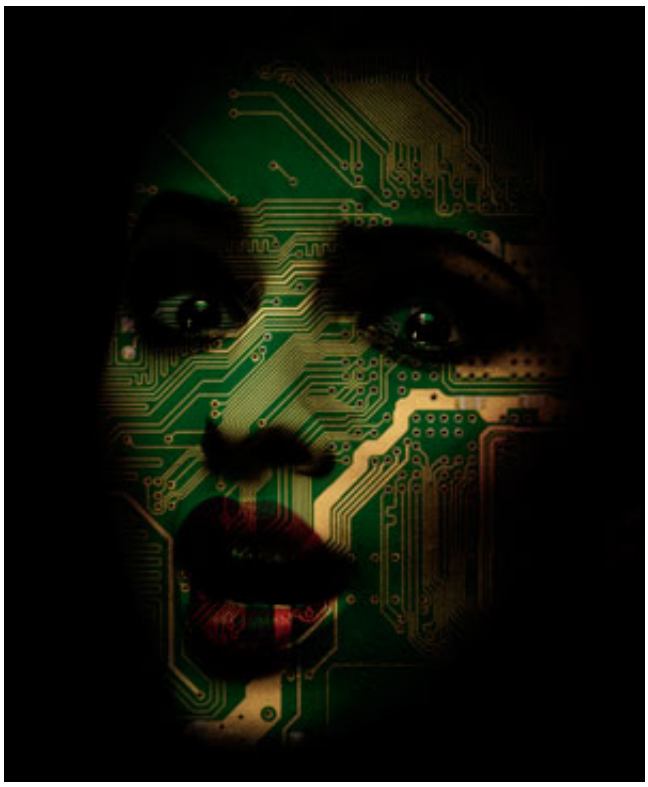
HIGH SCHOOL CYBERCRIMINALS WREAKING HAVOC

Why Are More Youths Committing Online Crime?



In June this year, UK authorities tracked down and arrested two people suspected of ring leading the largest international English speaking online cyber criminal forum. They were charged with stealing and selling the details of 65,000 bank accounts they had ransacked from computers infected with malware. They had sold the details at varying prices according to their origin, with US bank details going for $3, EU bank details for $5 and UK bank details for $7.

Furthermore, they had provided advice through their online forum on the best ways to use the details to wire money, purchase items online or pay for other services. According to the authorities, more than 8 million pounds (US$12.5 million) had subsequently been stolen from these accounts. The kicker – the two alleged criminals, Nick Webber and Ryan Thomas, were both teenagers (18 and 17) and still in high school.

Unfortunately, this is far from being an isolated case. With the continuing growth of the internet, youth cybercrime is fast becoming a mainstream issue. In a recent survey conducted by Tufin Technologies, an online security company, it was found that roughly one in six teenagers in the US, and one in four teenagers in the UK, had tried their hand at some form of internet 'hacking'.(1) Gone are the days when computer crimes were restricted to the socially awkward Napoleon Dynamite look-a-likes. These days, multi-million dollar damage can be caused by a teenager conducting simple 'point and click' attacks using the family computer. The question we have to ask is: why are contemporary youths so willing to jump into the world of cybercrime?

Theory 1: Cybercriminals are the New Rock Stars

In a 2008 interview with the BBC, Mark Bevan ('a reformed hacker') gave an explanation as to why more teenagers are becoming hackers: "The aim of what they are doing is to get the fame within their peer group."(2)
This suggests that many youths are turning to cybercrimes simply because it is the 'in thing' – a claim reinforced by the Tufin survey which found that almost 40 per cent of teenagers admitted that they thought illegal 'hacking' was cool.
Perhaps then, a finger of blame should be pointed at the portrayal of cybercriminals in popular culture. For years, the internet underworld has made appearances in mainstream culture – Matthew Broderick played the role of a hacker in the 1983 movie 'WarGames', while Keanu Reeves' character started out as an illegal coder in the blockbuster Matrix trilogy. Furthermore, when cybercriminals have made appearances in popular culture, they have generally been portrayed in a positive light. According to a study by Damian Gordon, which looked at the portrayal of computer hacking in popular media over the last 40 years, 70 per cent of hackers featured in films in this period were portrayed as the hero, regardless of whether their acts were illegal or not.(3) This trend looks likely to continue, with the current 'Millennium Trilogy' movies all celebrating the hacker Lisbeth Salander and her predisposition to frequently commit cybercrime.

As an 11 year old, my first impression of computer crime was heavily influenced by the 1995 movie Hackers, in which teenagers (including a youthful Angelina Jolie) used unconventional and illegal methods to take down an evil computer specialist who had framed them as terrorists. The teenagers – who wore outlandish outfits; went to nightclubs and parties; and gave themselves tag names such as 'Crash Override' and 'Acid Burn' – ended up outsmarting the ignorant and incapable secret service and gave hackers worldwide a 'cool' image in the process. And unlike the rollerblades and bright lycra that featured prominently in the film, it appears that cybercriminals have only become cooler.

For instance, a recent issue of Rolling Stone Magazine even jumped onto the issue of cybercrime. In its June issue, the magazine published a feature article entitled 'Sex, Drugs and the Biggest Cybercrime of all time,' which told the story of Albert Gonzales – the mastermind behind an international cybercriminal ring that stole over 170 million credit and debit card numbers at an estimated cost of US$200million to corporations and insurers, all while hosting lavish parties and consuming copious amounts of cocaine, ecstasy and LSD.

There is little doubt that youths are influenced heavily by popular culture, and youths will always use popular culture as a guide to achieving notoriety among their peers. Unfortunately in this case, the way popular culture has increasingly portrayed cybercriminals in a positive light appears to be encouraging youths to commit unlawful acts.

Theory 2: Easy Crime, Big Reward

Other explanations also exist to account for the distinct increase in youth cybercrime. Some suggest that youths are committing cybercrimes simply to reap the large illicit rewards that it can provide. There will always be some youths on the look out for an easy dollar. Unfortunately, the advent of new internet technologies has given rise to a situation in which opportunistic youths have now been given a means to commit crimes that were commonly perceived to be massively disproportionate to their age. Before the internet era, youth crime was more or less limited to minor offences such as shoplifting and other simple thefts. Nowadays however, cybercrimes committed by youths can include anything from large-scale software piracy to multi-million dollar credit card fraud.
According to the US Department of Justice, the ability of juveniles to portray themselves as adults in the online world has allowed them to access brand new areas of criminality. Areas which would deny youths access in the real world, such as online auction sites, financial service websites, and discussion forums, are all easily reachable with the click of a mouse, regardless of the user's age. The internet allows an individual to commit serious and far reaching offences. It has become almost impossible to ban someone from the internet, with connection points available in so many areas (e.g. schools, cafés, and libraries) and young people everywhere can easily log on and get up to all kinds of unsupervised online mischief. And they do: one in ten of the teenagers that admitted to 'hacking' in the Tufin survey also admitted that they had done so for money.
In addition to the wide accessibility that the internet provides to youths, the level of skill required to commit

many online crimes is very low when compared to the skills required to commit large scale crimes in the physical world. Youths no longer need to be highly and technically skilled to commit online crime. Nowadays, any novice user can download a wide range of 'Hacker Tools' with easy-to-use guides, and this alone has greatly increased the number of potential online criminals. Crimeware tools such as Zeus, Sploit and Fiesta are easily attainable online, and at no cost. With online weapons so easily accessible to youth, and so easy to operate, it is of little wonder that so many young people are trying their hand at cybercrime.

Theory 3: Malicious Curiosity

There are also many youths that actually possess highly technical skills, and are using these skills to increasingly commit serious cybercrimes that reap little to no personal gain. Just last month, a Canadian student was charged with hacking into a school board website and exposing the passwords of 27,000 fellow students. Furthermore in September this year, a 17 year old Australian was found to be the creator of a computer worm that crippled Twitter for several hours. The worm exposed a flaw in the microblogging site which allowed other hackers to send unsuspecting users to Japanese pornography sites. When asked to explain why he hacked Twitter, the student's response was 'To see if it could be done.'4 This answer sums up the major motivation behind many of the more highly skilled young cybercriminals, in particular the young 'black hat' hackers – they simply do it to see if they can, without any thought to the real-world consequences. If they break through a system and cause large amounts of financial damage in the process, it is the system's fault for being 'weak'.

Theory 4: An Ethical Deficit

It is incidents such as the ones mentioned above that somewhat justify the US Department of Justice's (DOJ) claim that young people have an 'ethical deficit' when it comes to computer crimes.5 In the movie 'WarGames', there is a scene where Matthew Broderick's character, David, uses his computer to dial a large list of phone numbers without charge.
Jennifer: 'You could go to jail for that!'
David: 'Only if you're over 18!'
While the movie was made in 1983, the scene still typifies the present generation of youth's naïve and cavalier attitude towards computer crime. In a Scholastic Inc. poll referenced by the DOJ on their website,6 48 per cent of elementary and middle school respondents do not believe that hacking is a crime. Furthermore, in another study quoted by the DOJ, 34 per cent of university undergraduates admitted to illegally pirating copyrighted software. The existence of this ethical deficit increases the likelihood that even young people that are unlikely to commit traditional crimes in the physical world may be much more inclined to commit crimes online.

The Solution?

There is no doubt: today's youths are becoming more and more willing to commit cybercrimes. While explanations may differ as to why this is the case, one question that needs to be answered is 'What can be done to address this problem?' According to the US National Crime Prevention Council, the best way to halt the youth cybercrime phenomenon is through widespread education.7 They suggest that young people need to be taught the legal and ethical rules of the internet, as well as how to use the internet responsibly. Currently, most children do not view cybercrime in the same light as crime in the physical world, and they need to understand that illegal actions online carry real consequences and cause large scale emotional and financial costs to victims. This concept is also supported by the US Department of Justice, which has launched a campaign aimed at both parents and children with the goal of raising awareness on the importance of 'cyberethics.' On the website 'Cyberethics for Kids'8 the DOJ provides a children-targeted explanation of the harmful effects of cybercrime, while on its website 'Cyberethics for Parents and Educators'9 the DOJ attempts to outline an appropriate syllabus that adults can use to teach young people about the specifics of internet responsibility.

The UK and US have also adopted much more specific initiatives to reduce the instances of youth cybercrime.

Targeting teens with highly technical skills, the two governments created a contest aimed to test the skills of young hackers and to attract them to the idea of using their skills for positive purposes, rather than becoming cybercriminals. In one of the US challenges, competitors were required to analyse a hard drive to find evidence to convict criminals, while in another they had to defend a network from attacks. One eventual contest winner earned bonus points by breaking into the contest scoring system and awarding himself 10,000 extra points. The aim of the programme was to encourage young hackers to consider careers in internet security, either for the government or private corporations, rather than using their skills for criminal motivations.

Nevertheless, the internet is spreading and the number of global youths with online access is increasing significantly. Unless successful and widespread initiatives are implemented soon, the number of young people willing to commit online crime will continue to increase just as drastically.

Andrew Dornbierer is a UNICRI intern assigned to activities related to the prevention of cybercrimes.

---

1 R Gan, 'Tufin Survey Finds One in Six New York Teenagers Hack - And Rarely Get Caught', Tufin Technologies, 14 April 2010, http://www.tufin.com/news_events_press_releases.php?index=2010-04-14

2 M Ward, 'Alarm Raised on Teenage Hackers', BBC News, 27 October 2008, http://news.bbc.co.uk/2/hi/technology/7690126.stm

3 D Gordon, 'Forty years of movie hacking: considering the potential implications of the popular media representation of computer hackers from 1968 to 2008', International Journal of Internet Technology and Secured Transactions, Vol. 2, No.1, 2010, pp. 59 - 87

4 B Malkin, 'Australian Teenage Hacker 'Easily' Crippled Twitter', Independent.ie, 22 September 2010, http://www.independent.ie/world-news/asia-pacific/australian-teenage-hacker-easily-crippled-twitter-2348715.html

5 J DeMarco, 'It's Not Just Fun and War Games – Juveniles and Computer Crime', United States Department of Justice, http://www.justice.gov/criminal/cybercrime/usamay2001_7.htm

6 Ibid.

7 National Crime Prevention Council, 'Teaching Youth Cyberethics', United States National Crime Prevention Council, http://www.ncpc.org/programs/teens-crime-and-the-community/monthly-article/teaching-youth-cyberethics

8 United States Department of Justice, 'Cyberethics for Kids: The Internet –Know Before You Go Into Cyberspace', http://www.justice.gov/criminal/cybercrime/rules/kidinternet.htm>

9 United States Department of Justice, 'Cyberethics for Teachers – A Lesson Plan Outline for Elementary and Middle School Children' http://www.justice.gov/criminal/cybercrime/rules/lessonplan1.htm