

Tech Talk TV Show

Identity Theft Episode

1/23/05

The text on the screen reads Digital Media Center, University of Minnesota
Bagels pop out of a toaster. A couple is at the breakfast table. The phone rings and the man says, "I'll get it."

Text at the bottom of the screen says, "Patterson home 8:15 a.m., present day."

He answers the phone saying, "Hello? Hey Joyce! Any word yet? What? I don't understand; what credit cards?"

The man turns to his wife and says, "Do you have any credit cards that we don't know about?"

The woman replies, incredulously, "No."

The man continues on the phone, "But we never even got a past due notice. Maryland? No. There has to be some sort of mistake. We don't even live there. Can we get a copy of the credit report or what? That's not our address. Well, who should I talk to? Look, I understand, but. And the bank ... What about the loan?"

The woman mouths questions to the man.

The man continues on the phone, "All right. Okay. Thanks for calling."

The woman says, "Well, what did she say?"

The man says, "They apparently can't approve the loan for the new house. They said that we've got three delinquent credit card accounts."

The woman says, "Well, that's impossible. We only have the... "

The man interrupts, "It's not even our address. They're billed to an address in Maryland."

The woman asks, "Maryland?"

The man says, "I know! It's crazy."

The woman says, "What about the house?"

The Tech Talk Intro plays.

Susan: Hello and welcome to Tech Talk from the University of Minnesota; your source of information about the technology that surrounds us every day. I'm your host, Susan McKinnell. In today's program you're going to find out what to do if what happened at the beginning of this show happens to you. We'll tell you how to secure yourself, who to go to for help and what the government is doing about it. It's a serious issue, I'm glad you're here with us. Some of the terms you'll hear include *phishing*, *patches* and *firewall*. Joining us today to discuss securing your identity is Mark Powell. He is the director of OIT data security which is responsible for the security design and management of data access and systems security for enterprise systems at the University of Minnesota. Thank you for being here today, Mark.

Mark: Thank you for inviting me.

Susan: What exactly is identity theft?

Mark: Identity theft is when someone is stealing information; your personal information without your consent; without your knowledge and pretending to be you. They're taking information from you in terms of, you know, taking your social security number, your driver's license number, your name and address, your date of birth and they're...I'm sorry.

Susan: No, that's fine. Other than the kind of "icky" factor of them pretending to me, what else is wrong with that?

Mark: Well, they can tap into your existing credit card accounts, and run up big bills. They can open up additional accounts under your good name and your good credit.

Susan: Which may not be good for much longer?

Mark: They can also do loans; they can even apply for jobs using your social security number.

Susan: How is most of identity theft happening these days? How do people steal that information?

Mark: Well, it's been around for a long time, I mean people have been stealing wallets for a long time, but since we're doing so many things online now, we do so many purchases online, we even do banking online.

Susan: Absolutely.

Mark: It's become a higher risk.

Susan: Okay. I know that it's been increasing exponentially recently, is there any reason other than the fact that we do so much online. Is there anything in particular online that is contributing to that?

Mark: Well, there is a thing called phishing that's spelled p-h-i-s-h-i-n-g and it's a scam where someone will send you an email and pretend to be from your bank or from another prominent company and try to get you to click on their url which looks right, they use the company logos, everything looks normal but it's really a scam. It's really going to some other computer website and then they try to encourage you to provide all of your private information; your account numbers, your mother's maiden name, all your passwords and then they kind of got you.

Susan: Well, we've got an example of this right here, don't we? It looks like something now what website this is the antiphishing.org

Mark: anitphishing.org

Susan: And this is something that looks like an email that came from PayPal.

Mark: Right.

Susan: A lot of people use PayPal these days.

Mark: Yep. Yes. If you do stuff on ebay.

Susan: By gosh! This looks like something that's really real. It has the PayPal logo, it has this lovely information about how to keep your account secure, but this whole thing is false isn't it?

Mark: It's a scam.

Susan: Mm.Hmm. If you click on the link, the link looks like the link is actually going to the web address of this link says that it is going to PayPal.com but it's probably going somewhere completely different.

Mark: Yeah. It is going somewhere else.

Susan: What's the rule of thumb then, with this? How am I supposed to know if it's really PayPal or not that is really contacting me?

Mark: Well, the rule of thumb is "be aware of it" and just ignore it. PayPal would never send you a letter and say, you know, without personal information about you in it. It's kind of a generic letter that's coming to you through email and most companies won't ever ask you for that information online so, the best advice is to just delete it. If you really think that you need to talk to PayPal, you can go directly to their website

Susan: Put in their address yourself.

Mark: Or pick up a telephone and call them.

Susan: So the rule of thumb is, "If they're asking for the information, if they're initiating the contact, it's the same thing as with the telephone. If you've got someone calling you saying, "Hey I'm from your bank and I need your account number."

Mark: Right.

Susan: Yeah.

Mark: These little warning flags should go off in your head.

Susan: So, you make the contact. You initiate it. Great. What are some other ways that I can prevent identity theft?

Mark: Well, there are a lot of common sense things that you can do. Being aware is probably the most important thing so that, again, those warning flags do go off in your head when someone calls you on the telephone and asks you for information. Be aware! You don't want to give out a lot of personal information on the telephone or through email so that's an important thing to do.

Susan: Mm. Hmm.

Mark: In terms of social security numbers, that's sort of the Holy Grail in terms of stealing identity theft. So you don't want to carry your social security card with you. It shouldn't be in your wallet or your purse.

Susan: Okay. Keep that somewhere safe in my house.

Mark: You should look and see what other cards that you have in your wallet or your purse and see if they are using your social security number as an identity number. I had my insurance company from my home that I opened up my wallet and looked at my own cards and found that my policy number was my social security number.

Susan: I wouldn't even think of that.

Mark: So, I called them up and said, "Change it." And they did but they wouldn't have done it if I hadn't asked them.

Susan: So probably the vast majority of their policy holders have.

Mark: Right and most...I think that a lot of companies are slowly changing over because of these risks but a lot of them are still using the social security number.

Susan: How secure then is my social security number, really?

Mark: Well, it's probably not as secure as we would all like it to be.

Susan: So that is something that people really should look out for.

Mark: But that doesn't mean that you want to publish it either, so.

Susan: Now, what about other things that I'm carrying around in my purse or wallet?

Mark: Well, you need to keep track of what you have.

Susan: Mm. Hmm.

Mark: Well, you know, do you know what's in your purse? Like if your purse were stolen today would you know who you need to contact to say, "Close down this account."

So, you need to make a list or make a photo copy and of course you have to keep that in a secure place.

Susan: Mm. Hmm. Okay. What about securing my identity with my computer? I know that there is...we just did a show recently on passwords and obviously that's a big issue, making sure that your password is secure and so forth. But are there other things that I need to be concerned about so people don't hack into my personal information on my computer?

Mark: Sure. Well, I would start with passwords.

Susan: Obviously that's the base.

Mark: That's the base, yeah. You want to make sure that you don't have your post-it note with your password on it, or even if it's a...

Susan: Well, isn't that what post-it notes are for?

Mark: Yeah, well, I actually do say that, or hidden underneath your mouse pad where no one would know to look for it.

Susan: It's like putting the key under the mat. Yep. Yep.

Mark: So there are basic things about keeping your patches current. Having antivirus software those kinds of things.

Susan: So keeping your patches current so like your Windows patches or your Apple/Macintosh operating system patches.

Mark: Right, antivirus software; firewall if you're, especially if you're on the, you know, like a cable modem.

Susan: High-speed.

Mark: High-speed network. Anti-spyware software is another thing that's come out.

Susan: Absolutely. Now for firewalls, now, don't Windows and Macintoshes have firewalls built right into their operating systems?

Mark: It depends on what version of the operating system you have.

Susan: If they're the latest ones. Yeah, the newer ones. Okay and then anti-spyware.

Mark: Spyware is sometimes called adware. A lot of it is not as bad as people might think it is, but there is not just one program out there that will take care of all the different

spyware there is right now until the industry sort of consolidates you need to be running one or more different spyware programs, anti-spyware programs.

Susan: And spyware is things that might watch what you're doing as you're doing things online.

Mark: They're tracking the cookies, those kinds of things.

Susan: Yeah. So that is something that you would have in addition to your antivirus software. That's great.

Mark: And then, other things that you can do with your computer is take sensitive information and take it off-line.

Susan: Okay.

Mark: You know if you're on your home computer and you've done your taxes and you have all sorts of information there, you may just want to burn that onto a CD and then remove it from your hard drive so that if your computer were compromised they wouldn't be able to get to that personal information.

Susan: Absolutely. That's a great idea. What about disposing of my computer?

Mark: Well, when you get rid of your computer you need to use a piece of software to wipe the hard drive completely clean.

Susan: Okay.

Mark: When you delete files or even format your hard disk they're really, the files are really there, it is just destroying the table of contents so you need to make sure that you actually wipe your hard drive clean before you give it to somebody else.

Susan: So, by throwing something in the trash it's...

Mark: It's fair game!

Susan: You can still find it, it's just a little harder to find. So, what would wipe my computer clean? Is this a separate piece of software you can buy?

Mark: It's a separate piece of software. Some of the utility software programs, the suites like Norton, Symantec that comes with a piece of software that you can use to wipe your hard drive.

Susan: Okay.

Mark: There are other software available. You can search for it on the web.

Susan: Okay. And sometimes it may not be that obvious to some people depending on what they use their computers for but just about everybody should wipe their hard drives clean, even if they don't keep financial information on there, there may be other things that

Mark: It's a good idea.

Susan: Yeah, absolutely a good idea. Great. A couple of other things, we talked a little bit about some less technical stuff; things you're keeping in you wallet and so forth. What about things like what you put on your check? Like...

Mark: Well, a recommendation is that you don't put your social security number on your check.

Susan: Yeah.

Mark: You don't put your driver's license on it, you don't even put your telephone number on it.

Susan: And people have been doing the driver's license and telephone number big time because...

Mark: I did it for years.

Susan: Yeah, because you go to a store and they immediately want to write that down and it takes forever. So, but what can people do with that driver's license number. I mean, why wouldn't you? What's so private about that?

Mark: Well that's another piece of private information about you that helps them fill in the pieces of a puzzle.

Susan: Anything else that users should really be aware of to would help protect themselves?

Mark: Well, in terms of non-technical things you should use a shredder.

Susan: Mmm. Simple stuff.

Mark: Yeah, simple type of things. You should shred your bank statements when you're done with them, your checks when they come back.

Susan: It's horrible to think someone might be going through that trash, but really!

Mark: And you know you get, a lot of people get unsolicited credit card offers and you should be shredding those up or putting those through a shredder as well.

Susan: Absolutely. Thank you so much for being here with us today, Mark.

Mark: My pleasure. Thank you.

Susan: But what happens if you do all those things and your identity is still stolen? Then what do you do? Report it to the police, for sure, but they can only do so much.

Officer Jason Tossey: Over the last three years I've handled the majority - three to four years - I've handled the majority of identity theft, fraud and forgery cases at the University of Minnesota Police Department. We had an individual who made a report with the university police that said three credit cards were opened up in his name. That case, I was not able to get anywhere on it at first, I contacted the creditors, they said this individual did open up these credit cards, they believed it to be so. The address that the credit cards were issued under were actually the victims address. So I was unable to do any tracking because this was all done via the U.S. Mail. So I contacted the United States Postal inspectors hoping that they would be able to help me but there was really no way to identify who had done this. That case went inactive for some time, about eight months, and then all of a sudden another case crossed my desk and I recognized the name. It was actually the University of Minnesota bookstore was where this person attempted to charge books via the internet. In other words, charge it on the victim's credit card. That left a lead for me because I was able to trace the internet protocol address that individual made the purchase from. That person attempted to make a purchase on the internet from a house in St. Paul. I brought the guy in for a voluntary interview. When he came in he brought an attorney and myself, the postal inspector and the agent with the secret service we did an interrogation, it wasn't a custodial one, I never put him under arrest but we asked him questions. He all but admitted to it. Now there were problems, and it really shouldn't be a problem but unfortunately there is, this occurred over, well not only...because if you consider not only my other victims many different states but this occurred over counties. And one of the difficulties that I had was trying to figure out who should prosecute this. So I realized that I had to bring this forward on the state level and as police officers we do that through the county attorneys and one county attorney that I contacted they weren't sure that the theft actually occurred in their county. And I contacted another county attorney and just because he lived in their county doesn't necessarily mean that he did the theft, the identification theft and fraud and forgery in that county and they're correct. And I found out this individual, the reason why he had hundreds of social security numbers, credit cards and routing numbers was because he worked for a collection agency and so when people would call to make payments, they would give that information to him and he would copy it down and he would save it and he would use it. And that occurred in different county. As of this date, there has been no prosecution.

Susan: Not a conviction. Not even a county prosecution, so now what do you do? Who do you go to? Her name is Susan Matt. Sue has worked for the postal service for over fifteen years in a variety of positions but is currently a postal inspector, a federal law

enforcement agent who specializes in mail fraud investigations. Thank you for being here today, Sue.

Sue: My pleasure.

Susan: Now, I talked with Mark a few minutes ago about how so much identity theft is happening over the internet why is the postal service involved in identity theft?

Sue: The postal service is involved because, typically at some point, throughout a case of identity theft an address is used or the mail is used and we have investigative jurisdiction over any type of crime that committed using the U.S. Mails.

Susan: Okay, so even if someone might use the internet to get you to put in your credit card account number, but when that person orders a credit card it has to be delivered through the mail to their house.

Sue: Exactly. They might fill out an application online but the physical credit card will be mailed to them or they may order merchandise over the internet and the merchandise will be mailed to them. So that's the nexus there; that's why we're involved in these investigations.

Susan: So, that's what puts it in the postal service jurisdiction, great. What exactly do postal inspectors do?

Sue: Well, as you mentioned we are federal law enforcement and we investigate any type of crime that happens using the U.S. Mail. As we are speaking about today about identity theft, but really anything illegal such as child pornography through the mail, drugs, bombs through the mail, mail fraud, mail theft, robberies, burglaries any of that stuff.

Susan: Okay, okay. With the situation that officer Tossey just talked about, what can the postal service do about that? Can they help out in this particular situation?

Sue: I believe that we can. Simply because we are federal law enforcement so we can assist local law enforcement when they do run into those problems that have to do with county jurisdictions; crossing county lines or crossing state lines. We can help aggregate those charges and pursue federal prosecution.

Susan: Mm. Hmm. I suppose since you keep track of things in different counties and different states as well you may also be able to take care of situations where... when someone is stealing one person's identity, I assume they might be stealing other people's identity as well. Can you make some connections with those crimes?

Sue: You are absolutely correct. It's not usually a person who does this one time and victimizes one person. These are rings of individuals who victimize many, many, many people and that is something that we, with our databases and agents across the country,

we can keep track of that information and hopefully tie things together and bring a larger case to a federal, a U.S. attorney's office for a federal prosecution.

Susan: And a larger case, I think, could be a big issue. We've kind of been focusing on the idea that if someone steals your identity they can do a lot of bad things, but sometimes it's just a little bit. They might just put a little bit of something on your credit card. A little bit from one person; a little bit from another.

Sue: Exactly.

Susan: So you really do have to aggregate it before you have a case that's even worth prosecuting at all.

Sue: Correct. And sometimes I think that criminals are onto that. They know that if they do just a little bit here and a little bit there that they may be able to circumvent the system and we want to show them that that's not at all the case.

Susan: It's good that we have someone taking care of that. I know that there was some a recent law passed that helps out with your with the postal service's jurisdiction. How exactly does that work?

Sue: It's a federal identity-theft statute that says that if you are convicted of identity theft you will serve a mandatory two-year prison sentence consecutive to any other sentences that you might be serving related to that crime that you've committed. So I know that sounds a little bit confusing but basically, if you have committed a crime you are probably going to be charged with several different things. Perhaps bank fraud, false statements, identity theft. If you are found guilty of all three of those things you are going to be sentenced. You'll get a sentence for bank fraud, for example, if you are sentenced to three years, then in addition to those three years, then after you serve that, it is mandatory that you will also serve an additional two years for your conviction of identity theft.

Susan: Okay so this really puts some...some teeth in the prosecution.

Sue: Exactly.

Susan: Great. Identity theft has really been on the rise recently. This is why we are all hearing about it.

Sue: Yes.

Susan: What's the difference between now and say, five years ago?

Sue: It's been doing nothing but increasing. And that's the reason for the change in the federal statute, because it is a problem and it's something that we all know is a problem and we need to be able to address it.

Susan: I think we've got a lovely chart here that show the increase and it looks like we don't really quite have numbers here for last year; I would assume that it's probably gone even farther. This is a very conservative estimate of what happened in 2003.

Sue: Conservative at best. What we find in law enforcement is that many people don't even report that they've been a victim and so the chart that you're referring to only the people who have gone to the trouble to report it to the Federal Trade Commission.

Susan: So in one year we've gone from less than 2,000 victims per year to over 210,000.

Sue: Correct.

Susan: What do you do; what should you do if your identity is stolen?

Sue: The very first thing that I recommend that a person does if they think that they've been a victim is contact your local police department. They are in the position to respond immediately and file a report. The quicker you can do that the easier it's going to be for you in trying to get your credit back on track. So that first call is going to be to your local police department.

Susan: Okay.

Sue: If you suspect that your mail has been stolen or that the mail has been used in any way, shape or form, the second call is going to be to the postal inspection service.

Susan: Okay so even though the police might contact them as well you should contact them as an individual too.

Sue: Yes. I always recommend to people; take the initiative. Do as much as you possibly can because the more you do, the more control you have and the better the chance of the outcome of your case is going to be.

Susan: Absolutely.

Sue: So then following notifying law enforcement, definitely contact your bank or financial institution. You're going to want to contact your credit card companies and also the three major credit reporting agencies. It's very important to do that. You can put a fraud alert on your credit so if anyone attempts to take out additional credit using your personal identifiers, you will be notified of that.

Major Credit Reporting Agencies

Equifax
(800) 525-6285
Experion
(888) 397-3742

TransUnion
(800)680-7289

Susan: I know that if you do a Google search on credit bureau they are the top three listings.

Sue: Yes, they are.

Susan: Another thing you can do to prevent stuff is check your credit ratings. Isn't that a good thing to do to make sure that who is...Everytime you open up a new credit card there gets to be a listing in your credit report and so it's a good idea to check and see, "Oh. I didn't ask for that particular credit card."

Sue: Exactly. I always recommend that you check your credit history at least once a year just to keep on top of it.

Susan: Mm. Hmm.

Sue: Because we have heard of very sad stories where people have been applying for a mortgage or wanting to purchase a vehicle or just take out a personal loan for whatever reason and suddenly you're denied credit and you have no idea why until you get a copy of that credit report.

Susan: This I think is one of the insidious things about identity theft. A lot of people may not realize that they've been a victim. You have maybe just a small thing on your credit card you many not always keep track of exactly what you use your credit card for, and you forget to check into it, but these are things that people should be double checking on.

Sue: Yes. It's very important to check those monthly statements when you receive them because you have a limited amount of time to dispute any fraudulent charges.

Susan: Mm. Mm. Absolutely.

Sue: So it's important to keep an eye on that.

Susan: Absolutely. It sounds like if you are a victim of identity theft really there is a lot of responsibility on the victim to do a lot of stuff.

Sue: There is. There is, because in fact, sometimes what happens is you're really almost put in the position of having to prove that you're innocent. A lot of people don't pay their bills and they're on the bad collections lists and credit card companies may think that you're just one of those people trying to get out of paying your bills.

Susan: That's exactly what we saw with Officer Tossey. At first they thought it was the individual who'd made those expenses.

Sue: Exactly. You kind of have to prove that you're the victim.

Susan: Absolutely. How much money is lost to identity theft per year these days, do we know?

Sue: It's a startling figure. Statistics show that annually for financial institutions, credit card companies, et cetera the cost is approximately fifty billion dollars.

Susan: That's a staggering number and it's obviously rising tremendously every year.

Sue: It is. It's something that identity theft investigations and complaints have been the top complaint to the Federal Trade Commission for the last four years and it just continues to grow.

Susan: Well, Sue, thank you so much for the information that you've given us today.

Sue: You're welcome.

Susan: It's been very helpful. Well, that's our show on identity theft. All of our guests have offered a number of suggestions for securing our identity; many of which we've included in this For Your Files.

Susan: Data security director, Mark Powell, outlines some common sense ways to prevent identity theft.

Mark: Be aware! You don't want to give out a lot of personal information on the telephone or through email. There are basic things about keeping your patches current. Having antivirus software firewall if you're, especially if you're on like a cable modem.

Susan: High-speed.

Mark: High-speed network. Anti-spyware software is another thing that's come out. And then, other things that you can do with your computer is take sensitive information and take it off-line.

Susan: Okay.

Mark: You know if you're on your home computer and you've done your taxes and you have all sorts of information in there, you may just want to burn that onto a CD and then remove it from your hard drive so that if your computer were compromised they wouldn't be able to get to that personal information.

Susan: Absolutely.

Susan: And Mark said beware of phishing spelled with a "p-h"

Mark: It's a scam where someone will send you an email and pretend to be from your bank or from another prominent company and try to get you to click on their url which looks right, and then they try to encourage you to provide all of your private information. Most companies won't ever ask you for that information online so, the best advice is to just delete it.

Susan: Finally Mark said, when you get rid of your computer

Mark: You need to use a piece of software to wipe the hard drive completely clean.

Susan: Okay.

Mark: When you delete files or even format your hard disk they're really, the files are really there, it is just destroying the table of contents so you need to make sure that you actually wipe your hard drive clean before you give it to somebody else.

Susan: Postal Inspector, Susan Matt said that if your identity has been stolen

Sue: So that first call is going to be to your local police department.

Susan: Okay.

Sue: If you suspect that your mail has been stolen or that the mail has been used in any way, shape or form, the second call is going to be to the postal inspection service.

Following notifying law enforcement, definitely contact your bank or financial institution. You're going to want to contact your credit card companies and also the three major credit reporting agencies. It's very important to do that. You can put a fraud alert on your credit so if anyone attempts to take out additional credit using your personal identifiers, you will be notified of that.

Susan: And a couple of final reminders from the postal inspector

Sue: It's very important to check those monthly statements when you receive them because you have a limited amount of time to dispute any fraudulent charges.

Susan: Mm. Mm.

Sue: I always recommend that you check your credit history at least once a year just to keep on top of it.

Susan: If you missed any portion of our program on identity theft or want to see it all again, stop by our website. All of the programs we've done so far including this one are right there for your viewing, our address is techtalk.umn.edu. And if you have a question about his program just post it on our website and we'll have one of our specialists answer it. Next week we're going to talk about spyware, adware, pop-ups and cookies. And

they're not games or food or books, they are on your computer and you may not even know some of them are there. Thanks for watching, until next week, I'm Susan McKinnell.

Tech Talk is produced by Academic & Distributed Computing Services and the Digital Media Center, Office of Information Technology in cooperation with University Relations, University of Minnesota

Executive Producer
Robert H. Bruininks

Special Thanks to:
Steve Cawley
Shih-Pau Yen

Host
Susan McKinnell

Producer / Director
Susan J. Tade

Associate Producer
J.B. Eckert

Field Shooting
Jonathan Kranzler

Assistant Director
Rich Reardon

Technical Director
Steve Barbo

Audio
Gary Bleskachek

Floor Director
J.B. Eckert

Cameras
Laura Cervin
Jonathan Kranzler
David Lindeman

Lighting
Laura Cervin

Set Design
Richard Stachow

Graphic Design
Nicky Torkzadeh

Effects Design
Paul Pecilunas

Make-Up / Prompter
Sharon Davis

Web Development Team
Christina Goodland
Lance Cunningham

Thanks to:

U.S. Postal Inspection Service

University of Minnesota Police Department

CLA Studio B

Radio K

Bakken Library & Museum

KSTP Meteorology Department

Pavek Museum of Broadcasting

Antique Telephone Collectors Association

2005 University of Minnesota

.