Male 1: Okay. You all have time at the break to go out and delete things off your Facebook pages? Please do. So you all know Facebook and Twitter and Myspace and a couple of others, but that's not all. This is just a small sampling of some of the social media sites that are out there in the world. We're just gonna concentrate right now on this presentation on some of the biggies, Facebook, Twitter, a little bit of Myspace and some LinkedIn.

So first, little background. Social media is also called social networking, web 2.0, just about all of them that was on that previous slide, they all operate the same way. You're a member of an online community. Your key features are your profile that tells all about you and friends, people you want to share all your information with. The most common is still Facebook, it's huge. Twitter is catching up with it, more and more people are starting to use Twitter. Lot of trust going on out there and a lot of sharing.

There was an interview with the CFO of Facebook at Tech Crunch and he said that people are getting more and more comfortable with sharing a lot of information with a lot of people. They're being more open with the information that they're sharing. It's a complete cultural shift and they like it. And it's becoming the norm.

For a security person, that becomes very scary. But social media is a marketers dream. So let's crunch some numbers. 2009 Facebook announced they've surpassed 300 million users. The current number is 500 million and growing. So in just a year they've grown over 200 million users. Twitter, far behind but growing fast, 100 million users. 68 percent of the internet traffic in the world right now is on social media sites and search sites. Facebook, fourth largest website in the world. Grew 157 percent between 2008 and 2009. Almost 2000 percent in the U.S. alone and it's still growing.

Forrester Research says that social media, marketing will grow from $714 million to $3.1 billion in the next 5 years. So what does that make? A prime target. With that growing, attacks are also growing. 240 percent in just phishing attacks alone. So the attacks are on the rise then. As the systems grow, so do the attacks. 70 percent rise in firms accounting for attacks with their social media sites. 57 percent receives spam, 33 percent malware. If you look at the chart, the chart only covers 8 months, but it shows anywhere from a 10 to 20 percent rise.

So what kind of harm can social media do? We'll talk about something we call the Avenue of Distribution. And we'll use a computer worm. Computer worm is a self-replicating nasty piece of malware. After it first gets started by someone, it keeps going by itself using your e-mail, using your internet connections, sometimes it does nothing but simple go around the world, sometimes it carries nasty payloads.

Two internet worms that caused some damage were Blaster and Code Red. Blaster affected 55,000 users in the first 24 hours through the internet and e-mail. Code Red, excuse me, 359,000 in the first 24 hours. Samy, the first social media worm affected over 1 million users actually in the first 20 hours before we shut that. So social media, Avenue of Distribution whole lot bigger.

So what else is out there? Three quarters of the 100 million Twitter registered accounts are either unused or used to distribute malware. There's new easy programs out there for hacking into things such as Facebook. The newest one is called Firesheep. Click and drag, anyone can use it. Steal a lot of information off of Facebook accounts. Twitter, Twitter's had some problems. They had a worm that was posting obscene messages on people's walls. Not a nice thing. The outside of flaw that let people go to other websites, some of them malicious simply by moving your mouse over a link. Facebook had some problems too, they had a glitch that allowed users to log into other users accounts.

So if it's not through criminals out there trying to get you in trouble, it's the systems themselves doing it. So who's number one? Well, we are. Not a good thing. 50,000 web pages hosting malware discovered every day; 34 percent of the new malware and variations of the old malware, over 20 million instances have been discovered in the last 10 months. That's 20 million nasty pieces of software running around out there.

And it's a global problem. We're number one, but there's some people that's gaining on us. But it's because of the way that we're connected, the way the internet's connected that you can't escape it. So, let's look at some real world examples. First, we're gonna start out with scareware. Scareware's that nasty little box that pops up when you go to a website that says your computer is infected with a virus and if you send them $19.95, they'll remove it. Well, sometimes when you click on that box, you don't get anything. Sometimes you get something nasty.

This shows some Twitter Tweets, you click on them, takes you to a web page instead of showing the video you wanted to see. It has a little box pop up. You click on it, you pay them $19.95, the box goes away. You probably never had a virus. But some of it can get really nasty. There's also stuff called ransomware. Does the same thing, the box pops up, doesn't go away; takes over your computer so you've been infected.

Facebook privacy. In the previous presentation they talked about privacy default, your privacy settings. Here's an example, this is kind of the British version of the movie we just saw. The wife of the Chief of the British Secret Service, the head spy in Britain, she set up her Facebook page and posted all the family information and location of the family photos, what was going on. The problem is she left her privacy settings at default so everybody on the London network knew everything about the head spy in Britain. Definite security risk, he wasn't happy.

Fake Tweets. This is pretty normal, that you see these a lot. Famous people, celebrities, people in the news are all gonna start showing up with malicious ware, with spam. Here is a case of the one with the Apple Evangelist 140,000 followers. His account got compromised. Someone put up there, "Here, click on this link. See this sexy video." Well, they figured, "Well, he must think it's a pretty good video so let's click on the link." Well, the problem was it took you to a website that infected your system, your computer, your account. Don't know how many of the 140,000 got infected, but it was pretty nasty.

The next one hits a little closer to home. Justin Timberlake. Someone attacked his account, hacked into it, put a malicious link up, 257,000 people clicked on that link and had their accounts affected, which could have been worse since he has 2.1 million friends, very popular guy.

This one's really scary. This is something that we call the Evil Twin, when someone can take the information out of your profile, create a duplicate account, and then use it for malicious intent. In this case, it was Interpol's Secretary General, the head of the National or International Police Force. Someone duplicated two accounts in his name and started gathering sensitive information on an upcoming investigation that involved 29 countries, 130 arrests. We don't know how many people got away because information was leaked off of those two other sites, but this is not just posting funny things on someone's page. This is actually affecting people's lives.

Okay, story time. Just imagine your 11-year-old daughter or son just saw this come across Facebook, that their hero Justin Bieber hit some girl. Oh my God, so there is no way that their hero could have done something like that so they just have to find out what was going on. So they click on this link. It takes them to a fake Fox news page with a picture of this young lady on it. Well, of course, they think she's absolutely not his type so there must be something going on. So they click on the picture to find out more information. Up pops a little box that ask for account information, passwords, user account information, personal information and permission to access all their accounts. And of course, by now they've gone this far, they've got to find the information out so they say yes to everything. So what they don't get is the information on the young lady. What they do get is their account completely compromised.

And if it happens to be on the home computer, then who knows what's on your computer now. Okay, let's talk about some whats and some whys. The first type of threat is probably one of the simplest because it's user controlled. Individuals take direct actions to do this. It's when personal information is revealed that could have serious repercussions. But it can be deliberate, in other words, someone gets your information and puts it out there. But more than likely it's inadvertent. You set your privacy defaults low, you let them go with everything open and your information got out there.

And as I said before, once its out, you're not going to put the genie back in the bottle. So, by the nature of social media, it's all open, it's all sharing and that's why they set the defaults the way they do. For a security person, you never accept defaults on anything. You always look at it first to make sure it's what you want.

So back in the dark ages when I was younger, the mid 90s, the hackers and the script kiddies, we were all out there just showing what we could do. It was capture the flag, the ego thing, let me show you what I can do, that I'm smarter than you are. Nowadays, it's all financially motivated, completely different. When we were doing it, not that I was ever doing it, but when they were doing it, back in the younger days, you wanted to make sure everybody knew what you were doing. You were defacing the websites. You'd put your name on it and everybody knew what was going on.

Now that's not the case. The criminals don't want you to know that they just stole your information because there's too much money involved and completely different mindset out there.

So social media, it's valuable to hackers; 500 plus million users out there and $3.1 billion dollars, kind of a no-brainer what they're gonna go after. And they could use social media for almost anything, destroying information, destroying identities, and stealing.

So what's the bottom line? What's the end goal? They want to steal your data because personal information, your personal data equals money. Whether it's stealing your Social Security Number, or your credit cards, or buying things in your name, or stealing your whole identity, that's their bottom line.

Okay, story time. January 2009, gentleman named Bryan Rutberg had his Facebook account hacked. And it was compromised. Well, someone posted up on his wall that he was in Europe. Someone stole his wallet, he needed money, wire it to this address. Well, one of his friends did to the tune of $1,200.00. Another one, a little while later, $600.00. That person got an e-mail from the criminal saying that the $600.00 wasn't enough, he needed more so the friend wired another $600.00. While this was going on, Bryan knew what was happening. His daughter had told him that someone had hacked into his page. Tried to get a hold of Facebook, no joy.

Decided well, he'd go to his wife's account and use his wife's account to get into his account so he could fix it. The problem was criminals had thought of that too, so took his wife off the friend's list so he had no more access into it. Also, changed the password and the user name so he couldn't log back into it; took him 40 hours before it was finally straightened out. A lot of e-mails, a lot of phone calls to friends to try to straighten this out. Luckily it didn't cost him a lot of money, but it cost him enough and his reputation. So nasty things can happen.

All right, three major threats: spam, phishing, malware. Spam, unwanted e-mails, unwanted Tweets, kind of like the digital junk mail. Phishing, phishing is trying to trick someone into giving up your personal information. And, of course, malware is the nasty stuff. That's the viruses, the spam, the Trojans, all the things that can really hurt.

So let's talk about spam first. Okay, here's a nice little Tweet, said, "Get a $500.00 Victoria's Secret card. Just click on the link." The problem is when you click on the link, what you get is a site from the crazy internet multimillionaire talking about how you can get rich quick. And he's not even wearing Victoria's Secret lingerie so.

Next one here, it's another one. This one offered a job at Google. And instead sent you to a fairly decent looking newspaper that's got some really dodgy links on it and asking for money, but they're gonna get you a job at Google, never fear.

Another one, this one's from Facebook, little spam. The account's been compromised and someone posted on the wall that the victim got where he is today by using the dodgy pharmaceutics that they're selling and if they'll click on this link to buy some pills, they can be just like him.

That's what happens when your account gets compromised. You don't know what's going to wind up on your wall, just like poor Bryan.

Look at the numbers, 57 percent of social media users report they were hit by spam by just dug four, that's an increase of over 70 percent in just a year. Now I read an article yesterday that said spam has, in the last two months, has actually declined. But they also say that with the holiday season coming up, they expect it to catch up real quick.

Okay, phishing. This is my favorite because the criminals get really creative with this. It's always nice to see – you remember the old days with the e-mail, the Nigerian e-mail that promised if you help out the widow of the Finance Minister, hide her $60 million dollars in your bank account, then she'll give you a percent of it and just send your bank account number to Nigeria.

Yeah, well they've gotten a lot more sophisticated than that. Here's one. They were trolling the web saying, "Hey, check out this guy. Click on this link." And when you do, you go to the Twitter login page. Well, maybe not. What you go to is tvvitter.com Now with my old eyes, those two v's put together look like a w so I probably would have fallen for this. But when you log in, you give them your password, you give them your user account and some of these are so good, I haven't tried this one, but some of them are so good that they would actually log you into

Twitter after they steal all your information. Then you get to go to Twitter and do whatever you wanted to do.

And in the meantime, like I said, they hide what they're doing so you don't know that you've just given everything up until something bad happens to your Twitter account. Another phishing, this one's another fake site. This one's for Facebook. Two new ones that are floating around out there is Win an iPhone. All you've got to do is take a little quiz, give them your cell phone number, and instead of wining an iPhone, you just signed up for $10.00 a week cell phone service from some company overseas that's almost impossible to get rid of.

Another one, my favorite is that you'll get a free $1,000.00 Best Buy card for first $20,000.00 users that log into the Best Buy fan site; so when you get there and fill it out, give them all your credentials and everything, you don't get a card, but you get a lot of other stuff like viruses and Trojans and keyloggers. They're getting good. I like this one because it's a very, very sophisticated phony site. When there's that much money, $3.1 billion dollars involved, it's not a cheap little misspelled e-mails that we used to see. They're paying big money to build really nice sites. This one's got a quiz on it, it's got surveys, it's got links to other decent sites. It still steals your information and does nasty things to your computer, but it's very well done. You know?

They put a lot of money into this because they expect to get a return on it and they do. And that's why it's getting more and more difficulty to actually catch them and be able to differentiate between the really bad sites and the decent ones. So phishing, 30 percent of users report phishing attacks. Yeah, those sites up almost 43 percent in a year.

Malware, this the nasty stuff. These are the Trojans, these are the worms, things that destroy your computer, things that steal information off of your computer, just because your account in Facebook got hacked and downloaded some nasty stuff doesn't mean your Facebook account was messed up. It got onto your computer where you stored your Quicken, where you stored all your passwords to your bank accounts, where you stored your bank account numbers. That's what they're looking for. They could care less how many friends you have, unless they can trick your friends into doing things.

They want the information off of your systems. Too phony sites, always promising something, the new videos and the sexy videos

are always the big draws so that and when celebrities are in the news. Sarah Palin, George Bush. When the stimulus checks went out, phishing, spam, fake sites offering to help you spend all your stimulus money popped up everywhere. So you can watch the news, whatever's going to be big in the news, that's what we start looking at for the new malware, the new Trojans, the new attacks because whether it's the hurricane in some place, whether it's an earthquake in Haiti, whatever it is, there's going to be some fake site whether it says Red Cross, put the money here or something. There's somebody out there trying to steal.

This one's kind of a combination too and that's – this is an e-mail that directed you to a phony Facebook site that promised another sexy video. But what you actually got was infected with a Trojan. This kind of scares me. If you read the previous presentation, they were talking about the newest Facebook e-mail that's gonna combine chat and e-mail and everything all together into one big bundle. That's like taking all the bad stuff and putting it in one place so. Hopefully, they'll get good security on it, but it's bad enough we've got e-mail over here doing linked in with Facebook doing bad things. Now we're gonna put it all in one spot into a whole lot of bad stuff so.

I'm gonna reserve judgment until I actually see it in operation. Now this one. This is a good one. Click on the link to get a funny picture. Well, the funny picture is a malware called Koobface, which is an anagram for Facebook, by the way. I just read that this morning. Koobface is a very sophisticated system. When you get infected, it can actually create bogus accounts on Facebook without your knowledge. It will actually validate those Facebook's using gmail. It'll go out and randomly select friends to add to those Facebook pages and then it'll start sending them things like get rich quick schemes or malware. And if you think all you Mac users and smartphone Android users out there are safe, Koobface has been ported to Mac. Android has its own Trojans. There's no safe system out there.

We used to say, "Can't hack the Mac." Well, yeah, you can and they are. So what now? Scared yet? Let's say you should be cautious. So what can we do to stay secure? Number one, know the rules of your organization. Your university web pages, your university media pages, know what you're allowed to put up there, what you're not allowed to put up there. If you don't have a policy, if you don't have a good plan in place for setting up social media sites, you need to get one. You need to think this through.

This is not a matter of just let's hook it up there and run it default. This will not work.

Use secure passwords, and change them often. A lot of this, you know, is geared towards organizations, a lot of this is geared towards presentations, geared towards your person, your children's stuff, children sites, but it all makes good sense. Default settings, like I said, they want us to share information. They want us to be open; default settings, everything's open. Think twice about your friends' setting, your friends' of friends' setting, your everyone's setting. What's in this? What are you giving out? What should be given out?

Think before you post embarrassing pictures or information. Recruiters are starting to do searches on social media sites to pair them up with resumes. And I think if you were at the last presentation, Susan actually talked about Department of Education did refuse employment to someone because of something that was on their social media site. So it's kind of like my mom used to tell me about tattoos. Even though I was in the Navy, I didn't get a tattoo so.

Consider everybody's watching you because they are. The hackers are out there trolling for information on you. Also, we talked about the evil twin, somebody setting up a website or setting up a profile with your name. Go out there and do a search on your name on Facebook. Make sure you don't have an evil twin sitting out there raking in millions of dollars in your name or doing something else. Do the same thing on all your accounts. Check and make sure that you're the only one. It's too easy. I can step you through how to set up the bogus accounts, how to set up - it's – there's just not enough checks and balances on some of the social media systems to keep this from happening.

Use good computer security, anti-viruses, firewalls, anti-spamware and for goodness sake, don't do social media on the same computer that you're doing your online banking. $385.00 Walmart laptop dedicated simply to doing online banking or social media will save you thousands of dollars in stolen money and months and months of headache. So consider separating the two, at least those two. And think before you click. Just use common sense. You don't really need to see too many sexy videos and yeah. I don't think Best Buy's going to give away a $1,000.00 card, not to 20,000 people. So some of it is a little shaky. We all get taken occasionally, but that happens. There's an old saying when we talk about risk, "You can ignore the risk." Not a good thing to do.

"You can accept the risk," because there's not a whole lot you can do about it. "You can mitigate the risk or fix the vulnerability," which is a good thing. And that's getting a different computer and things like that. "And you can transfer the risk." And that's what I do. I have insurance on everything so steal my identity, I make money off of it and so think about things like that. There's a lot of companies out there that do sell identity theft insurance. It's becoming probably one of the biggest problems in computer security right now is identity theft and it can take years to get it cleaned up and a lot of money. And if the insurance is cheap, not that I'm selling insurance.

I love this quote. This is from the former FBI Chief Information Officer, he said, "I think this level of awareness in communication needs to start in elementary school because I'd like to say everyone is armed today. Everyone you see has a cell phone, and very cell phone has an IP address and every device with an IP address is a point of entry or intrusion into our network because we're so well-connected, we communicate so well with each other so therefore we need to start education as early as possible."

So I've added some helpful links, Federal Trade Commission, very good website, talks about social media, but also different types of online, internet; very, very good site, big on identity theft, prevention. You can report fraud, you can report identity theft to them. They have a lot of good links with the FBI, with other agencies. Microsoft also has some good security information up on their website. Sofas excellent, a lot of this presentation came from their tool kit.

The next one is an e-book by Linda McCarthy, *Own Your Space: Keep Yourself and Your Stuff Safe Online*. It's a digital book for teens by Microsoft, it is excellent. If you have children, I highly, highly recommend that you go out, download this and give it to them to read. *Consumer Reports*, also another one talking about the different cyber security information that needs to be done. Staysafeonline.org, excellent site. Also talks about how to prevent a lot of the issues, not just with social media, but with your whole online experience. Some references, like I said the social media tool kit. If you really want to get under the hood and understand how some of these things happen, the next one, the *Seven Deadliest Social Networking Attacks*, excellent book. There's a whole series of these *Seven Deadliest Attacks* on web networks. But this one goes through these attacks and explains exactly how they happen, how it could happen and what to do about them.

Social Networking spaces gives you a lot of background on the history. Architecture, Homeland Security, *Daily Cyber Security Report*. Most university's governments, they can get this simply by getting an RSS feed or they can sign up for this. Security awareness course and a lot of the different security websites, like Security Computing News and others, they have excellent RSS feeds, they have excellent online magazines. They talk about different aspects of social media. They talk about the web, online experience, some of the latest hacks that are going on, some of the latest threats. Excellent background reading. Some of it is kind of over my head, but – so in summary, I love this picture of the iceberg because it really shows that there's a lot below the surface that we don't even know and it's growing.

The risks are real. They're out there. We see them every day. We try to mitigate or fix them every day. The criminals are basically out there to steal your information cause information is money to them. It's how they're making their living. The security controls in the social media sites are getting better, Facebook, Twitter, all of them are really improving, but you have to understand them. You have to understand what those privacy defaults mean, understand how to set the controls, understand what you need to release and what you don't want to release. As they said before, "If you don't want your grandmother to see it, better not put it up online."

And you can control a lot of the risk yourself. Think about what you're doing. Thank about if you really need to do that, do you really need to put all that information up there? Spend some time to double-check your account. I mean, you double-check your check book, so double-check your Facebook account because it can steal money just as easily as you can write the wrong number in your checkbook and be overdrawn.

I went to a conference and a security professional said, "With the current situation, we cannot afford to use social media, but also we can't afford not to." So use it, share it, enjoy it, make some honest money with it, but most of all, stay safe. And we appreciate your feedback and there's my contact information. So any questions? Okay, thank you.

[End of Audio]