Global Information Assurance Certification Paper

SECURITY ESSENTIALS PRACTICAL ASSIGNMENT:

What Should I Tell My Kids About Hacking?

Lee Biard

Abstract:

As we have moved into a connected environment where the world is joined by a single communications arena that is called the Internet, many wonderful things have happened. Scientists and physicians have been brought together to share information across the world. Students (old and young) seeking information have at their fingertips research that in the past would only be available by going to the largest libraries in the world. In these great libraries of the past, a "gatekeeper" existed to select and include materials that were beyond challenge. Copyrights were carefully protected. You knew when you were doing research that only you had access to your work unless you granted view to others.

Often a gem comes with a curse. With the Internet, there is no "gatekeeper". Anyone can post information and the value can only be guessed. Regarding privacy, while there is a perception that it is just you, your computer and a great store of information; little can be further from the truth. "Hackers, crackers, packet-monkeys, cyber-vandals, script kiddies, cyber-gangs, and cyber-crime" are terms which had little or no meaning 20 years ago, but are now waiting at the "other end of the line", or within your own computer for unsuspecting web surfers. The worst part is that often these criminals are our own children, 15-25 years old, with too much time on their hands and too little parental involvement.

"It is just harmless fun!"

People entering other computers without permission can do significant damage, with or without intent. This is called hacking.

Tell your child hacking is a crime!

What is a hacker?

Simply put, a hacker is someone who gains access to another computer without permission.

Why is hacking bad if someone just enters a computer, looks around, and does nothing to change or destroy information?

When someone breaks into a house, that is breaking and entering or burglary. Even if that person steals nothing or does no physical harm, it is still breaking and entering or burglary. There is a reason for this. People need to feel safe in their homes. Our laws recognize this.

When someone enters a computer where that person does not have permission to be, this is no different than breaking into a house:

- It belongs to someone.
- Others store possessions there.
- Others need to trust the safety of that location.

If someone were to break into a school locker, take information (a term paper or a bankbook) they would have valuable information of yours they could use. If someone broke into your computer and took that same information, would not the injury to you be the same?

> ***Tell your child that honest people, those who want to be respected, respect the rights and property of others.***

.

What real harm do hackers cause?

Hackers have been known to enter computers and:

- Alter files.
- Delete files all together.
- Use the computer time or other resources for their purposes.
- Send obscene e-mail from that computer.

Let us say that hacker was just having fun, trying to cause a little mischief, wanting to be noticed, wanting recognition for his/her knowledge. Let's say he/she entered the computer of a drug company and altered some of the files. The impact could be tremendous.

- If chemical formulas were changed, the next time the company tried to manufacture the drug the results could be deadly.
- At the very least, the company could recognize their computer was entered and files were potentially altered. The company would then have to spend many hours or days to determine when the hacking occurred, which files were altered, and how to best restore them.

- The cost of this recovery incurred by the company is then passed along to the consumer in price increases, making the product cost higher.
- This not only causes individual families to pay more for drugs, but causes insurance companies to pay more.
- Insurance then has to raise its rates, and again individuals incur more cost.
- As companies (who pay a part of employee's insurance costs) see price increases, they raise their prices on their products to maintain an acceptable profit for those people who own the company. Stockholders own most companies. Stockholders are people who invest their college funds and retirement funds in companies to make a profit.
- If consumers use their products, as the product cost rises, the customer's cost of living increases, and the amount of money they can spend on entertainment, eating out, vacations and other optional items is reduced.
- If other companies use their products, as the product cost rises, the companies' cost increase, and hence the cost of their products increase.
- In the end, **the consumer pays**.

Let us say the hacker enters the system, but alters no files.

- Once noticed, the company must still spend time to check and validate their systems and data, and to re-secure their systems.
- The cost spiral outlined above still is present with the same result.
- In the end, **the consumer pays**.

Let us say the hacker steals telephone time and computer time.

- There is $2 billion of telephone fraud every year. This is paid for by the telephone companies (and their stockholders) or by the companies who are held liable for that fraud because their computers were used by hackers (and their stockholders).
- Stealing computer time has similar results. If a company senses that their computers can no longer handle the load, they upgrade. This costs the company money, and affects their costs and their profits (and their stockholders).
- In the end, **the consumer pays**.

Let us say the hacker decides to crash systems, causing them to malfunction or not work.

- This causes the company to expend significant amounts of unplanned work in recovery and can often cause lost sales. The companies (and their stockholders) pay for this.

- What if this happened in a hospital, government agency, or other critical support function? It can reasonably be expected that people dependent on the services provided would suffer, and might even die.
- In the end, **the consumer pays**.

Let us say the hacker decides to steal intellectual properties. An intellectual property is the physical expression of ideas contained in books, music, plays, movies, and computer software. All of these can be sold in stores or on the Internet.

- Hackers steal valuable property when they copy software, music, graphics/pictures, movies, and books.
- Steven King recently published a book on the Internet entitled The Plant. He issued it in six installments. Twice he considered stopping the publishing because people were downloading the book and not paying the small fee ($1-$2). To quote Steven King from his web site "…Internet users have gotten used to the idea that most of what's available to them on the Net is either free or should be." This attitude will diminish or stop real creativity from going to the Internet first, or in some cases, going there at all.
- It costs the owner of the intellectual property real money to protect his asset, hence raises prices in a spiral as outlined above. It also limits potential sales thus discouraging future efforts.
- Our government has already identified real penalties for this type of action involving copyright materials. A copyright holder can sue for money to cover loss of sales or other loss, or a criminal remedy can involve jail or a fine to be paid.
- Is this different from walking into a store and stealing a product (say a book or computer software package) which someone has invented and manufactured? **It is not!**
- In the end, **the consumer pays**.

> ***Tell your child just as you want them to enjoy and feel safe on the Internet, you want others to have the same privilege.***

What can law enforcement do?

Kids cost parents a lot of time. They always have, but many parents do not understand this perspective. Parents are busier than they ever have been. Many feel that to have the nice things in life, both parents must work. You just can't be with your child every moment. Having a computer and Internet connection in a child's room allows him/her to keep them busy without infringing on the parent's time. One might be willing to assume there is no real danger in allowing children to entertain themselves in this manner if one operates under the following assumptions:

- It is not like the child is out running in a gang.
- If these companies really cared, they would put sufficient “locks” on their sites as to keep children from getting into trouble.
- These aren’t really crimes; it is just somebody getting picky.
- There are no “real victims” in these crimes.
- There is no physical trail.
- Law enforcement agencies don’t have time to deal with such “minor crimes”.
- It is too hard to track down these kids.
- These are just kids doing things kids do.
- He/she is learning about computers, after all.

These are poor and very dangerous assumptions. The following are just a sampling of articles available on the Internet. These were withdrawn with only a very small effort:

1) WOLFEBORO, NH (Reuters) - A 17-year-old New Hampshire computer junkie known as ``Coolio'' was arrested on Wednesday, March 8, 2000, and charged with hacking into a Los Angeles Police Department anti-drug Web site, officials said. Dennis Moran has admitted breaking into the Los Angeles police department's Drug Abuse Resistance Education Web site. Moran is being charged as an adult. If convicted on the felony counts, he could face up to 15 years in prison.
Moran, a high school dropout, told authorities and local media outlets that he hacked into http://www.dare.com because he disagrees with the site. ``I disagree with D.A.R.E.'s propaganda,'' Moran has told the Concord Monitor newspaper. ``Their program is misleading and they lie.''
According to the New Hampshire Attorney General's Office, Moran defaced the D.A.R.E. site with pro-drug slogans and pasted a graphic of Donald Duck with a hypodermic syringe in his arm into the site's home page. Moran also admitted hacking into the U.S. Government's Chemical Weapons Convention site, http://www.cwa.gov, and Internet Security Company RSA Security Inc. http://www.rsa.com. His attacks took place in November. The FBI interrogated Moran twice before Wednesday's arrest and confiscated the youth's computer.

2) A 19-year-old Houston hacker has agreed to plead guilty to one count of conspiracy for teleconferencing fraud and computer hacking in one of the government's most notorious cyber-crime cases, court documents show. Patrick W. Gregory, better known in Internet circles by his alias, MostHateD, is expected to plead guilty in U.S. District Court for the Northern District of Texas for his role as a founding member of a hacking ring called GlobalHell, who are said to have caused at least $1.5 million in damages to various U.S. corporations and government entities, including the White House and the U.S. Army.

Gregory, a high school dropout who has said he wants to start his own computer security business, admits in a plea agreement to stealing telephone conferencing services from AT&T, MCI, and Latitude Communications and holding conference calls between 1997 and May 1999 with other hackers around the country. Gregory could receive up to five years in prison for his crimes, and could be ordered to pay up to $2.5 million in restitution. "He just doesn't get it. He just doesn't see that all this damage is any big deal," said Matt Yarbrough, the former assistant U.S. attorney for the Northern District of Texas.

GlobalHell co-founder Chad Davis, also known as Mindphasr, was sentenced to six months in prison in March of last year for cracking the U.S. Army's website in June 1999. Davis, of Green Bay, Wisconsin, was ordered to pay $8,054 in restitution to the Army, serve three years of supervised release after the six-month prison term, and gain approval from future employers to use the Internet.

(Martin Stone, Newsbytes) [2]

3) A 17-year-old Colorado Springs boy was charged in juvenile court May 9, 2000 with one count each of computer crime and criminal mischief after he broke into the city's Web site in October, 1999 and replaced it with the message, "i love this city ytcracker 9d9 palmer high." The two felony charges carry a maximum penalty of two years of juvenile detention. The boy, known online as "ytcracker," said he is a benevolent hacker who was trying to alert officials of potential security glitches.

"I never had any intentions of doing damage," he said. "At first it was funny, and then I wanted to alert people to the security vulnerabilities in everyday software - and the fact that no one is immune." The boy said what began as a joke last summer turned into a precarious game between administrators of online Web sites and his own expertise. He said he started hacking into local business sites, then graduated into more complicated systems, like the Bureau of Land Management National Training Center.

The teen, who dropped out of school because he was "too bored," is a self-taught computer whiz who said he started using a computer when he was 2 years old. "I understand what I did was wrong," he said. "I'm hoping something good will come out of it."

(Danielle Nieves/The Gazette) [4]

4) What could have been a lengthy trial for a Canadian teen hacker evaporated January 19, 2001 when the youth known as "Mafiaboy" pleaded guilty to charges that he broke into Internet servers and used them as launching pads for attacks on high-profile Web sites. The 16-year-old from Montreal, Quebec, was facing 66 charges of mischief resulting from the attacks on sites that included Amazon.com, CNN.com, Yahoo.com, and the Web home of computer maker Dell. The teen, who can't be identified under Canadian law, had earlier pleaded innocent, but Crown prosecutor Louis Miville- Deschenes said today that "Mafiaboy" pleaded guilty to 55 of those charges. The charges

against "Mafiaboy" related both to the crippling of the Web sites and the network break-ins required to build the army of zombie hosts. The youth now awaits sentencing.
(Steven Bonisteel, Newsbytes)[1]

United States Attorney General Janet Reno said the boy arrested in Canada for jamming the CNN.com Web site and other sites in February must face punishment. Canadian police in Montreal announced charges against the hacker known online as "Mafiaboy" for jamming the CNN.com Web site and up to 1200 CNN-hosted sites for 4 hours on February 8. "I think that it's important first of all that we look at what we've seen and let young people know that they are not going to be able to get away with something like this scot-free," Reno told reporters on Capitol Hill. "There has got to be a remedy; there has got to be a penalty." Reno says the United States government continues to work with the computer industry on that incident and others, now that law enforcement has shown it can crack cyber-attack cases. "I believe this recent breakthrough demonstrates our capacity to track down those who would abuse this remarkable new technology and track them down wherever they may be," she says.
(Reuters)

5) FBI agents have arrested a Seattle youth as part of an investigation into a ring of seven juvenile hackers - three in the US and four based overseas - who are suspected of plotting a series of virus and denial-of-service attacks on Christmas and New Year's Eve 2000. The FBI reportedly arrested a 16-year-old suspected member of a suspected hacker ring that allegedly broke into severs of several Internet service providers in an attempt to use those computers to launch massive denial-of-service (DoS) attacks against an arbitrary set of targets.
Four Israeli hackers also have been arrested in connection with the case. US and Israeli authorities have received some help from one of the alleged victims in the case, DALNet.com, an Internet relay chat service. FBI sources say field offices have executed a series of search warrants in the case, and that more US arrests should be forthcoming.
(Brian Krebs, Newsbytes)

6) Jason Allen Diekman, alias "Shadow Knight" or "Dark Lord" has pled guilty in a California court to hacking into hundreds of NASA, US government and university computers. He could face up to 16 years in prison. Thom Mrozek, a spokesman for the US Attorney's Office in Los Angeles, said Diekman pled guilty to one misdemeanor count of hacking into a government computer, one felony count of damaging a computer, and one felony count of unauthorized use of a credit card, according to Reuters. He also admitted causing $17,000 in damage to the hacked computers. Diekman is scheduled for sentencing in February, 2001. In addition, he reportedly stole credit card numbers and ran up $6,000 in charges.

(Ian Stokell, Newsbytes)

7) Two Michigan youths were arrested September 15, 2000 on felony criminal charges for alleged hacking incidents, one of which left a pornographic image on a public school computer system in place of a photograph of the superintendent of schools.
Brian Salcedo, 17, and Jesse Salens, 19, were each charged with one count of unauthorized use, alteration or destruction of a computer system, the first computer intrusion cases brought under a 1986 Michigan law, according to the state attorney general's office. Both were arraigned today and released on their own recognizance. "Using a computer to break into a company from the comfort of your living room is just as illegal as using a hammer to break down that company's front door," attorney general, Jennifer Granholm, said at a news conference today. "Because the Internet makes the crime easier doesn't mean that it makes it right. These are the first hacking charges in this state; you can bet that they won't be the last." If convicted, the suspects face prison time of up to 5 years and/or a fine of $10,000. The $1,000 damage threshold under the law will be dropped by an amendment that takes effect next Tuesday.
(Dick Kelsey, Newsbytes)

> ***Tell your child hacking is a crime. Law enforcement agencies are making significant gains in enforcing laws that cover hacking and cyber-crime. Costs of legal defense must be born by the families of minor children, and come from funds that would otherwise be available for college, retirement, or vacations. Don't become a criminal for the "fun of it".***

What conclusions can we draw?

Rebecca Camber of Network Executive puts it well when she says, "Bands of teenage e-vandals, armed with readymade hacking codes, are threatening the integrity of the Net. They may sound like a bunch of schoolchildren in a drama class, but script kiddies are far from harmless. These kids are not the intelligent, high-tech hackers that every company dreads but the latest threat to the Internet as they deface, destroy and crash anything they can get their hands on in one costly electronic joyride. Mostly aged between 15 and 25, script kiddies, or "packet monkeys" as they are more affectionately known in America, are changing the electronic landscape. In the past, hackers had to spend years learning the inner workings of computer technology, programming and hardware. But now these young crackers are copying the work of the experts to wreak havoc online."

Part of the problem is that this is a world in which criminals are invisible and technical knowledge is power, hence law enforcement just doesn't work the way it does outside of the Internet. We as parents must teach our children ethics, standards that anyone can use to determine right from wrong. [5]

Children need to understand that it is wrong to look at another's e-mail. In "real life" we would not think of opening another's mailbox and reading, taking or destroying their mail. Not only is it well covered by federal law, neighborhoods contain eyes that watch.

In an unusual posture for law enforcement, the Justice Department is touting ethics education as a potentially powerful tool for addressing computer crime, from theft of intellectual property to digital vandalism. It has earmarked $300,000 as seed money to develop curricula, identify successful programs and spread the word that kids need ethical as well as technical education to become successful citizens in the Internet age.

"The standards of conduct that guide our lives are premised on the notion that we are going to have face-to-face relations with people," says Paul Thompson, philosophy professor at Purdue University in West Lafayette, Ind., who will teach a mandatory ethics course in the school's soon-to-be-established interdisciplinary computer security masters program. "But in the virtual world, that reinforcement dissipates."

Thompson says that is especially true for those drawn to computing. "Most people with science or engineering backgrounds tend to think consequentially," he says. If there are no apparent consequences to behaving badly, some might see no reason to do otherwise.

"Plato even recognized this," says Nancy Willard, professor of education at the University of Oregon in Eugene. "He tells the tale of a young shepherd boy who finds a ring that makes him invisible. The question becomes: If you are invisible, how will you act?"

"Why not target these young people into responsible positions with youth technology programs, where they are receiving advanced training, and direct them to apply their skills where we need them?" she asks.

The bottom line of all this is that it is up to a parent to see that the child behaves in a manner consistent with family values, just as you would monitor behavior when the child is in the public. Children need to know what is acceptable behavior, and that the parent will check to ensure appropriate behavior is forthcoming. Children also need to see this behavior modeled by the parent. This means paying for copyrighted items, and making certain your child sees this happen.

The computer the child has access to should be in a public, well-traveled area, not behind closed doors in the child's bedroom. The parent should have a good understanding of what the child is doing on the computer, and monitor that activity on a regular basis.

Remember, children often have little ability to think in terms of consequences. Per Susan Koeppen, trial attorney in the Justice Department's Computer Crime Section "They don't realize the illegality or the consequences."[3] Brendan Koerner Part of the love we show our children is not letting them play unsupervised in the streets of life (physical or cyber) until they are prepared with knowledge and maturity to do so safely.

Tell your child you love them. Show that love by becoming involved in what they are involved in.

Notes:

1) Bonisteel, Steven. "'Mafiaboy' Takes Rap On 55 Counts." Hacker Sitings and News. 19 Jan 2001. URL http://www.infowar.com/hacker/01/hack_011901b_j.shtml. (20 Jan 2001).

2) Burke, Lynn. "MostHateD to Plead Most Guilty." Wired News. 29 Mar 2000. URL http://www.wired.com/news/politics/0,1283,35264,00.html. (23 Jan 2001).

3) Koerner, Brendan. "Only you can prevent computer intrusions." News & Views. 22 Nov 1999. URL http://www.usnews.com/usnews/issue/991122/hack.htm. (21 Jan 2001).

4) Nieves, Danielle. "Teen Accused of Raiding City Web Site." Hacker Sitings and News. 10 May 2000. URL http://www.infowar.com/hacker/00/hack_051000a_j.shtml. (20 Jan 2001).

5) Zuckerman, M. J. and Rodger, Will. "Linking Online Kids With Real-World Ethics." USA Today Tech Report. 07 Jun 2000. URL http://www.usatoday.com/life/cyber/tech/cth562.htm. (23 Jan 2001).

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event