Online Fraud: The Fleecing of Populace

By Jeff Lanza

My conference presentation covers many things that we can do keep in ourselves and our information safe in a world that poses many threats at the cyber level and in a physical sense. This paper summarizes key points to help us mitigate the threats we face at cyber and non-cyber level in our personal and corporate environments.

Corporate Security

As an organization it important for leaders to set the standard for security. Make it job one from day one. Leaders should set the standard for security, by not only talking the talk but walking the walk. Live by your words, department heads and managers should be involved in training sessions, attending like everyone else. Incidents should be taken seriously and action taken where appropriate. Before too long people will realize how important security is and begin to adapt is a part of an organizational culture

In thinking about protecting information at an organizational level, you must also then ask yourself this question: what information are we collecting and why. If it isn't necessary to collect for any business reason, then don't collect it. If it is necessary to collect but not store, then don't store it. Be particularly sensitive to SS numbers. They are the key to stealing a person's identity and you must pay special attention to this information.

Don't forget about digital media. A single hard drive can hold the records of hundreds of thousands of people. It costs just pennies to store a Gigabyte worth of documents – the equivalent of 1,000 thick paperback books. Flash drives, DVDs and CDs, all can contain the equivalent of what is in thousands of file cabinets. It makes sense to lock file cabinets that contain personal records. It defeats that sense if you leave a flash drive or a floppy disk containing those same records on your desk overnight or much worse yet in your car.

Since the Internet has become such an important part of our everyday per lives, it is important to keep in mind that it is still not really secure. We have made great strides in making it better, but the criminals have made great strides too. Most personal computers are now connected to the Internet and to local area networks, facilitating the spread of malicious code. Today's viruses may also take advantage of network services such as the, email and file sharing systems to spread. So it is best, if possible in your business to avoid storing sensitive information on a computer that is connected to the internet unless it is necessary for you business.

Personal Security

Protecting your computer

There are three basic things a home computer should have to protect against threats on the Internet: a firewall, virus protection and spyware protection.

The term firewall derives from the construction terminology referring to a physical wall put in place to protect the spread of fire. In computer jargon, it refers to the same concept, except the wall in this case is computer software or hardware that protects the entry of electronic communications that are not authorized. Computers that operate on the Internet without a firewall are susceptible to outside attack from hackers who could potentially place unwanted and

dangerous programs on your computer, including ones that could steal your information and possibly your identity.

A computer virus, like a human virus can infect a “host” and thereby create various levels of problems. A computer virus can potentially take many actions, some of which will be unknown to the computer user, such as helping to send spam e-mails for others or capturing your keystrokes and sending them to a third party as you type on the computer.

Spyware refers to computer programs that can, among other things, spy on a computer user and create vulnerabilities with regard to your privacy and personal information.

It is important to protect your home computer against these threats by having an active firewall and installing anti-virus and anti-spyware programs and keeping them up-to-date. Fortunately, there are numerous programs that can do this and many basic versions can be installed for free. Most current Windows software versions have a basic built-in firewall and some virus and spyware protection. A more powerful program for viruses and spyware protection is provided by Grisoft. It is called AVG and a free version for home use can be found at www.grisoft.com.

It is generally not a problem to conduct transactions and provide personal information online if your computer is protected from viruses and spyware and your communication is encrypted. You can check to see if your communication is encrypted by looking at the Web address. If you see “https”, the communications with a Web site are encrypted, as the “s” stands for secure. If the “s” is not present, the communication, if seen by a third party online, provides that party potential access to sensitive information.

If you have wireless Internet, also called Wi-Fi in your home, be sure that it is protected with password access. Keeping your home network private protects it from being accessed by neighbors and others. Anything they do online on your network, including illegal activity, will be done through your network address and can be associated with you.

Finally, if you have a portable phone in your home, look on the bottom of the base for a sticker that tells the frequency the phone uses for communicating to the handsets. If the number is less than 900 Megahertz, your conversations could potentially be heard with a baby monitor or scanner in your neighborhood. For privacy consideration, you might want to get a new phone with a higher frequency that makes this more difficult.

Identity thieves often exploit electronic vulnerabilities to steal information from the unprotected and unsuspecting. Protecting your electronic communications will help ensure that you don’t become a victim.

Online advertising

More and more people are using the Internet to advertise products for sale through free services such as Craig’s List. The nature of this anonymous advertising has perpetuated fraud that has claimed many victims, including some very close personal friends.

One of the more popular frauds is called the “payment overage scam”. It targets people who advertise a product for sale. The seller receives contact from a potential buyer who sends the seller a cashier’s check for an amount that exceeds the advertised price. The buyer, making up a reason for overage, asks the seller to wire transfer the extra money back to them, so that don’t have to write another check. Since the funds from the cashier’ check are usually made available immediately, the seller, if fooled by the scam, can provide the excess funds back to the buyer. It turns out, however, that the cashier’s check is fraudulent and that the buyer has no intention of purchasing the product. The seller is out the money or “overage’ that they provided to the buyer.

Protecting your identity

When I was in college, my professors would routinely post student's grades outside their office. To protect the student's privacy, the grade would not be next to a student's name, but instead, next to the student's social security number.

Protecting privacy by posting a social security number! My have times have changed. Identity theft wasn't even a blip on our radar screen back then. Even if I thought someone stole my identity from my professor's grade list, I might have said. "You want my identity? Go ahead, it's yours. Pay back my student loans while you're busy being me."

Here are some basic tips to help keep your information safe:

1. **Protect your social security number. Don't provide it unless required and never write in on checks.** Remember the social security number is the most difficult piece of personal identifiable information for a bad guy to obtain. Don't make it easier for them.
2. **Never routinely carry your social security card, passport, or birth certificate with you.** These types of documents would be a bountiful treasure for a potential identity thief.
3. **Photocopy the front and back of all cards you carry in your wallet and store the copy in a safe place at home.** This will come in very handy if your wallet or purse is stolen. Remember that store credit card you got when you signed-up for free financing on an expensive purchase? The credit card arrived in the mail and you shoved in your wallet and didn't use it again. You may forget you had that card in your wallet and wouldn't know to cancel it upon a theft or loss of your personal items.
   Having a copy of the front and back of all your credit cards provides you easy and quick access to the card number and the toll-free number to call to cancel the card.
   Copy other important documents as well. It would be nice to know what a crook has if you are the victim of a theft. It also may surprise you to learn how many things you carry around with you.
4. **Shred your confidential trash with a cross cut or diamond cut shredder.** Don't buy or use a strip-cut shredder. They don't shred well enough. Even though I have never been in a crook's house in twenty years of law enforcement and found taped together financial statements, a person could get information from strip shredded documents. Get a cross-cut or diamond cut shredder. The pieces are too small to put back together.
5. **Don't provide personal information to anyone from an unsolicited contact over the computer, telephone or personal.** Remember the key here is "unsolicited". When someone contacts you in person, on the phone or through e-mail, never provide personal information. This may be an attempt at "phishing", a disguised attempt to obtain your personal information.
   One "phish" that has seen resurgence lately is the "jury duty scam". This occurs when a caller identifies himself as an officer of the court and says that you have failed to report to jury duty and face arrest. You know nothing about it since you never got a notice. The caller offers to clear things up by asking to provide your social security number and birth date for verification purposes. Don't be fooled by this or other "phishing" scams. They are just fraudulent attempts to obtain your personal information.
6. **Order your credit reports three times per year. You are entitled to three free reports each year, one from each credit reporting agency.** You should do this separately for yourself and all family members. Investigate any unusual activity or entries that you don't understand.
7. **Check financial accounts often and investigate any unusual activity.** It is always a good idea to scrutinize bank account and credit card transactions. Sometimes crook charge small amounts because they think it will go unnoticed.
8. **Don't leave outgoing mail with personal information in your mailbox for pick-up.** There is a lot of information about you and your accounts in an envelope containing a bill and your check. It is safer to take bills and other items containing personal identifiable information on them to the post office or drop box.

9. **Don't let mail accumulate in your box and retrieve it as soon as possible after delivery.** Your mailbox is a potential treasure trove of information. Try not to let mail accumulate for too long and investigate if any statements don't arrive on time. A crook may have stolen them and even changed the address for future deliveries.
10. **Keep personal records in your home out of sight from visitors such as cleaning crews, workers, repairman, etc.** You really don't know who may be after your identity. Sometimes identity theft is accomplished by people with legitimate access to your home. So don't take any chances.

Your credit report

It is a good idea to run a credit report on yourself and family members to determine if you have been a victim of identity theft by noting any suspicious activity in the account. A federal law, phased in completely in 2005, allows everyone to obtain a free copy of their credit report from each of the three credit reporting agencies every year. That gives each person three free credit reports per year. If you wanted to be very diligent about checking, you could order one from each agency on a rotating basis every four months and it won't cost you a dime.

The three credit reporting agencies that maintain our credit reports are Equifax, Experian and Transition. The agencies share information, but it is still a good idea to check the individual reports from each one.

The automated system to order a credit reports on the phone can be accessed by calling 1-877-322-8228.This is the number that has been set up to order a report from one or more of the three agencies. The system will prompt you to enter personal information, including your social security number. After the call, you will receive the credit reports you ordered through the mail.

I prefer to order credit reports online, so I can access the reports without having to use the mail. To do this, direct your browser to www.annualcreditreport.com. Make sure you have typed this directly into your browser window. If you do a Web search for "annual credit report", you may end up on a Web site that looks like you may be able to get a credit report for free, but you will actually be charged on the credit card they ask you to use for this "free" service.

One example is the Web site www.freecreditreport.com. This business is owned by Experian and seems to be designed to take advantage of consumers who are unaware that they are not getting a credit report for free. It is a total rip-off.

The official site that has been set up for the purpose of issuing consumers free credit reports is the aforementioned www.annualcreditreport.com. Again, you will have to provide your social security number and other information to get a copy of one or more reports, which are provided immediately through the Internet.

Once you have your credit report, you should be able to tell whether or not there have been credit accounts opened in your name without your knowledge. Any unusual activity or transactions that you don't recognize should be investigated.

Smishing

A few weeks ago, decked out in business attire and on my way to give a speech on Identity Theft, I stopped at my favorite little coffee shop along the way.

"What are you doing all dressed up?" the barista asked. "I thought you were retired."

"I'm on my way to give a speech," I replied.

“What’s the topic?” she said, loudly enough to overcome the ear piercing sound of ice being crushed for a cold drink.

“Identity Theft,” I said matter in matter of fact fashion.

“Really?” she asked rhetorically. The ice crushing stopped in mid-sentence and for a second it sounded as if she were talking through a megaphone. “Someone tried to steal my identity!”

Not missing a chance to obtain a real life, barista next door, identity theft example, I asked, “What happened?”

“Well, I starting getting these e-mails from my credit union that said there was a problem with my account and they wanted me to login to fix the problem,” she replied while deftly pressure packing espresso grounds for the perfect brew. “I didn’t pay any attention to them because I thought it was probably some scam.”

“Right,” I interrupted.

“But then I started getting the same messages on my cell phone,” she said in an exasperating fashion. “After that, I thought it was too much of a coincidence to be a scam.”

“Weird,” I blurted out, as she took a customer’s order for something with low-fat froth.

Then she started to build to the story’s inevitable climax, “So I went home and got on my computer to login through one of the e-mail messages to take care of the problem.”

This is when I started thinking that it would make a better story for my speech if she actually did provide her personal information to the identity thieves and had her bank account drained, credit accounts opened her name, a new car bought with her credit and shipped to Mexico. Good for me, bad for her. In spite of these thoughts, I still hoped for a happier conclusion.

“I provided my personal information including my pin number to the site,” she lamented. “About a day or two later, my dad told me he had seen a fraud alert on the credit union’s Web site about the scam. I called the bank and they took action before the crooks could get access to the account. I was lucky, they almost got me.”

“I’m glad for that,” I blurted, as I waited for what seemed like an eternity for someone to finish stirring their coffee so I could get access to the half and half. “Some people get fooled and it can cause a lot of problems that take a long time to fix. Besides, how would they have found a barista to replace you while you are getting your finances straight?”

She went to packing coffee beans and laughed when I told her I would use her story in my presentation, which I did because it makes a very good point, which is that crooks are very determined to get your information. Like an aggressive bacteria, they evolve and mutate to trick our self-defense. Knowledge, with a little bit of common sense thrown in is our antibiotic against these threats. To overcome this defense, phishing (general attempts to trick you), mutates into vishing (voice or phone attempts), which then further evolves into Smishing (simple text messaging attempts). In the case of the barista, a combination of attacks was the formula that worked.

It is important to remember that legitimate entities do not send unsolicited requests for personal information. If you receive one through any means of communication, never provide personal information in response. If it looks like it is from your bank, report it to them, so they can warn others.

Then you can sit back, relax and enjoy a drink made by your favorite barista.

Please see the following pages for more information about protecting yourself from fraud.

Simple Safeguards:
Identity Theft Prevention for Organizations

Presented by
FBI Special Agent Jeff Lanza
(Retired)

Physical Security

- Take stock of what personal information you have. Keep only what you need for your business.
- Records you need should be protected by layers of security. All layers, including outer building, inner office and record storage areas should be secure from unauthorized entry.
- Protect digital media with the same secure safeguards as physical records.
- Personal information inside a business should be protected during regular hours if the area is not monitored.

Computer Security

- Ensure your computer is protected with a firewall and against viruses and spyware. Update this software and operating systems on a regular basis.
- Make sure all wireless access is encrypted and accessible only through a user created strong password.
- Use strong passwords to protect computer access. Don't store passwords on computer hard drive or post near the computer.
- Employees should memorize passwords and should be required to change them every 90 days.
- Set computers to log-off automatically after a few minutes of non-use.
- Restrict the use of laptops to employees who need them to do their job.
- Limit take home laptops. If they most go home, remove or encrypt personal information from them or any other digital media that leaves the office.
- Require employees to store laptops in a secure place. Never leave a laptop visible in a car.
- Limit download capability on employee's computers.
- Make sure a Web site has 128 bit encryption before conducting transactions.

Policy - Personnel - Training

- Establish and enforce a company-wide policy related to personal information.
- Regularly train employees to be sensitive to identity theft issues and personal information protection.
- Create a culture of security by holding employees accountable to the company policy.
- Have a defined and required way to report violations and suspicious activity related to information security.
- Establish a need-to-know policy and compartmentalize personal information to only those in your company who have a legitimate need to know before granting access.
- Disconnect ex-employees immediately from access to any personal information.

Information Security

- Use secure shredders or a secure shredding service.
- If you outsource shredding, make sure the shredding company complies with security standards such as employee background checks.
- Be cautious on the phone. Positively identify callers before providing personal information.
- Don't e-mail personal information. This method is not secure.

Resources on the Web:
www.ftc.gov/privacy **www.ftc.gov/infosecurity**
www.sans.org **www.onguardonline.gov**

Speaker Information: Jeff Lanza
Phone: 816-853-3929
Email:jefflanza@thelanzagroup.com
Web Site: www.thelanzagroup.com

Simple Safeguards:
Stopping Identity Theft Before it Stops You

Presented by
FBI Special Agent Jeff Lanza
(Retired)

1. Protect Your Personal Information
- ✓ Protect your social security number. Don't provide it unless required and never write it on checks.
- ✓ Photocopy the front and back of all the credit cards you carry in your wallet and store the copy in a safe place.
- ✓ Never routinely carry your social security card, passport, or birth certificate with you.

2. Protect Your Documents
- ✓ Shred your confidential trash with a cross-cut or diamond cut shredder.
- ✓ Don't leave outgoing mail with personal information in your mailbox for pick-up.
- ✓ Retrieve mail as soon as possible after delivery and avoid leaving it in your mailbox overnight.

3. Be Vigilant Against Tricks
- ✓ Never provide personal information to anyone in response to an unsolicited request.
- ✓ Never reply to unsolicited e-mails from unknown senders.

4. Protect Your Communications
- ✓ Ensure your computer is protected against viruses and spyware and set to update often.
- ✓ If you have wireless internet, make sure it is password protected.
- ✓ Make sure your cordless phone is digital and has a frequency of at least 900MHz.

5. Check Your Credit Report
- ✓ Order your credit reports at least three times per year (free).
- ✓ Check financial accounts often and investigate any unusual activity.

To remove your name from mail and phone lists:
- www.dmachoice.org
- www.donotcall.gov (1-888-382-1222)

To stop preapproved credit card offers:
- 1-888-5-OPTOUT (567-8688)

Credit Monitoring and Identity Theft Protection
Two options to get started:
1. Talk to your insurance agent about what they offer
2. www.debix.com

To sign up for my free newsletter, e-mail a request to:
jefflanza@thelanzagroup.com

Credit Reporting Bureaus
Equifax: (800) 525-6285
P.O. Box 740241 Atlanta, GA 30374
Experian: (888) 397-3742
P.O. Box 9530 Allen, TX 75013
Trans Union: (800) 680-7289
P.O. Box 6790 Fullerton, CA 92834

Credit Reports
You are allowed 3 free reports each year; to order:
On Web: www.annualcreditreport.com
By Phone: 1-877-322-8228

To Report Internet Fraud:
www.ic3.gov

Key Numbers
FBI (202) 324-3000 or your local field office
FTC 1-877-IDTHEFT
Postal Inspection Service 1-877-876-2455
IRS 1-800-829-0433
Social Security Administration 1-800-269-0271

IF YOU ARE A VICTIM
1. Contact any one of the three credit reporting agencies and place a **fraud alert** on your account.
2. Contact affected financial institutions.
3. Contact affected creditors.

IF A LOVED ONE DIES
Send a copy of the death certificate to the three credit reporting agencies.

Web Sites referred to in presentation
online search engine to search your name
www.zabasearch.com
virus protection for your computer
Norton or McAfee Software Security Suite
to hold your mail
www.usps.com

Speaker Information:
Jeff Lanza
Phone: 816-853-3929
Email:jefflanza@thelanzagroup.com
Web Site: www.thelanzagroup.com

IFMA Knowledge Library

Want even **more Content?**

Since you're already a user, you know that IFMA's Knowledge Library offers all FM content in one place. But did you also know that by signing up via email to become a registered user, you can unlock even more resources?

Signing up via email for registered access within the Knowledge Library brings more content and functionality to your fingertips. Expect to grow your facility management knowledge, career and network faster than ever before.

REGISTER TODAY