Title of Session: C3 - Cybersecurity: The forgotten element
Moderator: Davina Pruitt-Mentle
Title of File: 20080303c3security
Date: March 3, 2008

Room: Cyber 3 Group

BJB2: Welcome to this month's C3 discussion

BJB2: The topic is Cybersecurity: the forgotten element

DavinaP: Good evening everyone please into yourself

BJB2: I teach communication and am in Pennsylvania

ChristinaN: Hello, my name is Christina. I am currently student teaching in third grade. I am currently located in Houston, Texas.

DavinaP: Davina director for Ed Tech Policy research and Outreach and the C3 Institute and Univ of MD

LaurenKa: Lauren, California-Grad student in educational technology, elementary computer teacher

ShayneTr: I teach computers and art in Toronto the cold

LisaAK: Hi, Everyone! I teach visual communication technology and am in Ohio.

DavinaP: so we are all over the place tonight WELCOME!

DavinaP: please share your interest in cybersecurity?

ShayneTr: I teach teenagers, I am raising teenagers :)

LaurenKa: I want to know more so I can pass it on to parents and students...

ChristinaN: I'm constantly worried about spywares, viruses and trojans. Especially on this computer (brother's) because it does not have an antivirus scanner.

LisaAK: mostly from a developer standpoint -- that's where my interest is...

DavinaP: developer?

LisaAK: my husband's a software developer and I have been involved in the UI design of some of his work --

LisaAK: I hope that makes sense! :)

DavinaP: Got it Excellent so let's begin

DavinaP: I want to begin by sharing some interesting stats (or at least I think they are interesting) but please pop in at any point if questions....then will move on to how-to's etc... sound good?

LisaAK: Sounds great...

ChristinaN: Yes, sounds good.

DavinaP: From the 2007 FTC report Consumer Fraud and identity theft complaint data ---7th year in a row, identity theft tops the list, accounting for 36 percent of the 674,354 complaints received

ChristinaN: That's crazy.

DavinaP: Consumers reported fraud losses totaling more than $1.1 billion; the median monetary loss was $500. 85 percent of the consumers reporting fraud also reported an amount lost.

DavinaP: The percentage of fraud complaints with wire transfer as the reported payment method continues to increase. Twenty-three percent of the consumers reported wire transfer as the payment method, an increase of eight percentage points from calendar year 2005.

DavinaP: Credit card fraud (25 percent) was the most common form of reported identity theft, followed by phone or utilities fraud (16 percent), bank fraud (16 percent), and employment fraud (14 percent).

DavinaP: FTC reports that identity theft now affects more than 10 million people every year representing an annual cost to the economy of $50 billion

DavinaP: do these stats sound new?

LisaAK: I'm not sure the topic is new but the numbers are to me. This happened to me, but fortunately, it did not result (yet anyway) in any financial damage.

LaurenKa: I knew no stats. :)

DavinaP: but did you realize the issues with identity theft?

LaurenKa: Protection is widely commercialized so it is not too surprising…but is staggering!

LisaAK: Yes -- however, I think many people do not think it will ever happened to them, so the seriousness of the issue isn't always validated.

LaurenKa: But for $12.99/mo my bank will give a report...seems like they should anyway? I still feel scammed.

DavinaP: 2007 CSI Computer crime and security survey (surveyed IT admin from govt agencies and organizations (like banks) indicated 1/5 had suffered "targeted" attacks from malware

DavinaP: same CSI survey--financial fraud overtook virus attacks and insider abuse outdid virus issues as biggest security problem

DavinaP: can you think of any "insider abuse" ..several lately in the news

JeffC joined the room.

DavinaP: Hi Jeff

LisaAK: What about IT employees of department stores stealing customer credit card information?

DavinaP: that would be one--Jeff we were talking about "insider abuse" (security related issues)

DavinaP: another one in the news at least around the DC area ...see link http://www.washingtonpost.com/wp-dyn/content/article/2008/01/23/AR2008012302511.html?wpisrc=_rsstechnology

DavinaP: can anyone think of the "security issue" related to the DC issue (from the link?

LaurenKa: 200 times per work day...that's not just a slip on your mouse...

JeffC: yeah... employees stealing from their employers... pretty much a never ending issue I think.

JeffC: it's probably because most people think of their work as "jobs" (something they have to do to make money) rather than "careers" (something they love to do and get paid for it).

DavinaP: probably

DavinaP: but besides DC employees surfing "porn sites" 200+ times/day what would the security connection be? anyone think of anything?

JeffC: viruses

JeffC: porn sites are riddled with them

LaurenKa: If the gov't could track their IP addresses...so can anyone???

DavinaP: correct viruses, spyware, malware you name it and they are packed

DavinaP: Here's another security issue in the news
http://www.campustechnology.com/articles/57790/

DavinaP: while this is common and makes it into the headlines more than K-12----K-12 has become another hotbed.

ChristinaN: Yeah, the data stolen from universities is so common now, it's scary especially when I am still in college.

DavinaP: why are colleges and now K-12

DavinaP: ....targets do you think

LaurenKa: That's why it is important to spend all your money as fast as you get it so no one else can take it. :)

JeffC: usually easier to hack than businesses.

LisaAK: We had a major problem at our university with a professor who lost his pen drive that had years worth of students' SS #s on it -- is that relevant?

JeffC: that's why I'm glad I have lousy credit.

ShayneTr: So much is done on-line. I have some kids in university and all their info can be accessed on-line.

ChristinaN: hmm b/c there's a lot of students and maybe b/c the students are new to credit, et....

ChristinaN: and thefts can easily make accounts?
hmmmmmmmmmmmmmmmmmmmmmmmmmm.

ShayneTr: The students I teach have lousy passwords and they think nothing of giving them out the friends

LaurenKa: My life (and credit) is an open book online...banking, shopping, investing, EVERYTHING!

DavinaP: Lisa YES!!! and stolen laptops etc.. which also have student ID's etc... since usually needed to tag with grades etc...

LaurenKa: I discuss password creation with my students in sixth grade.

DavinaP: take a second or two and look at the debate with the national ID initiative http://newswire.ascribe.org/cgi-bin/behold.pl?ascribeid=20080116.080849&time=09%2019%20PST&year=2008&public=0

LisaAK: We've had both happen recently -- pen drives being lost and then laptops being stolen out of professor's offices....

DavinaP: Lauren this is GREAT!!

JeffC wonders why a prof has student SS#s. of course, I think it's a farce that our credit system is so lapse in this country that having someone's SS# is almost enough in and of itself to create a fraudulent account.

LisaAK: As a prof, I can look up and have access to anyone soc. # -- we're talking years of data here that the professor -- for WHATEVER reason (who knows!) -- kept in one area, on one source (his pen drive). Prior to student university id#'s, our id#s were our SS#s.

LaurenKa: In college a few years back our social was our ID number....we verbally announced it everywhere.

DavinaP: Jeff it use to be that the SS# were how you assigned grades, saw the class roster etc... not SS# are "no longer" an option and University ID's have to be used

ChristinaN: Yeah, now at the universities we get different numbers.

DavinaP: what does everyone think about the "national ID plan"--I heard on news today that Bush wants all health records for all citizens digital by some year (can not remember)

LisaAK: Different #s are assigned, but I'm sure a professor can find your SS#s very easily -- I know I can.

DavinaP: couple more stats and then we will move on...

DavinaP: SANS came out with their top 20 security threats http://www.sans.org/top20/

DavinaP: and GA Tech's Info security center also came out with their 2008 top 5 which indicate same items http://www.gatech.edu/news-room/release.php?id=1531

LisaAK: I think zero day attacks are a bit scary --

DavinaP: Web 2.0 and Client-Side Attacks – including social networking attacks and new attacks that will exploit Web 2.0 vulnerabilities

DavinaP: Targeted Messaging Attacks – including Instant Messaging attacks and malware propagation via online video-sharing

DavinaP: Botnets – specifically the spread of botnet attacks to wireless and peer-to-peer network

DavinaP: Threats Targeting Mobile Convergence – including voice spam, vishing and smishing

JeffC: on the flip side... I want to share a site with you that can help troubleshoot any virus/worm/etc. problem: http://www.techsupportforum.com/ ...registration and help is 100% free. there are security experts there. you go through several steps, post a "hijack this" log and the experts there will step you through whether or not your system is infected, and if it is, how to fix it.

LaurenKa: Are you a virus spreader...how can I trust you, Jeff?

DavinaP: Excellent!

JeffC: just remember... don't trust anything or anybody on the net Lauren... except for me, Bj and Davina!

LisaAK: I have been curious as to how long it would be before Web 2.0 technologies were targeted. People think nothing of putting their entire life on social networking sites, etc.

DavinaP: All the upcoming concerns are very "basic" and impact our students (cell phones/websites file sharing etc...

LaurenKa: How does PC vs. Mac play into this whole game? Does it matter?

JeffC: much fewer Mac attacks... because.. there aren't as many... hackers go after the big game.

LisaAK: There are fewer macs viruses because PCs are easier to hack into....

ShayneTr: What are the potential problems with social networking sites? My students are into Facebook.

JeffC: but like anything... they're vulnerable, especially because newer mac OSX systems allow PC programs to run on them.

DavinaP: PC's have been targeted because more folks use them but there was recently an article that indicated the MAC invasions were on the rise

LisaAK: ID Theft, Shayne -- I think that's the major concern.

DavinaP: Here are top 10 concerns : and then we will walk thru as many as we can in the remaining time with how to step thru links

DavinaP: Limit personal information in email --

JeffC: Facebook and MySpace are notorious for "phishing attacks"... you click on a link in a comment, etc., and then are prompted to "login to do that." ... trouble is... you're logging into a hacker's page who will then have your password, and usually immediately send out spam comments in your name.

DavinaP: 2-Backing Up Files How many here back up files (including email) and how often?

LisaAK: I preach it, but rarely do it!

DavinaP: any others?

ShayneTr: guilty!

LaurenKa: I have a 160GB iPod that backs up my computer

ShayneTr: automatically, Lauren?

LaurenKa: Weekly maybe...

LaurenKa: not automatically...

DavinaP: 3. Passwords strong passwords needed

DavinaP: 4. Watch out for phishing, pharming & social engineering schemes/ recognize a hoax

DavinaP: 5. learn how to Determine if a website is secure

LaurenKa: httpS

ShayneTr: lock icon?

DavinaP: 6. Install/enable email filter & pop up blockers

DavinaP: they are disabled by default

DavinaP: 7. Use/install a firewall and anti virus protection

DavinaP: 8. Use/install Anti-spyware and how to check for spyware-malware-adware 9. Recognize risks in wireless environments

DavinaP: and last...Review your Annual Credit Report

LaurenKa: how often?

LisaAK: Sheriff's office told me every six months is ideal for checking the credit report.....Ideal is the operative word there....

DavinaP: they suggest once per year (credit reports)

LisaAK: That's more realistic, I think.

DavinaP: annualcreditreport.com

LisaAK: I'm sure he told me that since mine had already been stolen.

DavinaP: actually 3 organizations that give out but they all use the same above site...only site you should be using (the sound and look-alikes are all subscription based scam artists)

LaurenKa: FYI...people with more common names seem to have more theft problems...has anyone else heard this?

DavinaP: However...The credit reporting agencies can and will try to sell you things (FICO scores, monitoring, insurance, etc)

DavinaP: You do not need to give anyone your credit card number to obtain your free credit report

DavinaP: Yes Lauren I have heard that

LisaAK: I hadn't heard of this, Lauren, but it makes sense. Mine was a case of the man literally guessing my number....completely random.

DavinaP: Activate your built-in firewall or download/install a firewall for your computer. is another #1 item on your to do list

DavinaP: Prevents unauthorized Internet traffic from entering or leaving your computer.

DavinaP: A firewall helps make you invisible on the Internet and blocks all

communications from unauthorized sources

LaurenKa: can you "undo" the damage you have done if you haven't had a firewall thus far?

DavinaP: here is a great site that walks you thru step by step how to install http://security.getnetwise.org/tools/firewall

ShayneTr: Is there somewhere you trust that rates the firewalls, etc? ZoneAlarm, for example?

LisaAK: Has anyone seen ads for this company called LifeLock?? http://www.lifelock.com/ The man's advertisement (billboards, web, etc.) has his SS# displayed right on it -- claims he can protect you from anything....Just thought it was interesting....

LaurenKa: I know of someone who swears by lifelock...but he dumped last week so he must be an idiot...:)

LisaAK smiles

ChristinaN: I have heard of a commercial on the radio that has a man telling us his social security, I was surprised to hear it on the radio.

DavinaP: I'll have to check it out--the firewall works to block out and somewhat filter out items so things that have already come in are in...responding to up above

DavinaP: Anti-Virus Protection....Detects and removes computer viruses

LaurenKa: thx

LaurenKa: very helpful

LisaAK: That's probably the lifelock company, Christina...

ChristinaN: Yeah, most likely it is

DavinaP: RE: firewalls try the same getnewwise website (part of the federal trade comm) they do have explanations of diff types and links to several

DavinaP: RE antivirus protection...

DavinaP: in a recent study/survey by Mcafee over 50% of the people who thought they had anti virus protection...

DavinaP: did not realize that 1. the "demo version" had expired and 2. that they need to

update for new DAT files DAILY

LisaAK: I'm sure many people do not stay current on their anti-virus software....

DavinaP: Most programs can check every day for new DAT (virus definition-description files)

LisaAK: And sadly, there usually is a new one that needs to be downloaded!

LisaAK: Daily, that is!

DavinaP: how about the group here? how often does your computer scan? update?

JeffC: daily

LaurenKa: whenever I log-in

JeffC: avg

JeffC: free

LisaAK: Every evening (on my office machine) -- I'm much less diligent at home and I should be better about it.

ChristinaN: hMmm well on my laptop, it scans every time I boot it

ShayneTr: I'm using AVG and it updates whenever there is new definitions

ChristinaN: On my parents computer, it does it every morning at 8AM

ShayneTr: also when I open e-mail attachments

DavinaP: excellent! what a great group you are!

ChristinaN: Yeah, I use AVG too on the laptop and my parent's computer

JeffC: avg scans all attachments

DavinaP: Anti-Spam Protection....

DavinaP: Program used to detect unsolicited and unwanted email and prevent those messages from getting to a user's inbox.

ChristinaN: The antivirus protection I hate the most is Norton!

JeffC: gmail is the best for anti-spam

DavinaP: Looks for certain criteria on which it bases judgments

DavinaP: Can use email program, filter or server software

JeffC: I get very few false positives with gmail, almost no spam in my inbox... love it.

ShayneTr: spybot and adaware, both look for different things

DavinaP: Great to know!

LisaAK: Just a general FYI:: Another site everyone may be interested in reading more about later: http://www.educause.edu/security

ChristinaN: I agree with you about Gmail. Gmail is great.

DavinaP: http://www.ftc.gov/bcp/conline/edcams/spam/consumer.htm is a great resource to learn more and see different programs

LaurenKa: Google for life!

BJB2 checks the clock on the wall.

BJB2: The next Cyber3 discussion will be on April 7

ChristinaN: Thanks for the great chat I learned so much!

ShayneTr: Thanks, Davina. I'll be revisiting some of the links once I get my copy of this chat.

LaurenKa: Thanks!

LisaAK: Thanks, Everyone!

ShayneTr: bye

DavinaP: we will pick up where we left off since we did not get thru the 10 items

DavinaP: see everyone then

LisaAK: Bye, Davina -- thank you!