

**PAULA ZAHN NOW**

# Stopping Identity Theft



Aired May 26, 2005 - 20:00 ET

THIS IS A RUSH TRANSCRIPT. THIS COPY MAY NOT BE IN ITS FINAL FORM AND MAY BE UPDATED.

PAULA ZAHN, CNN ANCHOR: And good evening, everybody. Welcome. Glad to have you with us tonight.

It is a multibillion-dollar epidemic. And it's all about you and your most private information, stuff you would never want to land in criminal hands. Well, a new generation of thieves is stealing billions and sticking you with the bill.

(BEGIN VIDEOTAPE)

ZAHN (voice-over): Your secrets bought and sold in a cyberspace black market.

UNIDENTIFIED FEMALE: They can open up new accounts in your name. They can drain your existing accounts.

ZAHN: It is your money. It is your time. It is your life.

UNIDENTIFIED FEMALE: I've been living identity theft for seven years now.

ZAHN: A nightmare that won't go away. Tonight, stolen identity, what you need to know and what you can do to protect yourself.

(END VIDEOTAPE)

ZAHN: And thanks again for joining us for this special broadcast.

If you think identity theft can't happen to you, you are dead wrong. Take a look at these numbers. According to the Federal Trade Commission, 10 million people a year, about 27,000 people a day -- that adds up to 19 people every minute -- are the victims of identity theft. And it is happening all the time. Just today, we heard that nearly 10,000 Social Security numbers were stolen from Stanford University computers two weeks ago.

Also this month, account information for almost 110,000 Bank of America and Wachovia customers also may have been stolen. And, here at Time Warner, tapes holding personal information on as many as 600,000 current and former employees vanished during shipping.

When crooks start using your name, your Social Security number, your credit card numbers, your life becomes a nightmare. You may want to grab a pen and some paper, because, tonight, we're going to give you some information you need to protect yourself and your family and, if it is too late, what you need to do to get your identity back. A panel of experts is with me tonight. Most of them have been

victims themselves. They'll be answering your questions. You can call us at 1-800-304-3638. That number once again, 1-800-304-3638. Or you can send us an e-mail at [idtheft@CNN.com](mailto:idtheft@CNN.com). Once again, [idtheft@CNN.com](http://idtheft@CNN.com).

First, though, a dramatic demonstration of just how easy it is to steal and sell personal information from technology correspondent Daniel Sieberg.

(BEGIN VIDEOTAPE)

DAN CLEMENTS, CARDCOPS.COM: Here is a thief that says he has a Citibank credit card or checking account and he wants to be paid via W.U., which is Western Union, to make a deal. And if you want to make a deal with him, message him.

DANIEL SIEBERG, CNN TECHNOLOGY CORRESPONDENT (voice-over): Dan Clements of Card Cops doesn't carry a badge or a gun. But he's on patrol in cyberspace, in virtual black markets, where thieves buy, sell and barter personal information in underground chat rooms. The format is called IRC, or Internet relay chat, a low-frequency hum in the World Wide Web. Think of it as the Internet equivalent of C.B. radio.

CLEMENTS: This is just a guy posting that he's hacked into a checking account with a \$2,100 balance and he's X'ed out the numbers. He's proving he has access to it and he wants to trade for some type of tool or ware and he wants to split the money on this account.

SIEBERG (on camera): So, this is somebody's checking account just waiting to be robbed?

CLEMENTS: Yes. Yes. And he's -- he's looking for help. He's looking for an accomplice.

SIEBERG (voice-over): It is a live look at identity theft, chitchat among con artists happening in real time. If you have heard about personal data being stolen, a lot of it ends up here.

CLEMENTS: This is what they call a gold profile. This is all the information on this lady. We have her e-mail address, eBay account, PayPal account. We have her first name, last name. We have her address, phone. We even have her Social Security number. We have her MMN, which is mother's maiden name. If the thief has this information, he can absolutely rip this lady's identity off in seconds.

SIEBERG (on camera): Dan, help me understand this I.D. thief community or black market, if you will. Each of those names down the right-hand side there, they're actual people in this virtual world trading all of this very real data in real time?

CLEMENTS: That is correct. And these people in the chat room, they're usually in Europe and they're trading credit cards and identities. They're swapping out different types of wares and tools, so they can commit crimes. But they're real. They're doing this right now.

SIEBERG (voice-over): Clements doesn't have the means to track down the criminals. But he earns his living by spreading the word. His team alerts law enforcement, credit card associations and merchants, many of whom pay for his information. And he even notifies consumers whenever they spot a crime in the making.

CLEMENTS: Hello, Nestor. My name is Dan Clements with Card Cops and I'm investigating some fraud on your MasterCard ending in 1992.

SIEBERG: A man name Nestor's entire personal profile is posted. We have no trouble calling him

since, well, we have his home number.

(on camera): How do you feel knowing that all of this personal information of yours is in this chat room, where anybody could come across it and buy and sell it? How does that make you feel?

UNIDENTIFIED MALE: Oh, my gosh. It's in a chat room?

SIEBERG: Yes.

CLEMENTS: Yes.

UNIDENTIFIED MALE: Well, no wonder, because, at this moment, I'm still getting charges from -- even from Spain, Italy.

SIEBERG: Does it scare you that this is happening?

UNIDENTIFIED MALE: Well, it does, yes.

SIEBERG: Is it too late for Nestor now that his information is out there, Dan?

CLEMENTS: Well, it is too late in one regard. But, Nestor, you can put a fraud alert on your credit file.

UNIDENTIFIED MALE: Well, I did that.

CLEMENTS: Oh, you did that. That's good.

SIEBERG (voice-over): A little later, Clements gets a private communication.

(on camera): So, Dan, somebody is messaging you right now?

CLEMENTS: Right.

(CROSSTALK)

CLEMENTS: Yes. They're sending me an instant message. And let's see what they're -- what they have to say.

SIEBERG: What do they often want?

CLEMENTS: This particular gentleman is offering credit cards with CVV-2, full info and PayPal. So he has those available and he wants to either sell them to me or trade them to me.

SIEBERG (voice-over): A whole new meaning to the phrase online shopping, price tags on your priceless information, bought and sold in a marketplace right under our noses.

(END VIDEOTAPE)

ZAHN: CNN's Daniel Sieberg and cyber security expert Daniel Clements joins us now from Los Angeles.

Welcome.

Daniel, how easy is it for these guys to get their hands on this information? We just got a sense of it in the chat room. And who are these guys who are stealing our identities?

SIEBERG: Well, there is a whole range of different profiles of the type of person who is getting this information. It could be a kid operating out of his bedroom, simply getting this information transacted online. There is a whole underground community that is able to get this information. It is bought and sold. And it really is a valuable commodity, your personal data.

ZAHN: Dan, you made it look so easy to go into one of those chat rooms. For those of us that aren't as facile as you are, how easy is it to crack it?

CLEMENTS: Well, it takes a few years to season what they call a nickname or an alias. So, we have these names and nobody really knows who we are. But we have been watching these rooms for about four years now.

So, it is not easy to get in. But once you're in, like in the room we're in right this very minute, there's 300 people in there trading credit card and full information.

ZAHN: And you're going to be monitoring that tonight during the show, right, Dan?

SIEBERG: Yes. We can't overstate, Paula, how often this is happening. This is happening all day and all night. And we're in here right now with about 600 or so just in this one room, where all of this is happening. And we're going to be monitoring it throughout the hour.

ZAHN: Mind-boggling. Daniel Sieberg, Dan Clements, I want you to hang with us all night, because we want to check to see what you are hearing as you monitor that.

I want to now introduce you all to the rest of our panel, all of them well versed in identity theft. And all of them have been victims themselves. Joe Magee is a former hacker who is now chief technology officer for Vigilant, a computer security company. Ellen McGirt is a senior writer and columnist at "Money" magazine. And Jonathan Turley, law professor at George Washington University, who lectures on identity theft. Great to have all three of you with us tonight.

So, Joe, I know your biggest concern is the vulnerability of all of the consumers out there. How bad is it?

JOE MAGEE, FORMER HACKER: It's -- Paula, it is very bad. As I think we already heard, identity theft is just a growing problem. It is not getting -- it is not stopping or, you know, slowing down anytime soon.

ZAHN: Ellen, I know you have three very specific ways you think consumers could better protect themselves.

ELLEN MCGIRT, SENIOR WRITER, "MONEY": Absolutely.

One of the first things they can do is take advantage of some of the privacy protections by opting out, calling your banks and brokerages and saying, you can't sell my information without my permission. Clean up your own paper trail. There's no reason why you should have your Social Security in your wallet. Buy a about good shredder. Make sure that all of your personal information that you don't need anymore is gone.

And, finally, check your credit report regularly.

ZAHN: Now, Jonathan, even if you do those things, it is obviously not bulletproof. And you don't think our government is doing enough to provide protections for consumers.

JONATHAN TURLEY, CONSTITUTIONAL ATTORNEY: Well, the government is not only not the solution. It is part of the problem; 94 percent of Americans are vulnerable to identity theft because the government puts their Social Security numbers on public documents.

Over 75 percent of counties in this country have documents that have your Social Security number available for identity thieves. It is a one-stop-shop item for identity thieves.

ZAHN: That's astonishing.

(CROSSTALK)

ZAHN: So, people don't have to work very hard to get them. All they do is go down to the courthouse and they've got access to the records.

TURLEY: Business is good, yes. And their main supplier remains the government.

ZAHN: What is it that the government is afraid of right now to -- to regulate, is that the issue?

TURLEY: Well, I'm astonished that Congress has moved so slowly. You have a bunch of states that are creating these patchwork systems of laws. If there is one area that requires a strong federal presence, it is this one. But Congress is moving at a glacial pace. It is astonishing.

ZAHN: And we are going to talk a little bit later on about why and what is motivating them not to do much, in your opinion.

Our experts will be taking your questions a couple of minutes. So, call us now at 1-800-304-3638 or send us an e-mail at [idtheft@CNN.com](mailto:idtheft@CNN.com).

We're going to leave the graphic up there for a moment or maybe put it back, just in case you missed it the first time around.

But, coming up next, the catastrophic results of having your identity stolen.

(BEGIN VIDEO CLIP)

UNIDENTIFIED MALE: These were credit cards that I never had. I never even -- I never even received their catalogs.

(END VIDEO CLIP)

ZAHN: Stay right there. We're going to tell you what you need to know to protect yourself from a financial disaster.

(COMMERCIAL BREAK)

ZAHN: We're back.

Ten million Americans a year are victims of identity theft. It costs them a total of \$5 billion every year.

And, tonight, our panel of experts will be answering your questions about identity theft. The number to call is 1-800-304-3638, once again, 1-800-304-3638, or e-mail us at [idtheft@CNN.com](mailto:idtheft@CNN.com).

First, though, a detailed look at the cost of identity theft.

(BEGIN VIDEOTAPE)

ZAHN (voice-over): Suzanna (ph), Linda (ph), Maureen, just three of the millions of Americans who had their identity stolen, three victims in a major crime wave that the government says costs about \$50 billion a year.

Suzanna fell prey to an Internet phishing expedition responding to a request for her credit card information from a Web site that looked real, but was fake.

UNIDENTIFIED FEMALE: I got an e-mail from AOL saying that they needed to check my billing.

ZAHN: Linda's boss stole her Social Security number and other personal information right off her tax forms.

UNIDENTIFIED FEMALE: She used those to get credit cards and a cell phone, the very same cell phone I was calling her on, on a daily basis.

ZAHN: And Maureen's identification and Social Security card were stolen when she left her purse in a shopping cart. Two years later, she began getting strange bills in the mail.

UNIDENTIFIED FEMALE: These are credit cards that I never had. I never even -- I never even received their catalogs.

ZAHN: For each of these women, the means were different, but the results the same, fraudulent bills, damaged credit, hours of time and lots of effort spent trying to reclaim their identity.

BETSY BRODER, FEDERAL TRADE COMMISSION: With your Social Security, date of birth and name, they can open up new accounts in your name. They can drain your existing accounts.

ZAHN: The rise of the Internet has given birth to a new breed of criminal, a faceless thief who needs little besides your personal information and an Internet connection to wreak havoc on your life.

MARK RASCH, SOLUTIONARY, INC.: Every place you ever lived, every address, everything you ever have owned in terms of real estate, every time you've been sued, all of that information is collected.

ZAHN: According to the Federal Trade Commission, identity theft is the number one consumer complaint for the fifth year in a row. In 2003, the latest figures available, almost 10 million Americans were the victims of some kind of identity theft. Of those, 3.25 million had their personal information misused to open new credit accounts, take out loans, or commit other types of fraud.

The cost to the businesses, \$33 billion. The average cost to each victim, \$1,200 and an estimated 60 hours to resolve the situation. And, for some, the fallout can last for much longer.

UNIDENTIFIED FEMALE: I've been living identity theft for seven years.

ZAHN: In the past few months, ChoicePoint, LexisNexis, Bank of America, Ameritrade and a host of

other companies have admitted their databases have been compromised, putting the personal information of thousands of customers and employees at risk.

RASCH: It is really, really difficult for people to be able to prove to banks and insurance companies and other entities that, whoever it was who charged these accounts or created these false identities wasn't you. And getting your own identity back is very, very difficult to do.

(END VIDEOTAPE)

ZAHN: Once again, my guests tonight are former hacker Joe Magee, now a security expert, Ellen McGirt, senior writer and columnist at "Money" magazine, although you don't look too senior.

(LAUGHTER) ZAHN: And Jonathan Turley, law professor at George Washington University. All three of them have been victims of identity theft themselves. Also with me, CNN technology correspondent Daniel Sieberg and Dan Clements, a security expert at CardCops.com, a service that protects consumers from identity theft.

We're going to go straight to our first call right now.

Martie from Florida, what is your question?

CALLER: ... taking my call.

What I'd like to know is what is the average person can do to check to see whether or not their information has been compromised.

ZAHN: A very good question.

Ellen?

MCGIRT: Yes.

It's absolutely -- the onus is on the consumer to check and be vigilant and make sure that nothing is happening. One of the best things they can do is check their credit report regularly. Now, thanks to adjustments in the Fair Credit Reporting Act, we can all get our credit reports free. Go to [AnnualCreditReport.com](http://AnnualCreditReport.com) and you can get all three free every 12 months.

ZAHN: The red flag might not be that obvious, though, right, when you're looking at the credit report.

(CROSSTALK)

ZAHN: When you're talking that the average victim is, what, \$7,000 per victim. So, what should you be focusing in on? Could it be as little as \$100 or \$200 here per month?

TURLEY: Well, you particularly, on your credit report, want to look to see if anyone has actually made an inquiry for new credit in your name. That's one of the most important ones. It should alert you if someone has applied for a card in your name or if your credit has been checked out by another business.

If you -- if you're not doing business in the Bronx and you're in Boise, then there is an obvious problem here. Somebody in the Bronx is using your name to possibly get a credit card. That's the most important one. The other thing is to get a system that notifies you quickly. Some of them are 24-

hour notices. But if -- you've got to look very carefully, because some of these packages, it takes a week and they'll notify you every week.

Well, by a week, you could be -- your card could be cleaned.

ZAHN: A lot of damage could be done.

TURLEY: That's right. (CROSSTALK)

TURLEY: And these identity thieves know how to do it. They stay small. They hit fast. The average phishing site, which is these fake sites that get you to show, give information, lasts only five days before they shut it down. It takes an average of 5.8 days for the good guys to shut it down. So, they are just shutting down shy of when they know someone is going to be on their tail.

ZAHN: That's so scary.

We're going to take another call. And I want to come back to these phishing sites, because those, in and of themselves, are pretty murky places.

Karen from Toronto, what is on your mind?

CALLER: Yes. Thanks for taking my call.

ZAHN: Our pleasure.

CALLER: I have a real concern. My bank merged with a trust company in Canada. And the bank's -- the trust company in the merger lost track of me. I could not get into my safety deposit box. So, I don't know where my information went. They lost track of me as of 1999.

ZAHN: Daniel, what should she do about that?

MCGIRT: First of all, was that T.D. and Canada Trust?

CALLER: Absolutely. How did you know?

SIEBERG: OK. I'm from Canada.

(LAUGHTER)

SIEBERG: Just happened to know that.

That is something you really have to go to your bank and discuss with them. I know a lot of people, when that merger happened, felt like they were lost, sort of falling through the cracks in a sense. And, really, you are going to have to go to your bank and talk to them specifically, probably at the local level, to at least get something that will help you.

ZAHN: Now, Joe, that could be a pretty frustrating process, couldn't it?

MAGEE: Absolutely.

I mean, having to go through that and trying to explain to somebody who you are is very bizarre process, you know, for us humans. You know, you know who are. I have my I.D., whereas one of the

number one scams that these fraudsters, I.D. theft people will do is, actually, they'll have my name. They'll be another Joe Magee out there that actually goes and applies with my Social Security number and gets a credit card and then has it shipped to their address.

Essentially, you know, there is no way to prove that. So, it is word of mouth, basically. You have your signature, but even there is hearsay wrapped around that. So it's very difficult.

ZAHN: It almost seems like it is impossible to stay ahead of these guys. These guys are so agile, and like you said, working so quickly.

MCGIRT: Technically, it is true. It is impossible to stay ahead of them, which is why you have to be organized, why you have to stay on top of things, why you have to put everything in writing, memorialize every conversation you have, file complaints with the FTC.

They have a wonderful affidavit form that helps you to organize what your concerns are. And make sure you follow up with everyone.

ZAHN: Daniel, I see you nodding your head. Jump in here.

SIEBERG: Yes.

We have been monitoring this chat room for the last little while here. And we have got a really good example of what is being bought and sold in real time. What we have got here basically, and we're going to try and shield as much information as we can here. This is very sensitive. It is tough to do this in real time in a live situation.

What we have got here is a gentleman by the name of -- we'll call him Jeff. His personal credit card information, pin number, the security number that is also on your credit card, all of that is being offered if you will join him in another room.

Now, Dan, does he want something in exchange for all of this?

CLEMENTS: Of course. He wants money for this particular account. And because it has the pin number, it is extremely valuable. It is cash. They will create a fake credit card and go to an ATM and withdraw all of his money.

ZAHN: That is absolutely amazing. And this is something that is happening, like you say, once every 19 minutes or so. What kind of money are we talking about here, Daniel and Dan?

CLEMENTS: Well, it is going to depend on how much money this gentleman has in his checking account.

SIEBERG: And the more he's got, the more valuable he is as a target, right?

CLEMENTS: Right, absolutely.

SIEBERG: Right.

ZAHN: But the bottom line, Jonathan, we're talking about major dollars, billions and billions of dollars that are being made this way.

TURLEY: I think that's right. We can't delude ourselves. We're losing this war.

People that talk optimistically, the identity thieves are still driving this whole area. We are barely catching up to these sites and we're losing. And as soon as we recognize that, that it is good business to be an identity thief -- do you know, in Kiev, they actually held a conference on identity theft, not how to stop identity theft, for identity thieves.

(CROSSTALK)

ZAHN: Trying to bring people into the business.

TURLEY: Right.

ZAHN: Of stealing other people's identities.

TURLEY: It was an open conference.

Now, when you can act with that openness, you realize how little effort there is by nations.

ZAHN: I don't think that's what they had in mind when they talked about perestroika and glasnost, is it?

(LAUGHTER)

TURLEY: Right.

ZAHN: All right, team, we're going to be back. There was actually a really good e-mail that I want you to talk about, if you frequently change bank account numbers and credit card numbers, if that changes this picture at all. And I'll give you all a chance to take a stab at that on the other side when we come back.

We're going to find out what happens when you shop online. We're going to be right back with more of your phone calls and e-mails. The number is 1-800-304-3638. You can also e-mail your questions to [idtheft@CNN.com](mailto:idtheft@CNN.com).

We'll be right back.

(COMMERCIAL BREAK)

ZAHN: We're back with our special on identity theft. Our panel of experts will be taking your questions. The number again, 1-800- 304-3638. You can also e-mail your questions to [idtheft@CNN.com](mailto:idtheft@CNN.com).

But, first, about 27 minutes past the hour, that means it is time to check in with Erica Hill at Headline News to update the other top stories tonight.

Hi, Erica.

ERICA HILL, CNN CORRESPONDENT: Hi, Paula.

We start off in Washington, where there is filibuster frustration again in the Senate tonight. Republicans failed to stop debate over John Bolton's nomination to be U.N. ambassador. Again, they are accusing Democrats of obstructing a vote on the president's nominees. The Senate is expected to

resume debate after a weeklong Memorial holiday break.

We're also watching for the latest on the crew of a U.S. Army helicopter downed by small-arms fire in Iraq this evening. The military says the helicopter crashed north of Baghdad and that another chopper returned safely. Elsewhere in Iraq, another U.S. Marine died in fighting today. An improvised explosive device went off on a Baghdad highway when a U.S. military convoy passed by. The Iraqi government says it will launch a new operation to stop those attacks.

And, as you have been reporting, Paula, cybercrime, you know, is booming. Well, this week, the CIA is launching a series of cyber war games, the idea here, prepare for crippling attacks on government and business computers. Cyber attacks have intensified in recent years. And the CIA fears terrorists could go online and severely damage the U.S. economy.

And, finally, the biggest online auction house is coming under scrutiny. Here's Valerie Morris with tonight's "Market Movers."

(BEGIN VIDEOTAPE)

VALERIE MORRIS, CNN CORRESPONDENT (voice-over): EBay, once a standout stock, is trying to regain some of its luster. It released solid first-quarter results, with sales up 36 percent and profits up more than 25 percent. But investors see a different picture. EBay shares have lost almost half their value so far this year. The company's growth, both in terms of revenue and auction listings, has slowed drastically since eBay first went public in 1998.

While eBay continues to dominate the Internet auction market with more than \$10 billion worth of goods sold in the first three months of the year, rival auction sites from Yahoo! and Amazon are cutting into eBay's market share.

(END VIDEOTAPE)

HILL: And, Paula, that's the latest from Headline News -- back over to you.

ZAHN: Honest answer, Erica. Learn anything from our special tonight?

HILL: I have been learning a lot. I had my bank account broken into once, so this is very -- hits very close to home.

ZAHN: Yes. You have a very good reason to pay attention. Thanks, Erica.

And I know I'm learning some new things here tonight. We're going to check back with you in just about 20 minutes or so.

And I'm going to be back with our four experts to take your questions about identity theft. Call us at 1-800-304-3638 or send an e-mail to [idtheft@CNN.com](mailto:idtheft@CNN.com).

Also ahead, a warning for all parents.

(BEGIN VIDEO CLIP)

UNIDENTIFIED FEMALE: I thought I was doing everything to protect her and never even thought that I had to protect her from identity theft.

(END VIDEO CLIP)

ZAHN: Something else to guard against. They're actually trying to steal your children's identity. That's next.

(COMMERCIAL BREAK)

ZAHN: Tonight, we are taking your questions on how to protect yourself from identity theft and what to do if it actually happens to you. The number to call, 1-800-304-3638 or you can email us at [idtheft@cnn.com](mailto:idtheft@cnn.com).

My guests are former hacker Joe Magee; Ellen McGirt, senior writer and columnist at "Money" magazine; Jonathan Turley, law professor at George Washington University, and lectures on identity theft, having been a victim himself. In fact, all three of you sitting here on the sofa have been victims. Also with me, CNN technology correspondent Daniel Sieberg and Dan Clements of [cardcops.com](http://cardcops.com).

I'm going to go straight to an e-mail from Daniel from Texas who writes, "Would frequently changing account numbers for credit cards and bank accounts decrease the odds of identity theft occurring to me?" Ellen?

MCGIRT: Not significantly. Clearly, you should shut down any accounts that have been used fraudulently or any accounts you don't recognize, and that means, of course, cutting up the cards or following up in writing. But, it's really a fool's game at that point. You're driving yourself crazy, changing credit cards. You're not really increasing the risk of -- your chances of, you're going to be lucky and not be tapped. You're much better off just being vigilant and making sure that you take care of any statements lying around. You keep them safe and check your credit report often.

ZAHN: No gray area in that answer.

MCGIRT: No.

ZAHN: Thanks so much. On to our next call. Marta from Illinois, what's your question.

Caller: Good evening.

ZAHN: Good evening.

Caller: My question is, I have actually been a victim of identity theft. The amount seemed small, about \$300 to my checking account, but the emotions behind it have just devastated me. I kind of seem like I have no life. I'm checking my account every -- seems like every two, three hours. I'm afraid my payroll check that is, you know, deposited is going to be victimized.

Can you explain or help me -- is there any kind of programs out there that can help people of identity theft to move on with their lives? Thank you.

ZAHN: Very good question, Jonathan. I know that is something you address when you speak publicly.

TURLEY: Well, you know, actually, that's a very typical case. Most identity thieves stay small because they know prosecutors will not prosecute if the case is just a few hundred dollars. These people are very sophisticated, and so they get in, they hit you. They usually hit you for less than a grand, and they move on, because they know if they're caught, the prosecutors just not going to prosecute.

And you really get in this caller's voice the real cost of this. It's really not just the money. It's a sense of total invasion. You know, the one thing we hand to our children, the one thing I give to my three sons, is their name. You protect it, and every family sort of -- sort of an empire in making. These people steal that, and the sense of invasion is just enormous, and you can see this with this person.

The best you could do is monitor your credit, be proactive, and unfortunately, it will be part of your life. You have to monitor it because your number is probably out there floating around.

ZAHN: Ellen?

MCGIRT: You can certainly put a fraud alert on your credit report which, theoretically, is supposed to make sure people will contact you if anybody seeks to open new credit in your name. But, four states have something called a credit freeze which means you can freeze your credit report entirely and this is something that everybody needs to think more about and push with their own legislators.

ZAHN: On to an e-mail from Michael from Virginia who writes, "I receive phishing emails" -- that's p-h-i-s-h-i-n-g, a distinct difference between that and f-i-s-h-i-n-g -- "and they're from the same sender. I have repeatedly forwarded these emails to my internet provider and the FBI. Why can't they catch these fraudulent emails?"

Daniel Sieberg?

SIEBERG: Paula, that's because they are so good at covering their digital footprints. A phishing scam is one of the fastest growing online scams on the internet, and probably everybody who has an e-mail account has received a phishing e-mail. You may not even be aware of it. It looks like it is from a trusted source. It may have the logos of companies that you deal with. It has all the information. It says, we need to update your personal information. We need you to do it right now or we'll close your account, so it's kind of threatening you, and you think that could be real.

If you click on a link in the message, it might take you to a website that looks real, and it says update all your personal data here. Well, you go ahead and do that and you hit submit. It doesn't go to that company. It goes to the scam artist, and by then they've got your information and it's too late.

ZAHN: How many legitimate institutions would actually ask you for your Social Security number and any of these other personal information online?

SIEBERG: The easy answer is absolutely none. That is not how they do business, and never click on an e-mail link within an e-mail message to get to one of these companies' websites. Call them or type in the website address in your browser.

ZAHN: Daniel, thanks. On to Doug from South Carolina who joins us on the telephone. What's your question?

CALLER: Yes. Great show tonight, guys.

ZAHN: Thank you.

Caller: How problematic are these wireless routers that most people are using now in their homes?

ZAHN: Very good question. You want to take a stab at that Mr. Ex-hacker?

MAGEE: Sure. To Doug's point, the wireless routers today are just another type of communications

medium. You know, we've had -- we started out with modems that were -- work through the telephone line. You dial up. Now you have cable modems. Wireless is another medium. People want the flexibility of, you know, being able to sit on their couch and do their work and VPN in (ph) the work or what have you.

It is really a lot of the same fundamental problems, but the new problem is, you don't actually have to be in an organization, for example, that may have wireless to access their networks. As part of our business, we do a lot of security assessments and you would not believe how many times, by just being connected to a network, we can actually access databases...

ZAHN: You're kidding.

MAGEE: ...that are not configured -- seven out of 10 times, in a recent security assessments -- that our company...

ZAHN: Seven out of 10 times? MAGEE: Seven out of 10 times we're able to actually access customer information with PII, which is personally identifiable information, which is just a combination of a name, a phone number, (INAUDIBLE), Social Security number, a driver's license number, whatever.

ZAHN: Absolutely frightening.

MAGEE: You know, you only need two things. Like Jonathan mentioned, you only need a Social Security number to, you know, to be able to access -- pretty much get the rest of the data from an individual.

So, wireless routers are just another type of communication medium. A lot of people don't properly install them.

ZAHN: Sure.

MAGEE: So, you know, they access them from outside somebody's house.

ZAHN: We're going to take another short break right now and get to more of your questions on the other side. Our panel will continue answering them in a moment. Please call us at 1-800-304-3638, or send an email to [idtheft@cnn.com](mailto:idtheft@cnn.com).

And you just don't need to worry about protecting your own identity. Up next, the story of some unsuspecting parents who discovered thieves running up bills in their baby's name.

(COMMERCIAL BREAK)

ZAHN: And welcome back to our special on identity theft. A reminder that you can call us at 1-800-304-3638, or e-mail us at [IDtheft@cnn.com](mailto:IDtheft@cnn.com). Anyone's identity can be stolen. Yours, mine, and get this even newborns. Here's my colleague Aaron Brown with a truly alarming story.

(BEGIN VIDEOTAPE)

AARON BROWN, CNN ANCHOR (voice-over): At just 21 days old Andrew Brook was causing his parents a few more problems than your average infant.

JOHN BROOKE, ID THEFT VICTIM'S FATHER: I went out to get the mail one day and opened up the mail from a medical clinic and realized that Andrew was being billed for an office visit for \$94.

Apparently, he'd driven himself across town, walked in to see the doctor for a work-related back injury and then prescribed a narcotic pain reliever that can sell for up to \$30 a piece on the street.

BROWN: Since Andrew was barely drooling, let alone walking and working, his parents suspected something was up.

BROOKE: The first thing we did was call the medical clinic and say where did you get this information. What's going on? And they told us it had been provided by the person who had walked in.

BROWN: Andrew's full name appeared on only two pieces of paper, his birth certificate and his medical records. And neither had left the Seattle area hospital where he was born. Yet the hospital told the family it found no evidence of a security breach. And police, the family says, were of little help.

BROOKE: It took two months to actually to get them to actually file the police report. And that was only after weekly phone calls from me badgering them until they finally filed one.

BROWN: No one has been arrested for stealing Andrew Brook's identity. Just as no one is usually arrested in such matters.

BROOKE: It is the fastest growing crime in this country. It is the most expensive crime to this country, costing between \$46 billion and \$53 billion a year. That's billion with a B, depending whose study you look at. And what I find really amazing is fewer than 1 in 700 cases are even investigated.

BROWN: Compared to Andrew, Rebecca Bartelheimer was all grown up when at 3-years-old her I.D. was stolen. Her mother learned this when she tried to open a savings account and found that her daughter's Social Security number was already in use.

MICHELE BARTELHEIMER, ID THEFT VICTIM'S MOTHER: I felt very violated. I thought -- I thought I was doing everything to protect her and never even thought that I had to protect her from identity theft. You think of car seats, helmets, coats on a cold day. You never think of someone stealing your child's identity.

BROWN: She has no idea how this happened. But says she spent a thousand hours trying to undo the damage caused to her 3-year-old's credit rating.

BARTELHEIMER: I just cried tears, because every day, all day I would wake up and spend all day day -- if I wasn't taking care might have kids, I had to be on the phone or on the Internet researching this and trying to track it down and sitting on hold on the phone waiting for someone to talk to me. It was horrible. It was a nightmare.

BROWN: When you consider all of the things that can happen here to your child, identity theft may not seem like much. But as a parent, it does change you. It changed Andrew's dad a lot.

BROOKE: You don't relax any more. You're worried about everything. What information am I giving out? Who is going to use that information? How will it be used?

(END VIDEOTAPE)

ZAHN: Something a lot of us didn't even know we had to worry about.

Joining us on the telephone is Rachel from Arizona who happened to be victimized by this kind of scam. You have an 11-year-old daughter whose identity was stolen?

CALLER: I have an 11-year-old son. But I just didn't know the process of what to do, notifying local authorities or even legal action against the company that hired this so-called person that has my son's Social Security number.

ZAHN: What would you do, Daniel Sieberg?

SIEBERG: Well, it's very difficult. First of all, a lot of these I.D. thieves operate offshore where it is very difficult jurisdictionally to actually go after them. That's one challenge. Also the resources for law enforcement are often very limited for cases like this. They simply don't have the manpower to go after all of these different cases.

That being said, it's certainly worth reporting all of this. If anything -- if nothing else, it will make you feel better about it. It will start a process and action that will at least try to get you your name back and make you feel better about things. And unfortunately make you feel a little paranoid. Which believe it or not is probably a good feeling to have this day and age.

ZAHN: Terrible it has come to that, but I guess that's the way we all have to live. Daniel, thank.

Lori from Texas now joins us on the telephone. What is your question?

CALLER: Yes, my question is I would like -- I've been fighting something for five years. Our kids' schools use their Social Security numbers as their school I.D. numbers. And I would like to know how I can change that.

ZAHN: It's a question a lot of parents all across the country have. What would you do in, Ellen?

MCGIRT: The answer is to keep fighting, keep insisting. It is very dangerous practice. Under no obligation to write a Social Security and use it as an identification. For employers who need to check who you are, that's fine. If you're looking to see -- get credit, with a lender, that's fine. Opening a checking account, that's where you're obligated. But this is insane.

The Motor Vehicle Department also have to collect Social Security numbers. But they don't have to put them on your license. You can ask for another number. She needs to ban together, she needs be a vigilant consumer, not vigilante consumer. She needs to get the other parents together and insist.

ZAHN: Is that an advertisement for his company, Vigilant?

MCGIRT: Oh I know, I keep saying that.

ZAHN: Oh, my God, the plugs keep on coming.

All right, team. We'll take a short break, we'll be back with more of your question in just a minute. Stay with us. We'll take a lot of them on the other side.

(COMMERCIAL BREAK)

ZAHN: Those numbers add up. As we mentioned throughout the evening, there are 10 million victims of identity theft each year. We quickly go back to Los Angeles right now where Daniel Sieberg is standing by along with Dan Clements. They have access to a chat room where they know that the

bad guys have stolen information that is being traded even as this program has been on the air. What have you found out?

SIEBERG: Paula, this is very scary. We have found, really, the gold mine for any I.D. thief out there. Just to bring this home for people. We have been monitoring this chat room where only certain people can get in, basically, and Dan Clemens is one of them, where these thieves are buying and selling this information in real time.

What we have come across here is a gentleman we'll call Ron. And basically we have all of his personal information. Everything from his phone number, his address, his Social Security number, his mother's maiden name, driver's license, it popped up in here in seconds. And basically his identity could already be compromised. And Dan, I mean, how significant is this really?

CLEMENTS: Well, 600 people have access to this in the last five minutes. So this gentlemen is in big time trouble.

SIEBERG: And part of the issue here, Paul, is that a lot of these types of chat rooms -- that participants in them are offshore, they're in Europe. It's basically prime-time for them right now. They're up in sort of the wee hours of the morning, they're in there trading this information. It is happening very quickly. All the time.

I mean, just in the last 45 minutes or so that we've been live during the show, we've seen countless examples of people's information being basically bought and sold without them ever knowing.

ZAHN: And once you begin to focus in on how much of that has happened during an hour, you can begin to understand the enormity of this problem. Billions of dollars of fraud conducted this way.

We've got another phone call, this one from John in Florida. John, what do you want to know tonight?

CALLER: Yes. My question is why do the credit card companies, if they're so interested in cutting back on fraud, require you to put your credit card number on every check?

ZAHN: Good question, John.

CALLER: There isn't one bill I get from a credit card company that doesn't say they want -- I do not do it. But they request it on every bill.

How many people does that check go through before it gets back to -- and cleared at the bank?

ZAHN: What about that, Jon?

CALLER: (INAUDIBLE) credit card company, and the credit card company identified on the check, going all through the system.

TURLEY: Well, John, what you're raising is exactly why we need legislation in this area, why it is a federal issue, that Congress has the ability to step in and to say we want to stop the companies and hospitals and schools requiring you to give the Social Security number. We want to shut down on these types of practices and try to develop a safer way to deal with what is an expanding online business and the expanding use of identity theft techniques.

And we're not going to do that unless Congress says, this is now our area. We need to preempt it. It's crazy to have 50 separate systems.

ZAHN: Got an e-mail now from Donni from Wyoming who writes -- "Companies are now offering insurance in case of ID theft. Would you suggest buying such insurance?" Joe.

MAGEE: Yeah, absolutely. If it's -- if it's a decent price, I mean, you know, it's all based on what your credit is and you know, if it's a percentage. I actually have insurance, and many times it's a couple of cents, you know, 30, 40 cents a month, and that's worth it to me, just for the hassle of being traveling and not having my credit card for two days.

ZAHN: Well, no, I know, we (INAUDIBLE) from our caller about 10 minutes ago...

MAGEE: Absolutely, over \$300.

ZAHN: ... who said even though that was just \$300, she is living with the fear of this kind of invasiveness forever, basically.

MAGEE: Absolutely.

ZAHN: Thank you, all. We're going to be right back with more of your questions and more of your answers. Stay with us.

(COMMERCIAL BREAK)

ZAHN: And we're back with more on how to protect your identity from identity theft. Another phone call, this one from Shannon from California. Fire away, Shannon.

CALLER: Hi. I was concerned about obtaining a credit report and opting out, because you do have to give all your personal information, your mother's maiden name, Social, whatever. And I don't know the integrity of whoever may be either working at the company or intercepting mail, somehow or another, and how do I do that safely without endangering myself?

ZAHN: That's a question a lot of people want to have answered. Joe.

MAGEE: Yeah, I mean, basically, you're taking a leap of faith there, right? You can have people, just analysts behind the desk getting your information, running it through a computer, pulling a file and then, you know, either sending it out to you in the mail or faxing it to you, or whatever the procedure may be. You know, and there is -- you know, the thing is, you know, trust is something that comes easy when you've never been a victim. In this case, you're trying to identify the fact that have I become a victim, and you're worried about touching base with the one organization that you can. But I'd say definitely stick more to, you know, the -- I'm sorry, TransUnion, Experian and Equifax, because they -- go right to their Web sites to get your credit reports.

ZAHN: Great. We got Rebecca on the line from North Carolina. What do you want to know, Rebecca?

CALLER: Yes, I received a bill from 1993, supposedly, that someone took out a loan for \$2,177. What do I do?

ZAHN: What would you do, Jonathan?

TURLEY: Well, if that bill -- if you don't remember, you know, being connected to that company, you should definitely contest and tell the company that you didn't make that purchase.

The problem I think that we have right now is that no matter what you do, no matter how careful you are, you can still be compromised. We've had massive losses by companies, and those people did nothing to cause the release of their identity.

ZAHN: Jonathan Turley, thanks. Team, thanks. We'll be right back right after this.

(COMMERCIAL BREAK)

ZAHN: Think about this: Over the past hour, another 1,100 people have had their identity stolen. Another half-million dollars in damage has been done. But also in the last hour, we have learned the need to be vigilant, regularly checking our credit reports, cutting down on those unguarded moments with a purse or wallet. Did I leave anything out, Jonathan? Got it all?

TURLEY: No, that's pretty good. But monitor your credit card, look for phishing sites. Be careful of giving information on the computer unless you know who you're dealing with.

ZAHN: Want to thank all of our guests now. CNN technology correspondent Daniel Sieberg; cyber expert Dan Clements in Los Angeles, giving us a rare view into these chat rooms; Ellen McGirt; Joe Magee, Jonathan Turley. We really appreciate your expertise. I learned a lot. I hope you all did too. Thanks for joining us tonight. "LARRY KING LIVE" is next.

END

TO ORDER A VIDEO OF THIS TRANSCRIPT, PLEASE CALL 800-CNN-NEWS OR USE OUR SECURE ONLINE ORDER FORM LOCATED AT [www.fdch.com](http://www.fdch.com)