

# **“What Every Business Owner MUST Know To Protect Against Online Identity Theft”**

**If you want to prevent your personal or business identity from being stolen by a cyber criminal, this eBook is a MUST read!**

This eBook will outline in plain, non-technical English, common mistakes that many small business owners make with their computer and network security that puts their personal information and identity at risk of being stolen. It will also further explain what identity theft is, and how you can prevent it from happening to you and your business.

## **You’ll Discover:**

- \* The top 3 ploys used by online identity thieves to easily gain access to your business & personal information and how to avoid them.
- \* 10 sneaky e-mails used to steal your identity that you should IMMEDIATELY delete if they land in your inbox.
- \* One easy, sure-fire way to keep your network and computers safe and secure from online thieves.
- \* What you need to know about the NEW scams being used to steal personal information via social media like Facebook.
- \* Best practices to prevent you or your employees from inadvertently giving away passwords and other “keys to the castle” to Internet criminals.

# **“What Every Business Owner MUST Know To Protect Against Online Identity Theft”**

## **Table of Contents**

**Chapter 1: What Is Identity Theft?.....Page 3**

**Chapter 2: How Online Thieves Get A Hold Of Your  
Information.....Page 6**

**Chapter 3: Four Things You Must Do To Protect Your  
Company.....Page 8**

**Chapter 4: A Simple And Easy Way To Ensure Identity  
Theft Doesn't Happen To You.....Page 10**

## Chapter 1: What Is Identity Theft?

### **Ever have a fraudulent charge appear on your credit card statement?**

Now imagine having your entire identity stolen. Your social security number, business ID number, access to your personal and business bank accounts, retirement accounts – swiped out from under you. Your personal and business cards can be maxed out too. What's worse, you could lose your client database, financial records, and all of the work files your company has ever produced or compiled. *That's* identity theft.

Now imagine what would happen if you had to invest an enormous amount of time, money, effort, and energy to try to restore your credit and good reputation. Think about how much your business would suffer if one day your payroll money or the money you use to pay vendors was stolen out from under you.

Or, what if an online criminal stole your identity and used it to pull off other criminal acts? Could your business survive a front page news story about how you or your company ripped off hundreds of people? Though you might be “innocent until proven guilty” in the justice system, you are “guilty until proven innocent” in the media.

### **Could You Financially Survive If Your Business And Personal Identity Were Stolen?**

Many small business owners tend to ignore or simply don't know about taking steps to secure their personal and company information on their network from online hijacks. By then it's too late and the damage is done.

#### **But That Could Never Happen To Me!** *(And Other Lies Business Owners Like To Believe About Their Personal & Business Identity...)*

About 1 in every 30 people will experience identity theft every year. And with new and clever technologies developing all the time, this number could increase.

While it may be difficult to determine the actual financial impact identity theft would have on your business, you can't deny the fact that it would have a negative effect. Cash most definitely IS king. And if yours is stolen and used by a cyber criminal, the emotional toll such an event would have on you personally would certainly impact your business, even if you haven't put a pencil to figuring out the exact cost.

#### **Take a look at these statistics...**

- As many as 9 million Americans have their identities stolen every year. *(Source: The United States Federal Trade Commission)*

- The dollar amount of identity fraud over the last two years totals over \$100 Billion. *(Source: Javelin Strategy and Research)*
- 11.6% of all identity theft (over 1,000,000 cases) occurs online (with the remainder of personal information being stolen by more traditional methods like stealing wallets or overhearing a social security number). *(Source: Javelin Strategy and Research)*
- It takes the average victim of identity theft more than 600 hours – that’s equivalent to **nearly 3 months of 40 hour work weeks** – to clear their name and clean up the fraud conducted with their personal information. *(Source: Javelin Strategy and Research)*
- Because identity theft and Internet fraud are often misclassified crimes, a culprit has only a 1 in 700 chance of being caught by the federal government. *(Source: Gartner Survey, 2003)*
- Cyber-criminals stole an average of \$900 from each of 3 million Americans in the past year, and that doesn't include the hundreds of thousands of PCs rendered useless by spyware. *(Source: Gartner Group)*

## **Why Small Business Are Especially Vulnerable To Identity Theft**

With the constant changes to technology and the daily development of new threats, it takes a highly-trained technician to secure even a simple 3 to 5 person network; however, the cost of hiring a full-time, experienced technician is just not feasible for most small business owners.

In an attempt to save money, most try to do their own in-house IT support and designate the person with the most technical expertise as the part-time IT manager. This never works out because this makeshift IT person has another full-time job to do and is usually not skilled enough to properly support an entire computer network anyway.

This inevitably results in a network that is ill-maintained and unstable. It also means that the backups, virus updates, and security patches are not getting timely updates, giving a false sense of security.

It’s only a matter of time before an online hacker finds his way into your network and steals your information. If you’re lucky, it will only cost you a little downtime; but there’s always a chance you could end up like the companies affected by these criminals...

### **\$764,000 Stolen From Insurance Company**

A man was indicted, pleaded guilty to federal charges and was sentenced to 27 months' imprisonment for obtaining private bank account information about an insurance company's policyholders and using that information to deposit \$764,000 in counterfeit checks into a bank account he established.

### **Social Security Number Swiped From A Web Site**

A defendant has been indicted on bank fraud charges for obtaining names, addresses, and Social Security numbers from a Web site and using the data to apply for a series of car loans over the Internet.

### **\$13,000 Drained From This Business Owner's Account**

A woman was indicted and pleaded guilty to federal charges involving her obtaining a fraudulent driver's license in the name of the victim, using the license to withdraw more than \$13,000 from the victim's bank account, and obtaining five department store credit cards in the victim's name and charging approximately \$4,000 on those cards.

## Chapter 2: How Online Identity Thieves Get A Hold Of Your Information

Some identity theft does occur through more “old-school” methods such as stealing your wallet, raiding your business files, overhearing you give a credit card or social security number over the phone, or even raiding your business file cabinet. However, common-sense tactics such as avoiding public conversations that involve your personal or business financial information or putting locks on your file cabinets can be used to combat those threats.

Internet threats, on the other hand, are much more sophisticated and involve greater “know-how” in order to prevent them.

There are 3 basic ways cyber criminals gain access to your personal information over the web. They are:

**1. Phishing** – Phishing is where online scammers send spam or pop-up messages to your computer and try to get you to provide personal or sensitive business information over the web. Online criminals will typically send messages that look like legitimate messages from your bank, credit card company, or other financial institution. In the message, there is usually a web site link where it asks you to update your contact information.

Many of these websites look like EXACT replicas of your bank or credit card website. However, entering your information into one of these sneaky portals means you are handing over the keys to the castle to a complete “evil-doer.”

The Internet thief can now use your personal information to gain access to other private accounts, raid your business, and rack up thousands of dollars in faulty charges.

**2. E-mail Scams** – Offers, detailed sales pitches, links to informational websites. These seemingly harmless e-mails are actually the makings of an Internet crime. They’ll ask for your credit card information to buy a fake product, or to pay for shipping on a “free” gift.

The most common e-mail scams used to steal your identity are (as found on [www.onguardonline.gov](http://www.onguardonline.gov)):

*The “Nigerian” Email Scam.* Con artists claim to be officials, businesspeople, or the surviving spouses of former government honchos in Nigeria or another country whose money is somehow tied up for a limited time. They offer to transfer lots of money into your bank account if you will pay a fee or “taxes” to help them access their money. If you respond to the initial offer, you may receive documents that look “official.” Then they ask you to send money to cover transaction and transfer costs and attorney’s fees, as well as blank letterhead, your bank account numbers, or other information. They may even encourage you to travel to the

country in question, or a neighboring country, to complete the transaction. Some fraudsters have even produced trunks of dyed or stamped money to try to verify their claims.

**The Catch:** The emails are from crooks trying to steal your money or your identity. Inevitably in this scenario, emergencies come up requiring more of your money and delaying the "transfer" of funds to your account. In the end, there aren't any profits for you, and the scam artist vanishes with your money. The harm sometimes can be felt even beyond your pocketbook: according to State Department reports, people who have responded to "pay in advance" solicitations have been beaten, subjected to threats and extortion, and in some cases, murdered.

*Phishing E-mail Scam.* Email or pop-up messages that claim to be from a business or organization you may deal with – say, an Internet service provider (ISP), bank, online payment service, or even a government agency. The message may ask you to "update," "validate," or "confirm" your account information or face dire consequences.

**The Catch:** Phishing is a scam where Internet fraudsters send spam or pop-up messages to reel in personal and financial information from unsuspecting victims. The messages direct you to a website that looks just like a legitimate organization's site, or to a phone number purporting to be real. But these are bogus and exist simply to trick you into divulging your personal information so the operators can steal it, fake your identity, and run up bills or commit crimes in your name.

*Work-at-Home Scam.* Advertisements that promise steady income for minimal labor – in medical claims processing, envelope-stuffing, craft assembly work, or other jobs. The ads use similar come-ons: Fast cash. Minimal work. No risk. And the advantage of working from home when it's convenient for you. **The Catch:** The ads don't say you may have to work many hours without pay, or pay hidden costs to place newspaper ads, make photocopies, or buy supplies, software, or equipment to do the job. Once you put in your own time and money, you're likely to find promoters who refuse to pay you, claiming that your work isn't up to their "quality standards."

**3. Spyware** - Spyware is software installed on your computer without your consent to monitor or control your computer use. Clues that spyware is on a computer may include a barrage of pop-ups, a browser that takes you to sites you don't want, unexpected toolbars or icons on your computer screen, keys that don't work, random error messages, and sluggish performance when opening programs or saving files. In some cases, there may be no symptoms at all.

## Chapter 3: Four Things You Must Do To Protect Your Company

While it's impossible to plan for every potential scenario, a little proactive planning and proper network precautions will help you avoid or greatly reduce the impact of the vast majority of cyber identity theft you could experience.

### **Step#1: Make Sure Your Backups Are Encrypted.**

It just amazes me how many businesses don't have the security of encrypted backups. Encryption takes every little key stroke that you type and every little piece of data in your computer and turns it into dozens...or hundreds of other characters. For example, just one letter "A", could turn into 256 different letters, numbers and symbols when it is encrypted. It basically makes it a whole lot more difficult for a hacker to figure out what the data is. On the other hand, if you DON'T have encryption, you are opening yourself up to a BIG risk of your identity and other important data being swiped. That is why it is so important to make sure your backup is properly secured.

### **Step #2: Make Sure Your Virus Protection Is ALWAYS On AND Up-To-Date**

You would have to be living under a rock to not know how devastating a virus can be to your network. With virus attacks coming from spam, downloaded data and music files, instant messages, web sites, and e-mails from friends and clients, you cannot afford to be without up-to-date virus protection.

Not only can a virus corrupt your files and bring down your network, but it can also hurt your reputation. If you or one of your employees unknowingly spreads a virus to a customer, or if the virus hijacks your e-mail address book, you're going to make a lot of people very angry.

### **Step #3: Set Up A Firewall & Update It Regularly**

Small business owners tend to think that because they are "just a small business," no one would waste time trying to hack in to their network, when nothing could be further from the truth. I've conducted experiments where I connected a single computer to the Internet with no firewall. Within hours, over 13 gigabytes of space was taken over by malicious code and files that I could not delete. The simple fact is that there are thousands of unscrupulous individuals out there who think it's fun to steal your personal information just because they can.

These individuals strike randomly by searching the Internet for open, unprotected ports. As soon as they find one, they will delete files or download huge files that cannot be deleted, shutting down your hard drive. They can also use your computer as a zombie for storing pirated software or sending spam, which will cause your ISP to shut YOU down and prevent you from accessing the Internet or sending and receiving e-mail.

If the malicious programs can't be deleted, you'll have to re-format the entire hard drive causing you to lose every piece of information you've ever owned UNLESS you were backing up your files properly (see 1 to 3 above).

#### **Step #4: Update Your System With Critical Security Patches As They Become Available**

If you do not have the most up-to-date security patches and virus definitions installed on your network, hackers can access your computer through a simple banner ad or through an e-mail attachment.

Not too long ago Microsoft released a security bulletin about three newly discovered vulnerabilities that could allow an attacker to gain control of your computer by tricking users into downloading and opening a maliciously crafted picture. At the same time, Microsoft released a Windows update to correct the vulnerabilities; but if you didn't have a process to ensure you were applying critical updates as soon as they became available, you were completely vulnerable to this attack. It is an EASY way for someone to gain access to your information and steal your identity.

Here's another compelling reason to ensure your network stays up-to-date with the latest security patches...

Most hackers do not discover these security loopholes on their own. Instead, they learn about them when Microsoft (or any other software vendor for that matter) announces the vulnerability and issues an update. That is their cue to spring into action and they immediately go to work to analyze the update and craft an exploit (like a virus) that allows them access to any computer or network that has not yet installed the security patch.

In essence, the time between the release of the update and the release of the exploit that targets the underlying vulnerability is getting shorter every day.

When the "nimda" worm was first discovered back in the fall of 2001, Microsoft had already released the patch that protected against that vulnerability *almost a year before* (331 days). So network administrators had plenty of time to apply the update. Of course, many still hadn't done so, and the "nimda" worm caused lots of damage. But in the summer of 2003 there were *only 25 days* between the release of the Microsoft update that would have protected against the "blaster" worm and the detection of the worm itself!

Clearly, *someone* needs to be paying close attention to your systems to ensure that critical updates are applied as soon as possible. That is why we highly recommend small business owners without a full-time IT staff allow their consultant to monitor and maintain their network.

## Chapter 4: A Simple And Easy Way To Ensure Identity Theft Doesn't Happen To You

If you are sitting there thinking, "This all sounds great, but I don't have the time or the staff to handle all of this work," I've got the solution.

Thanks to a service we offer called, "GridWatch", we can completely take over the day-to-day management and maintenance of your computer network and **free you from expensive, frustrating computer problems, downtime, and security threats**, AND PROTECT YOUR IDENTITY from being stolen online. You'll get all the benefits of a highly-trained, full-time IT department at only a fraction of the cost.

*And here is the best part...*

**In most cases, we can cut your IT support costs by 30% to 50% WHILE improving the reliability and performance of your network and eliminating spyware, spam, downtime, and other computer frustrations!**

### The Benefits Are Obvious:

- **You'll eliminate expensive repairs and recovery costs.** Our network monitoring and maintenance will save you money by preventing expensive network disasters from ever happening in the first place. As a matter of fact, we guarantee it.
- **You'll avoid expensive trip fees while receiving faster support.** Our remote monitoring software will enable us to access and repair most network problems right from our offices. No more waiting around for an engineer to show up!
- **How does faster performance, fewer "glitches," and practically zero downtime sound to you?** Under this program, that is exactly what we'll deliver. Some parts of your system will degrade in performance over time, causing them to slow down, hang up, and crash. Our preventative maintenance and network monitoring will make sure your computers stay in tip-top shape for maximum speed, performance, and reliability.
- **You will have ALL of the benefits of an in-house IT department WITHOUT all of the costs.** As a Managed Network Service Plan customer, you'll have access to a knowledgeable support staff that can be reached immediately should you have any kind of problem or question.

- **You'll receive substantial discounts** on IT services that you are already buying. Most IT firms will nickel and dime you over every little thing they do; under this program, you'll pay one flat, affordable rate and get all of the technical support you need. No hidden charges, caveats, or disclaimers.
- **You will never have to fear a big, expensive network repair bill.** Instead, you can budget for network support just like rent or insurance.
- **You'll sleep easier** knowing the "gremlins at the gate" are being watched and kept out of your network.
- **You'll safeguard your data.** The data on the hard disk is always more important than the hardware that houses it. If you rely on your computer systems for daily operations, it's time to get serious about protecting your critical, irreplaceable electronic information.
- **You'll finally put a stop to annoying spam, pop-ups, and spyware** taking over your computer and your network.
- **You'll gain incredible peace of mind.** As a business owner, you already have enough to worry about. We'll make sure everything pertaining to your network security and reliability is handled so you don't have to worry about it.

## **How Safe Is YOUR Identity? FREE Network Security Audit Reveals The Truth**

Hopefully this eBook acted as an eye opener to all small business owners who are not adequately protecting their data and computer network. If you are not doing the 4 steps outlined in this eBook, your network is an accident waiting to happen and the most important thing for you to do now is take immediate action towards protecting yourself.

One of the biggest, costliest mistakes you can make is to ignore this advice with the false hope that identity theft could never happen to **you**.

Because you have taken the time to request and read this eBook, I would like to offer you a FREE Network Security Audit. Normally I charge \$270 for this service, but as a prospective GridWatch client, I'd like to give it to you for free as a way of introducing GridWatch to your company.

During this audit one of our trained technicians will come onsite and...

- ✓ **Pinpoint any exposure to or risk** from hackers, viruses, spyware, spam, data loss, power outages, system downtime, and even employee sabotage. This analysis will assess YOUR risk of identity theft.

- ✓ **Review your system backups** to make sure the data CAN be recovered in case of a disaster. You don't want to discover that your backups were corrupt AFTER a major disaster wiped out your network.
- ✓ **Scan your network for hidden spyware and viruses** that hackers "plant" in your network to steal information, deliver spam, and track your online activities.
- ✓ **Look for hidden problems that cause error messages, slow performance, and network crashes.**
- ✓ **Answer any questions you have** about your network or keeping it running problem free. I can also give you a second opinion on any projects you are considering.

## **There Are No Strings Attached, But You Have To Hurry...**

As you might have guessed, I cannot extend this offer forever, because time and staff limitations simply won't allow it.

If you want to say goodbye to your computer problems, protect your personal and business identity and stop worrying about the security of your data from hardware failures, viruses, hackers, and other threats, then you'll want to sign up right now for this Free Network Security Audit.

There is absolutely no obligation or pressure for you to buy anything, or to ever use our services again. As I stated earlier, this is simply an easy way for us to demonstrate how we can help your business at no risk to you.

### **How To Secure Your Free Network Security Audit**

1. Fill in and fax back the enclosed request form.
2. Call me direct at 703-968-2600
3. Send an e-mail to [msherman@csuinc.com](mailto:msherman@csuinc.com) with the words, "Security Audit" in the subject line. Be sure to include your company name, address, and phone number so I can follow up with you.

Good Networking,  
Michelle Sherman  
President  
Computer Services Unlimited  
703-968-2600  
www.csuinc.com



[www.csuinc.com](http://www.csuinc.com)

Phone: 703.968.2600

14240-G Sullyfield Circle, Chantilly, VA 20151

Fax: 703.968.5562

**P.S.** Please note that this offer for a **FREE Security Audit won't be around forever.** While we would love to be able to give these away to everyone, staff and time limitations simply won't allow it. That's why you must respond to this offer by the date stamped on the enclosed fax-back form today.

You have my word that you will not be under any pressure or obligation to buy anything, or to ever use our services again.



www.csuinc.com

Phone: 703.968.2600

14240-G Sullyfield Circle, Chantilly, VA 20151

Fax: 703.968.5562

## **“Yes! I Want To Make Sure My Network And Company’s Data Are Safe From Harm So I Can Prevent Identity Theft From Happening To Me”**

**Please sign me up for a FREE Security Audit so I can make sure I am doing everything possible to secure my network.** I understand that I am under **no obligation** to do or to buy anything by requesting this audit. I further understand that these audits are being made available on a **first-come, first-served** basis.

### **Please Complete And Fax Back:**

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Company: \_\_\_\_\_

Address: \_\_\_\_\_

City: \_\_\_\_\_ ST: \_\_\_\_\_ Zip: \_\_\_\_\_

Phone: \_\_\_\_\_ Fax: \_\_\_\_\_

E-mail: \_\_\_\_\_

Number of PCs: \_\_\_\_\_

Operating System: \_\_\_\_\_

**Fax To: 73-968-5562**

**Call Me Direct At: 703-968-2600**

This form **MUST** be completed and faxed back to our offices by: **December 31, 2011**

## Here's What Our Clients Are Saying About Us:

I am so relieved to be rid of unexpected downtime. I don't worry anymore about our computer network and all the irreplaceable data we have on it.

Our network is stable with CSU. We have eight different locations and our end users can email a problem to CSU, it immediately turns into a ticket in their system and is assigned to a network engineer.

I have the peace of mind knowing I have someone to call who will get us back up and running ASAP if something does go down. I feel I can trust Computer Services Unlimited to do what's right for my company. You don't find that with all IT firms."

*Katie Newbold, LVT, Practice Manager  
Chesapeake Veterinary Cardiology Associates*

**Almost 3 years ago Inova Fairfax Hospital Gift Shops and Treasure Trove thrift/consignment stores signed a contract for the CSU GridWatch Program. Our network holds a lot of critical data that would be devastating to us if we lost it. The GridWatch program is fantastic! It alerts CSU to any potential problems on our network so that CSU can proactively take care of the situation before it becomes a huge problem. CSU is constantly monitoring our systems to make sure that nothing goes wrong that would jeopardize the security of our data and our records. This enables us to remain productive and continue our sales with no downtime.**

**Sally Freedenthal, Senior Retail Manager  
Inova Fairfax Hospital**

### **"Our Network is Monitored and Supported 24/7"**

"The biggest reason I use Computer Services Unlimited is for the peace of mind they give me. The entire burden of computer support is taken off my back, and I don't have to worry about security threats or downtime. Their GridWatch service automatically monitors our servers, the logs, and the health of our network 24/7/365 to make sure everything is running properly and to make sure lower-level maintenance on the network is getting done. Now we are getting regular Microsoft updates, virus updates, spyware is

being scanned and removed, the temporary files are getting cleaned up, and our backups are being taken care of. It's really helped speed up our network, our programs run better, and we don't have the recurring problems that we had in the past. Plus, there is a live person behind that service that alerts me to anything that isn't right.

For a growing medical practice like ours, GridWatch just makes sense. It gives me the real necessity of support I need at a very fair price. I have to run my medical practice and maintain my focus on keeping our patients happy and the income coming in. That takes precedence over removing temp files or scanning for spyware. But you can't ignore those things either or they will come back and develop into bigger problems. The support provided through CSU's GridWatch takes that worry off my mind. It's really rare to find an IT support company that caters to the small business owner like me."

*Paul P. Boccone, J.D., LL.M.  
Chantilly Specialists*