agrees, and believes that education is needed for teachers to help identify teenagers at risk of being involved in hacking or other cyber offences, mainly as they do not realise that what they are doing is a crime. He believes that professionals need to be able to "spot" children who are at risk of this - and as young as 12 years of age. In this Guardian interview, he said that his idea of a new 'Cyber Prevent' scheme for young people would be used to both inform and recruit "tech-savvy young adults":

“A lot of kids are stumbling into this crime. This activity has consequences for them and others. There are legitimate opportunities for their skills,” Saunders said. The target group would be those aged 12 to 25. One major cyber-attack, which is currently subject to legal restrictions, was carried out by a teenager.

Analysis of investigations undertaken by the national cybercrime unit in 2015 found the average age of suspects was 17. The previous year, the average was 24.

Saunders said some cyber-attacks had been carried out by children who did not realise the harm they could do. “We are not dealing with serious criminals. Some are sucked in and damage their careers and do a lot of harm,” he said. “We need education for schools on the [1990] Computer Misuse Act, on what it is and isn’t [a cybercrime]. A lot of kids don’t realise they are committing a crime,” he said.

Dr. Jamie Saunders says, “We don’t want them to go to prison, we want them to come and work for us. The aim is to direct these talented coders and computer-whizzes into cyber security, rather than cybercrime. They are being shown they can earn a lot of money using their skills, instead of entering a life of crime".

© Achievement for All 2017