Title of Session: C3 - Your Kids Hacking into Trouble?
Moderator: Mary Radnofsky
Title of File: 20060703c3
Date: July 3, 2006

Room: After School Online

MaryLR: What exactly is "hacking?"

MaryLR: Hacking in today's sense refers to any unauthorized intrusion into a computer, its software, network, files, programs, addresses --- all of it.

MaryLR: Has anyone in this room ever had such an experience?

DanielLeje: Not I, I am a thirty year teacher, but just really getting into Educational Technology.

JeffC: Yes

JeffC: I've had experience with it... cracking (malevolent hacking)... happened when I was supporting a lab at a middle school.

MaryLR: I don't necessarily mean if YOU have hacked, of course, but perhaps you have received spam asking for personal information, or had a worm or virus?

JeffC: Oh... yeah... that stuff... *daily*.

DanielLeje: Same here

HeatherBu nods

MaryLR: OK. Well, so you know what an annoyance these things can be. Having a whole system hacked is much worse!

MaryLR: Here's a bit more about hackers: Hackers are people who basically try to find ways to access computers that do not belong to them. A hacked system can be one in which the intruder has just poked around, opened files and read documents. But hacking can also mean that someone is gaining special privileges and power so as to return to the computer and change or download its programs, insert spying software, spread viruses to other computers, redirect traffic to another website, steal the identity and passwords of everyone in the system.

MaryLR: One other piece of background information might also be helpful: There are black hat hackers and white hat hackers, and even gray hat hackers. Black hat hackers are essentially the bad guys: they try to sneak into your computer to do something malicious.

White hat hackers (many claim to be this, but actually few really are) are paid to verify the security of a company's computer and network by trying to hack in. Gray hat hackers also try to break into computers to test their security, but claim to do so for the good of the company or the public --- so that everyone is informed and so forewarned. These guys love the bragging rights, and mostly just want credit when they breach a supposedly secure system.

MaryLR: So, as educators and parents and generally responsible adults, how can we keep young people from engaging in this exciting activity?

JeffC: encourage them to stay away from the dark side of the force?

BJ: gosh, Mary, you do make it sound interesting?!

BJ: what about ethics of respect

MaryLR: Interesting, yes, but I'm not the one who started to make it so cool. In the news, television, movies, and online, we often see the exploits of computer hackers, both black hat and white hat, and their world looks like a 21st century version of a swashbuckling, romantic adventure on the high sea. There are also literally thousands of websites and tens of thousands of web pages devoted to teaching introductory hacking to young "script kids," as well as accessing "system administrator" privileges to the more serious and elite "crackers."

MaryLR: How do we compete with that?

BJ: I think you've stumped the audience, Mary Threats obviously don't work.

JeffC: cut and paste hackers abound on MySpace. As a result, cross-site scripting is fairly prevalent there... phishing attacks, redirects, etc. Of course, the standard K-12 admin response would be "shut it down." On the flip side though... they can really learn coding and gain skills that are marketable down the line.

JeffC: I'm not stumped... but I have to run.

DanielLeje: I guess supervision is not enough.

JeffC: We need to transform 21st century curriculum to adapt and allow for students to learn coding safely in K-12 schools... it ain't there now.

HeatherBu: It's one of the first things my middle school computer students want to know..."Miss, will you teach us how to hack?"

JeffC: trying to control it and clamp down will have a boomerang effect.

BJ: I really feel that values and ethics are also missing in our curriculum

MaryLR: Right on all counts. Some parents are teaching their kids to program at age 6; but something else must accompany the skills.

MaryLR: Logically, then, we have to find another way to show, convince and, when necessary, require kids to use their technical finesse to satisfactorily address their personal needs and emotions in legal, safe, and responsible ways. We can even help them to become better than we ever were --- and isn't that the mixed blessing of every generation?

DanielLeje: Sounds like a tough job.

BJ: it is a tough job, Daniel!

BJ . o O (there needs to be a manual on parenting too)

MaryLR: Here's one problem we CAN address: Kids will devote patient hours, weeks, even months to learn how to get in "back doors," write "malware" and design "packet sniffers." In fact what they are doing, respectively, is breaking and entering, vandalizing, and spying on their victims. But by giving these activities cute or invented names, cybercriminals have cleverly removed the aura of crime that surrounds their unethical and illegal behavior. That makes it harder to make the right choice as to whether or not they should hack, just a little. What6 if we called a crime a crime?

BJ: works for me...and why do these kids have so much time on their hands?

BJ: if they were being properly challenged in the classroom, they would be too busy to have time to hack

HeatherBu: Very true, BJ

DanielLeje: Where are they learning how to do all of this? Maybe I'm just to old to know this.

MaryLR: Teenagers are left to their own devices more and more after school, and most of them don't have the vaguest idea of the opportunities that are out there for clever computer kids.

HeatherBu . o O (they just search the 'net, Daniel)

MaryLR: Hacking n today's sense refers to any unauthorized intrusion into a computer, its software, network, files, programs, addresses

MaryLR: So kids just go poking around on the family computer, or the one in their own bedrooms.

HeatherBu nods

MaryLR: But we can show them some places they can best use their computer skills.

MaryLR: Most businesses now use computers in different aspects of their work, and many students could be placed in real-life interesting and challenging situations and rise to the challenge --- as well as to the expectations made of them in their jobs.

MaryLR: We can also work with after-school clubs, and invite some of these business people to talk with the kids, even choose one --- based perhaps on a competition to create something good (e.g. a new webpage for a new product) --- to become the company's intern for a week.

HeatherBu: I think that's a great idea for the older kids.

MaryLR: Is anyone familiar with such vocational ed programs?

HeatherBu: I've heard of them, but we don't have anything like that in my district.

DanielLeje: I spent thirty years in Vo -Ed, but the Agriscience side of it. We are always putting students out on work site for internships.

MaryLR: Moment - Technical trouble.

MaryLR: OK. So, teens can go out and do stuff. Maybe We can have them teach younger kids how to use the computer correctly. There are basic principles that must be learned, since we are not born knowing how to manipulate a mouse or write a program in C++, for example. Teens are often quite gentle with young children, and can teach them problem-solving skills on computer games even at a very young age.

DanielLeje: I am sure that in some of the larger schools, the business computer applications departments do something similar.

MaryLR: We could also have a productive version of hacking competitions, where there is a real-world effect of their cyberactivity: students could (and have, as you mention, in an increasing number of schools) designed computer games, animated movies, documentaries, multi-media presentations, and other creative products.

MaryLR: Did you find that in Vocational Ed the students found certain things particularly rewarding?

DanielLeje: Very much so! Anything that they could accomplish with their own hands always made them work hard at it.

MaryLR: Great. And the same is true in the cyberworld! Students are mature enough to realize that they want to do something REAL with what they have created. So the game

or the movie needs to serve a purpose, for example make a public service announcement about the environment, encourage recycling, raise money for a class trip, advertise a fundraiser, etc. Kids see problems all around them if they look, and so they could even identify their own cause.

DanielLeje: We have what is called CDE (career development events) which are competitions in every aspect of Agriculture. This could be applied in this area.

MaryLR: Sounds perfect. We can also provide students information about local organizations that need such products: non-profits or charitable groups, boys and girls clubs, the PTA, or the soccer team, for example. Anything to make it real, relevant, and meaningful.

BJ: especially since computers are being used more and more in agriculture, Daniel!

DanielLeje: We have several new CDEs this year including such things as job interviews.

MaryLR: But what if you find that you still have kids that want to hack? Let's talk about what you do then.

BJ: first impulse is to deny computer privileges at school, but that's probably the wrong thing to do

MaryLR: What about making the victims REAL people again? They are not just names and passwords on a computer screen.

BJ: community service?

HeatherBu . o O (just makes them want to hack into the school's system)

MaryLR: Punishments are certainly part of it. We want to get the kids to really understand, to sympathize with the victims of cybercrime, too.

MaryLR: While I do not advocate scare tactics, I do encourage adults to make it clear that hacking, with all its possible variants, is a potentially lethal crime, and that kids --- quite unintentionally --- can cause dire consequences with their online activities. For example, if all the phones go out in the city, how are you going to call 911 if your dad's having a heart attack? If you turn all the traffic lights red, how will an ambulance get to a hospital through the congestion and accidents? If you steal someone's identity and commit a robbery, it may be a nice single mom that wrongfully gets arrested in front of her child who is traumatized for life.

BJ: corrections facilities have victims awareness classes...

BJ: so a victims awareness class for hackers would probably be a good start

DanielLeje: I think that would be a great idea.

MaryLR: That would be a very good idea for juvenile hackers. I am not familiar with such programs, but will look into it!

MaryLR: Another example of how to make the victim seem more real to students is to create a simulated hacked environment for them. Deny them any access to the computer and/or cell phone for two days --- without prior warning ---, and see how they react. Let them realize on a personal level how their daily routine is disrupted, how they feel angry, manipulated, unjustly targeted.

BJ: can work for some, but might not work for others.

BJ . o O (you really have to know your students)

MaryLR: Good point. Since they probably know the denial is temporary, they may not get the sense of fear that many victims develop, nor will they necessarily understand the distrust that can happen. But they may develop a hint of sympathy for the everyday secretaries, clerks, or the tourists whose lives they may have otherwise complicated with their hacking activities.

HeatherBu: Mary, how do you suggest we teach younger students?

BJ: ahhhh...another topic that should be addressed...people on computers are real. They are not bots or animated characters

HeatherBu: Yes.

MaryLR: With both young and older children we need to demonstrate more compelling reasons not to hack, and these need to come from a sense of responsibility to community, society, and self.

MaryLR: One ethicist (Brian Harvey) compared teaching the ethics of computing to that of karate. He points out: "...Karate schools don't begin by telling novices, 'Here's how to kill someone.' They begin with simple, less dangerous techniques; the criteria for advancement include control and self-discipline as well as knowledge of particular moves. Instructors emphasize that karate is an art that should not be abused." I found that very wise indeed.

DanielLeje: I think the awareness idea is the best start. Many parents, students and even teachers (myself included0 are unaware of all of this hacking that goes on.

MaryLR: That raises an important point: How can I tell if my students or kids are hacking?

HeatherBu listens carefully

MaryLR: Exactly. Listen carefully. Do they use terms like, "spreading worms and viruses," "phishing or pharming," sending in a "Trojan horse," making a "zombie machine," becoming a "botnet herder," being treated like a "script kid, a lamer, or a n00b?"

DanielLeje: I guess by being fully aware that they are on task at all times while on the computer in the classroom and that parents are monitoring their children on computers at home.

JeffC is back.

MaryLR: That's tough, though, isn't it? Although there are programs that can help you monitor every keystroke of a kid's computer. But what if he's on at 3 am?

JeffC: The question is what tasks do you have them on with the computers? If they're bored out of their mind, they're more likely to get "off task" and into trouble.

HeatherBu . o O (Yes. They can hit Alt+Tab in a nanosecond)

MaryLR: Most of the time the kids are not hacking from the school classroom, of course. But if they are there, see if talk about their "work." Have they ever discussed all they can do while "packet-sniffing" as a "system administrator," in a "smurf attack" doing "DOS" (Denial of Service) hacks?

JeffC: They already know how to set up proxies on their home computers... and are usually a couple of steps ahead. Personally, if I had some bucks and was running an IT at a school I'd be sure I had NetOp School on the computers, so that they could be monitored. Barring that, make sure you have decent IUAs in place, try and stress responsibility. It would also be good if each student had an individual login so that history could easily be tracked. But really... all of this puts the burden on the schools, instead of responsibility in the hands (and minds) of students and parents.

MaryLR: Exactly. There are technical measures galore. But the kids will find a way around them. They need to learn a new culture.

MaryLR: I think it's important that we as adults learn --- and honestly believe --- that hacking is more than just a prank, mischief, or "no big deal." Some consequences of juvenile hacking have been to seriously affect the quality of life, as well as the very lives of millions of people.

MaryLR: (By the way, the chances are pretty good that your own computer has also somehow been hacked. A study last year found that 88% of home computers and 87% of corporate computers have been invaded by an unwanted program of some sort.)

MaryLR: (Unfortunately the odds of actually getting caught do not seem high enough to serve a real deterrent for most kids (though the justice system is coming down much harder now on juvenile cybercriminals, sending some to prison, banning many from computers, confiscating hardware, and imposing high fines).

JeffC: Mary... on my home computer I set up a "NetSurf" account that is limited... no .exe files etc. may be loaded. As a result I feel fairly safe from viruses, malware, browser hijackers, etc. and I surf *a lot*. Why isn't this possible on the K-12 level?

MaryLR: Most home and school users do not have nearly the expertise you clearly have. Many people also do not understand how to troubleshoot, so when some firewall or virus scan gets in the way of their word processing, they disable the safety mechanisms.

DanielLeje: Been there , done that.

MaryLR: But parents have such a vested interest in protecting themselves, both from the inside out and the outside in, that you'd think they'd be more careful. For example, Can I as a parent be held responsible if my child commits a cybercrime?

BJ: should you as a parent be held responsible if your child commits any kind of crime?

HeatherBu . o O (don't get me started on that one)

MaryLR: Well, there's an interesting twist: "can" I versus "should" I?

BJ: five more minutes, Mary.

MaryLR: OK. Thanks. Here's a little answer for you about responsibility: In California, for example, even if you are unaware of what your children are doing online, you can be held responsible if they get convicted of an Internet-related crime.

JeffC: What gets me is my little trick about setting up a limited account is so easy... just password protect Admin, set up limited accounts... you stop a heckuvalotta trouble.

MaryLR: And just for a bit more motivation to talk to your kids about what they're doing online, consider this. That means high fines, confiscation of property, and other ways of making amends. And, oh yes, cybercrimes often involve Federal law since the Internet crosses state lines and falls under the rules of interstate commerce. So you and/or your child could be guilty of a federal offense as well.

BJ: yikes! That might wake up a few parents.

JeffC: Well... I try to keep my 11 year old from downloading too much porn.

HeatherBu: Wow!

HeatherBu: Jeff!

JeffC: Of course, he is running several Nigerian scams right now... so I better have him cut back on that a bit.

MaryLR: You might also consider checking to see if the kids are more sleepy than usual. They may be IMing on different time zones...

BJ winks at Jeff...you bad boy!

JeffC: Actually... getting the kids involved with Snopes, Cybersafety, and a number of sites that help students learn safe surfing would be a good alternative for the hackers.

JeffC: kidding aside here.

BJ: the time zone thing can be a killer!

JeffC: But heck... paranoia runs so deep in my school district that wikipedia is banned.

BJ: is that paranoia the same in the homes, Jeff?

JeffC: We live in a world run on a foundation of paranoia... especially when tech and K-12 are concerned... 100% of the media relating to tech and the Net is negative... you need to get students positively involved with positive sites.

JeffC: yes, to an extent BJ.

JeffC: But "Just Say No" doesn't cut it on any level.

JeffC: Until you get kids actively involved with what they're doing, they'll be bored, and they'll do bad stuff.

MaryLR: There are some good, safe sites out there, and one that focuses on challenging girls in technology and the sciences, which is at zoeysroom.com. So let's keep them interested!

JeffC: and frankly... I think NCLB= Just Say No. It leads to boring curriculum and online activities that are usually of the "drill and kill" techniques.

MaryLR: So we have to keep kids thinking; they are very good at it, you know.

JeffC: I'm a member of cybersafety, wiredsafety and blogsafety...

JeffC: Well... they would be good at thinking if it weren't for these darned schools holding them back!

BJ: Mary, you've given us a lot of interesting facts and ideas to consider...

JeffC: thanks Mary

MaryLR: Just as a last piece of information, this past year, Virginia became the first state in the nation to pass an Internet Safety Law. (See http://www.eschoolnews.com/news/showstory.cfm?ArticleID=6261) It requires that Internet safety instruction be integrated into school curricula. Now safety involves not only protecting oneself from outside dangers, but it also means ensuring that children do not engage in dangerous Internet activity, even inadvertently. More states will undoubtedly be enacting similar laws, and it's about time.

HeatherBu: thank you, Mary

BJ: but it's apparent that the dialogue is far from over or concluded!

BJ: I hope you'll be able to join us again

JeffC: oh yeah... and isafe.org ...I'm certified there too.

HeatherBu . o O (I'm glad you were able to get your chat to work, Mary.)

MaryLR: It's been a pleasure talking with you all. If you have any questions, please feel free to contact me at my website, socratesinstitute.org.

HeatherBu: thanks

MaryLR: Good night.

DanielLeje: Thanks Mary, I've learned a lot tonight.

BJ: the next C3 discussion will be the first Monday in August

BJ: Thanks, Mary. Good job!