

Susan: Hello and welcome to Tech Talk from the University of Minnesota. I'm your host Susan McKinnell. Technology is all around us and it's a challenge to keep up. This program is designed to give you an insight into the technology we use every day. Today, we're discussing the privacy and security of computer systems. Some of the terms you'll hear today include "firewall," "patching" and "https." Issues about privacy and security seem to be in the news frequently these days. To help us understand some of the legal ramifications of these issues, we decided to talk to the University's lawyer. Mark Rotenberg is the General Counsel for the University of Minnesota. Previously he was a partner in a Minneapolis law firm and before that he served as an attorney in the justice department's office of legal council in Washington, D.C. He has also argued cases for the U.S. Supreme Court, the Minnesota Supreme Court and others. Mark, it's good to have you here.

Mark: Thank you, Susan. It's nice to be here.

Susan: Now can you tell me what is important about computer security?

Mark: Well, the basic problem we have today is that when you get on your computer at home, you are entering a stream that accesses your information on a world-wide basis and that's never really happened before in human history, where you can be sitting in your own tent, your own house, your office and be part of an international, world-wide information stream. So you're not sure, when you are doing your work, who is accessing information about you.

Susan: Mm. Hmm. What sort of information should I be concerned about people accessing about me?

Mark: Well, the basic kind of information is personally-identifying data [for example] your name, your birthdate, your social security number, your address, your email address, your telephone number, your credit card information, things like that, that enable others to learn about who you are and acquire or even steal your identity.

Susan: Mm. Hmm. Now if someone were to steal my identity, what sort of legal recourse would I have?

Mark: Well, that's a complicated subject because this is "new school" and the law does not develop as fast as technology does. Legislatures, congress, the courts are slow-moving, democratically-oriented operations and they don't respond like a machine would to a response from the outside. So, the law has developed some mechanisms to deal with the problem, but they're not very quick. The real answer to identity theft is preventive measures: not putting out there too much information about yourself.

Susan: Mm. Hmm. Absolutely. One other question about identity theft: Would I be responsible for what someone did using my identity?

Mark: Generally not, Susan. The law blames or holds accountable the actor who engages in the misconduct. So if someone steals your identity, say uses your credit card to purchase all kinds of things on eBay, you're going to end up being accountable for it only at the front end. In other words, your credit card account will show some debits. You are going to then have to take some responsibility to call up and say, "This is a fraudulent purchase." And then normally it's the person who engaged in the theft or the fraud that's accountable, ultimately. Again, that's a criminal law process. There is no sure bet here.

Susan: Okay. So, being preventative in the first place is the best aspect. Is there anything else I need to worry about other than identity things? Are there other things I should be secure with on my computer?

Mark: Well, in working on your computer there are many different things that take place. There are purchases, there is research, there is your own intellectual property, if you are working on poetry, if you are writing an exam paper, if you're developing a research model, if you're doing surveys, there may be unique things that you have on your hard drive. Or that you send by email or other ways that you send to other individuals or businesses and there are people out there who are looking for that stuff and not everyone is searching the web for innocent purposes.

Susan: So, anything that is valuable to me that also might be valuable to someone else is something I should be careful with?

Mark: You need to make sure that your hard drive and your internet provider have the kind of firewall protections; the kind of security that you need for the kind of work you're doing on your computer.

Susan: Okay. Now, what sorts of laws govern the distribution of the information about me that I may give to my internet service provider?

Mark: Well, in the last few years, the federal government and the State of Minnesota have enacted statutes that regulate the kinds of information that businesses can give about you to others. Health care information, for example, is very carefully guarded under a new federal statute called HIPAA. But there are other internet and information-related statutes and regulations that have been put into place just in the last few years by the federal government and the state government. They're complicated. They haven't been fully worked out. They are kind of like the Web used to be, say, ten years ago. The law is just beginning to deal with this sensitive area. But generally speaking, Susan, these laws, strictly regulate the amount of data—personally identifying data—that a business can give to a third party about you.

Susan: So, if I have an internet service provider; they've got information about me; they really can't give that information to someone else?

Mark: Without your consent, generally speaking, under the new laws. And that's why you see when you are browsing and you are into various different sites all kinds of questions.

Susan: I see those all the time.

Mark: Like click here and you'll be able to get all kinds of other data. That typically means that you are giving your consent to the location that you are on, to provide it to other third parties.

Susan: Absolutely. And you I've got my internet service provider, which hopefully is somewhat reliable, but then there are all of these sites that have their own security policies. How reliable are those? Are they under the same legal jurisdiction as...

Mark: Internet Service Providers are limited in terms of the information they can give and the business sites that you'll be on are also regulated. There is another layer of concern about privacy, too. That is your business computer. You are at your work place, your employer might have given you a computer to use. That employer may also be limited in terms of the information they can give others, but more importantly for your purpose, they may be sharing information about you inside the company. And that's what you need to be concerned about. What is your employer's policy about disseminating information within your workplace about you? Are you spending an hour looking at this website? Are you spending more time than you should on the internet? Are you spending too much time emailing family members and so on.

Susan: Now, since it's the computer of the employer, they have every right to look at the hard drive, to track what sites I go to, and so forth as long as I am using their computer and their internet connection. Is that correct?

Mark: Generally speaking, Susan, the private employers have the right to monitor what you're doing on their equipment, and their hard drives. Government employers are more limited in what they can do. Minnesota law has a privacy component to it. There is a common law of privacy in Minnesota. Again, the shape of that right, the contours of that right in the context that we're talking about now, the internet, is unclear. The courts in Minnesota have not definitively fleshed out how much privacy you have, as against your employer, when you are surfing during business hours, even not on business hours, but using the employer's hardware.

Susan: Mm. Hmm. General Council Rotenberg, Mark, thank you very much for being here with us today.

Mark: It's nice to be here with you, Susan.

Susan: As we were preparing this program we wanted to discover, not only the legal aspects of privacy, but we wanted to learn how to secure that privacy. To do that, we

asked Ken Hanna to stop by. He's the director of Security and Assurance for the U of M's Office of Information Technology. Ken, nice to have you with us today.

Ken: Thank you for having me.

Susan: Ken is director of Security and Assurance not just for the Twin Cities campus, but for the Crookston, Morris, and Duluth campuses as well and all of their various computer systems. Ken, can we start off with, "How can I keep my computer secure?"

Ken: Sure. I think the first thing to do is probably start to think about what kinds of information that you want to protect on the computer. For example, if you are a home user, you may have your tax return or something like that on there. That would be something that you want to protect or if you have a small home business, maybe something in that realm. So, you want to think a little bit about what is at risk. So, that would be the place to start. And then after that, I think you'd start thinking about, "What can I do that's pretty easy, if I don't have much information to protect, if I've got a bit more, I can do some other things."

Susan: What are some basic things I can do? I hear a lot about firewalls.

Ken: Yeah. That's one thing. I think that's probably more if you have a cable modem, a high-speed access or if you've got some really important information. It's something a home user could do, but I think I'd start with, sort of, the basics. The first thing, probably, is just to back up your information. If you've got tax returns or if you've got word processing documents or you've got things like that, you want to make sure and save those somewhere off the computer.

Susan: So, I that don't lose them?

Ken: Right. And that's the first thing that most people kind of put off and don't do. So that's the first thing, I always say, is to do that. After that, I think probably the anti-virus program is the most important thing. Nowadays, there are just an awful lot of viruses and worms and things like that going around. And you really can't tell so you really need something to protect yourself. So, you really need to do that, I think probably, first. After that I think probably, there are some other things you can do. You want to update your software. There are sometimes problems or bugs in software and you want to be able to update that.

Susan: And we're talking about the operating system here? Windows, or if you have a Macintosh Operating system?

Ken: Yes. Windows or Macintosh or something like that.

Susan: I see all the time little balloons telling me to update.

Ken: Yeah, sometimes you can do that, it depends on how the manufacturer set up your computer sometimes you'll get reminders, sometimes you won't, but it's pretty easy to do. It's very easy to do nowadays, really. You just need to find something called "Windows Update" in a Windows computer and I believe it's called "Software Update" on the Macintosh.

Susan: Could we take a look at it. We've got a Windows machine here. I know it's usually under the programs under the Start Menu, and you've brought it out to make it a little easier.

Ken: Right. Usually you'd go to the start menu, down in here, but we've brought it to the desktop. It'll just be the same thing. And so, if you click on this Windows Update, you'll get a screen and it look just about like this.

Susan: Is this taking you right to the Microsoft website?

Ken: Yes. This Microsoft [website] is the home for the Windows update. And it's going to take a look now, when I click on that. It's going to take a look at this computer and say how many patches or fixes and I see on this computer, we've got a lot. We've got critical updates, we've got 19 of them that aren't done. Some of the other things down here that are sort of optional and so those are things you sort of want to look at, you may not want to do those, but these critical updates and service packs? These are the security sorts of updates and fixes for the computer.

Susan: So they've improved the product so that my computer will be more secure?

Ken: Right. And this is a key component that is easy to forget. So whether you get reminded or don't get reminded, that's something that you really want to do.

Susan: If you don't get reminded, or even if you do, how frequently does this need to happen?

Ken: Well, they are issued periodically. I think, if you can do it, it doesn't take very long, so if you can do it every couple of weeks, it would be probably good. I mean, if you really want to do it you can check it every couple of days if you want to. It just takes a few minutes, but I know people are busy so, you know, if you can do it every week or two that's good. But you don't want to leave it to the point where you have 19 updates or something like that.

Susan: This one's not really very secure. Is it?

Ken: No. No.

Susan: Okay.

Ken: So, you want to keep up on those. And that's very important. So, if you have an anti virus and you keep the software up to date and you've backed up, then you start getting to the point of doing some other things. One easy thing is to turn the computer off if you are on a cable modem or a high-speed network of some sort. Turn it off at night, for example. When you're not using it rather than leaving it on.

Susan: Yes. I see people leaving their computers on all the time. I mean, they are connected all the time, so why not leave them on all the time?

Ken: Well, it's good security practice and it really does help. We see a fair number of systems that have problems within the University and many times, those are computer that have been left on. So, if they are left on over the weekend, or somebody goes on vacation, then there is no one really watching the computers. So, it really is a good practice.

Susan: So, really it's like leaving your house unlocked when you go on vacation?

Ken: Right. Something like that, yes.

Susan: Mm. Hmm. And that's an easy, cheap solution.

Ken: Yeah. It's probably one of the cheapest there is.

Susan: I like those. Now, firewalls may not be so necessary for basic users, basic home users depending on what they need to protect. If someone does want to look into firewalls, what are the issues there?

Ken: Well, if they use dial-up access, in other words, they use a modem, a regular telephone line, then I think it would be good if they put a software firewall in, but it's not quite as important as if they've got cable modem or high-speed access.

Susan: Like DSL?

Ken: Yes. DSL or if they are at work and they have high-speed access. So, the software firewalls are good products, there are quite a few of them, I think that Symantec makes the Norton brand one. The one I particularly like is called Zone Alarm from I believe it's called zonelabs.com and that one is a good one. It's pretty easy to use. Zonelabs has a free version for home and personal use.

Susan: Great.

Ken: You can't use it for business, but for home use you can use that.

Susan: So, what exactly does a firewall do?

Ken: Well, it sort of shuts off some of the ports in the machine. There are about 65,000 entry points into the machine in the software and it shuts off some of those things that you don't use. So what it does is just sort of screen off some of the material coming into your machine that is probably not good.

Susan: Okay.

Ken: So, it's quite helpful and a good protection.

Susan: Okay.

Ken: So, I think that fits into securing the machine, but it's probably not the first thing I'd do. After I get the other things we talked about.

Susan: Get the other things taken care of first. Viruses are a big issue. What about passwords?

Ken: Well, passwords are always something that everybody hates, I guess.

Susan: Mm. Hmm.

Ken: It's sort of a necessary evil.

Susan: I've got far too many of them.

Ken: Right. Right. And everybody has a lot of them nowadays. So, what you want to do is just make sure that those passwords that you have that are real important, your bank connection, maybe or, the ones that you use for work, things like that, make sure that you use complex passwords. By that I mean, passwords that have numbers, they have letters and if the system allows, even special characters such as a question mark or any of those in the upper row of the keyboard.

Susan: Okay.

Ken: So it's a necessary evil but you really do need to pay attention to those sorts of things.

Susan: And then you don't want to use the same password multiple times.

Ken: Yes. If you've got your bank account, you probably want to have a unique account for that and you want to have a unique password for that. And if you've got some of them for accessing a newspaper, I know New York Times and some of the places like that. Well, you may decide that you don't really consider that to be the most important password that you have so some of those you may not have quite as hard a password.

Susan: Now, talking about banking online. That's secure?

Ken: Well, we certainly hope it is.

Susan: (laughs)

Ken: Because I use it too. I think for the most part it is. You do have to pay attention to the password, because the password is the one that's protecting your account.

Susan: What about things like shopping online?

Ken: Well, shopping online for the most part, I think, is quite secure, but you've got to pay attention. There are people, just like anything else in this world, there are people that are doing things that are wrong or illegal or whatever. And so you just need to use common sense there. You wouldn't necessarily buy an expensive item in a back alley someplace and so you have got to kind of look for cues that sort of determine that this is a back alley on the internet. And it's hard to tell sometimes. So a couple of things that I look for is, first of all, you want to make sure that the lock symbol on your web browser is there. That indicates that they are using a secure means of communication. And the other thing is up there in the address bar, you can look for "https" with the "s" on the end of it and that stands for secure. And that provides some assurance that they're using the right protocols. But other than that, it's common sense. If there's not a telephone number or address for this business, you kind of wonder if somebody didn't make it up just to try to take money from people.

Susan: So you want to go to someplace that you feel is a regular establishment.

Ken: Right. You want to kind of stick to things that are brick and mortar businesses. Is the term, I guess.

Susan: Sounds good. Thank you so much for being with us today, Ken.

Ken: Thank you.

Susan: With all of the information we have given you so far, one item is still missing. Who wants the information on our computers? The question of who wanted our computer information led us to Tracy Smith, a U of M lawyer specializing in employment law and public records.

Tracy: There are two broad categories of people, I can imagine, wanting to look at people's privacy with respect to their electronic communications: your employer and the government. Employers who provide the computer system to their employees for their use, can access either the email or intercept the email if they choose to do so. That's an exception that is under the communications privacy act. They can also, of course, access the information with the consent of the employees and if an employer has a policy that gives employees notice that they're going to be monitoring their email, and the employees continue to use the email, the employees are deemed to have consented to that because they know about it. So, employers can, without violating statutory law, pretty

much, monitor their employee's electronic communication. The other things that employers have to keep in mind are whether they are violating either common law or constitutional law if they are public employers. With respect to the common law, there is a common law tort of invasion of privacy where any person can sue any other person who invades their privacy in a way that is violative of the law. And also for public employers, public employers cannot violate the 4th Amendment rights of employees unreasonably searching and seizing anything even in their workplace. The key to both of those things though is reasonable expectation of privacy

Text Appears: But why government?

Tracy: Oh! There are all sorts of reasons that the government might want electronic information. You know, like just routine financial crime, financial fraud, that might use computers. They might want it again for you know crimes like child pornography that are conducted via computers. They might want it, of course, for terrorism or foreign intelligence purposes, for investigations related those purposes. For computer hacking itself. You know, I mean that in itself is an enormous crime that costs untold amounts of money for service providers. So, just computer crime itself is something that needs to be investigated.

Text Appears: Has the Patriot Act made government access to private information easier?

Tracy: The U.S.A Patriot Act is a law that passed shortly after 9/11 in 2001 that amends a number of laws. It's a very complex statute. It amends a number of laws including laws that govern criminal investigative access to information and foreign intelligence access to computer information. Basically, what the USA Patriot Act does is amend a number of laws to change or reduce the standards for government to get access to information and that in some cases also reduces or changes the level of judicial supervision over government. The laws generally regulate how government can access information about us but in terms of how other private entities access information about us, that's not a fully regulated area.

Susan: Surprising isn't it? We've tried to cover as many of the security and privacy issues as we could in this past half hour which makes for the inclusion of some significant items for your files...

For Your Files

University General Council, Mark Rotenburg, suggested ways to negate identity theft.

Mark: The real answer to identity theft is preventive measures. Not putting out there too much information about yourself.

Susan: Mm. Hmm. Absolutely. One other question about identity theft: Would I be responsible for what someone did using my identity?

Mark: Generally not, Susan. The law blames or holds accountable the actor who engages in the misconduct.

Susan: To keep your computer secure, Ken Hanna suggested: back up your files, install antivirus programs, turn off your computer when not in use and use firewalls.

Susan: So, what exactly does a firewall do?

Ken: Well, it sort of shuts off some of the ports in the machine. There are about 65,000 entry points into the machine in the software and it shuts off some of those things that you don't use. So what it does is just sort of screen off some of the material coming into your machine that is probably not good.

Susan: Ken also described some of the elements of a safe and secure password.

Ken: Make sure that you use complex passwords. By that I mean, passwords that have numbers, they have letters and if the system allows, even special characters such as a question mark or any of the ones in the upper row of the keyboard.

And attorney Tracy Smith said that if you use your computer at work, remember this

Tracy: Employers who provide the computer system to their employees for their use can access either the email or can intercept the email if they choose to do so. That's an exception that is under the electronic communications privacy act. They can also, of course, access the information with the consent of the employees and if an employer has a policy that gives employees notice that they're going to be monitoring their email, and the employees continue to use the email, the employees are deemed to have consented to that because they know about it. So, employers can, without violating statutory law, pretty much, monitor their employee's electronic communications.

We've got one more reminder which is particularly topical in light of the mid-August outbreak of the Blaster and Welchia worms, as well as the Sobig virus. As Ken said, have a good, up-to-date antivirus program, and make sure to check for critical updates to your Windows or Macintosh operating system. Blaster and Welchia, which infected hundreds of thousands of computers worldwide and slowed networks to a crawl, both took advantage of security bugs in Windows. Microsoft actually released a patch for the bug that Blaster used weeks in advance of the worm's outbreak. Folks who, as Ken suggests, were checking for updates every few weeks should have had ample time to protect themselves from this time-draining worm. All the major anti-virus software companies had fixes shortly after the worms' releases. And running a firewall also provided some protection from both of these worms.

SoBig was slightly different--masquerading as a benign email attachment, this virus spread itself in a method similar to the Melissa and Lovebug viruses of a few years ago. The For-Your-Files message with this one is once again, be super cautious of

attachments, and update your antivirus program at least weekly, and right away if you hear of something going around in the news.

Susan: Next week, Minnesota commissioner of Education, Sherry Pierson-Yekke joins us to talk about education via the computer. Learning online. But be advised: learning online is not just for kids it's a lot more than Reading wRiting and aRithmetic on the next edition of TechTalk.

For more information about this and future Tech Talk episodes check out our website. The address is www.techtalk.umn.edu. And until next time, I'm Susan McKinnell.

Tech Talk is produced by Academic and Distributed Computing Services and the Digital Media Center, Office of Information Technology in cooperation with Learning Technologies, College of Continuing Education and University Relations, University of Minnesota.

Executive Produces

Robert H. Bruininks

Special thanks to

Steve Cawley

Sandra Gardebring

Mary Nichols

Shih-Pau Yen

Host

Susan McKinnell

Producer/Director

Susan J. Tade

Associate Producer

J.B. Eckert

Assistant Director

Paul Pecilunas

Technical Director

Steve Barbo

Audio

Nicole Wilson

Lighting Design

Paul Pecilunas

Laura Cervin

Set Design

Richard Stachow

Field Producer

J.B. Eckert

Floor Director

Bob Hanson

Cameras

Laura Cervin

David Lindeman

Jonathan Kranzler

Teleprompter

Jay Hopkins

Still Photographer

Nancy G. Johnson

Make up

Sharon Davis

Ms. McKinnel's wardrobe provided by: Herbergers

Graphic Design

Nicky Torkzadeh

Effects Design

Paul Pecilunas

Web Development Team

Christina Goodland

Lance Cunningham

Ann Valenty

Thanks to:

CLA Studio B

NASA

Radio K

Bakken Library & Museum

KSTP Meteorology Department

Pavek Museum Broadcasting

Antique Telephone Collectors Association

©2003 University of Minnesota

