PCPC
KNOWLEDGE IS POWER

# What every business owner must know to protect against online identity theft

## Want to prevent your personal or business identity from being stolen by a cybercriminal? *This is a must-read!*

We're going to use plain English to outline common mistakes made by many small business owners regarding computer and network security, which leave important information exposed and at risk of theft. We'll explain exactly what identity theft is, and how you can prevent it from happening to you.

### You'll Discover:

- The top three ploys used by online identity thieves, and how to avoid them
- Ten sneaky identity-theft emails you should immediately delete
- The number one way to keep your network and computers safe and secure
- The lowdown on new scams being used on social media
- Best practices to prevent inadvertently exposing personal or business passwords

# Table of Contents

# Chapter 1: What Is Identity Theft?

## Ever found a fraudulent charge on a bank statement?

Now imagine having your entire identity stolen—your social security number, business ID, banking, insurance and retirement account access—all in someone else's control. Credit cards charged, too. What about your client database, business filing records, and every work file your company has ever produced or compiled. *That's* identity theft.

Now picture investing an unthinkable amount of time, money, and energy to restoring your credit and good reputation. Imagine how much your business would suffer if payroll or vendor funds were suddenly at zero!

Or, what if an online criminal stole your identity and used it to mask other criminal acts? Could your business survive the front-page news story that comes next? 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 identity were stolen?

Many small business owners ignore, delay or are unaware of the necessary steps to secure personal and company information against online hijacks. Unfortunately, when it happens, the damage is already done.

## But that could never happen to me!

### *...and other lies business owners tell themselves about cyber security*

About one in thirty people will experience identity theft each year. With new and clever technologies developing all the time, this number could *increase*.

While it may be difficult to determine the financial impact identity theft would have on your business, you can't deny that it would likely be negative. They say, "Cash *is* king." If your cash were stolen by a criminal, it will impact your business, even if you haven't done the math.

## 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 million 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 — or to **nearly 3 months of 40-hour workweeks**—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)*
- Cybercriminals **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 computers rendered useless by malicious spyware. *(Source: Gartner Group)*

## Why small businesses are especially vulnerable

With the constant changes in technology and the daily development of new threats, it takes a highly trained technician to secure even a basic 5 to 10-person computer network. However, the cost of hiring a full-time, experienced technician is not always a feasible solution for small business owners.

In an attempt to save money, many businesses 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 the stand-in IT person has another full-time job to do, and is usually not skilled enough to properly support an entire computer network.

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 a way into your network and steals your information. If you're lucky, it will only cost you a little downtime, but take a look at the some real examples of what the damage can do:

## $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 website

*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 your details

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 three basic ways cybercriminals gain access to your personal information over the web:

### 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 criminal!

The Internet thief can now use your information to access other private accounts, raid your business, and rack up thousands in illegal transactions.

**Look out!** Some scammers will even phish by telephone to get your details.

**Tech Support Scams:** *Scam artists are using the phone to try to break into your computer. They call, claiming to be computer techs associated with well-known companies like Microsoft. They say they have detected a virus or malware on your computer to trick you into giving them remote access or paying for software you don't need.*

**The Catch:** These scammers take advantage of your reasonable concerns about viruses and other threats. They know computer users have heard repeatedly that it's important to install security software. However, their elaborate scheme isn't to protect your computer—it's to take your money.

## 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)*

**The "Nigerian" E-mail 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 remarkably official. Then, they ask you to send money to cover transaction and transfer costs and attorneys' 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 e-mails 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.

**Phising E-mail Scam:** *E-mail 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 web site 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.

## 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 ways to better 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 keystroke 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 virus protection is 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 and 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 into their network. Nothing could be further from the truth.

Experiments have been conducted where a single computer was connected to the Internet with no firewall. Within minutes, over 13 gigabytes of space were taken over by malicious code and files that could not be deleted. The simple fact is that there are thousands of unscrupulous individuals out there who make a pastime of stealing 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 reformat 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 system security patches as they become available

If you don’t 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. Out-of-date patches are 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. These days, these vulnerabilities are uncovered and exploited in mere hours or at most a few days!

## Headline news: "Meltdown" and "Spectre" security risks

You couldn't have missed the recent news about these two malicious security risks. These breaches have been well-documented (see documentation here by the Graz University of Technology), and yet nearly all devices are vulnerable.


Clearly, it's important 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 that organizations with no full-time IT staff allow their consultant to monitor and maintain their network.

# Chapter 4: How to keep identity theft from happening to *you*!

You may be thinking, "This all sounds great, but I don't have the time or the staff to handle all this work."

At PCPC, we recently rolled out a new group of remote monitoring and security services for our long-time existing client organizations. The scalable tiers have been well-received in both price and quality.

We'd like to suggest an MSP (Managed Services Provider) package as a solid way to enhance your existing IT solutions, and begin working with PCPC as your new, trusted off-site IT team.

## What will signing up for an MSP package entail?

Our skilled technicians will oversee the day-to-day management and maintenance of your computer network and free you from expensive, frustrating computer problems, downtime and security threats. Plus great savings!

> ***You'll get all the benefits of a highly trained IT department at only a fraction of the cost.***

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

Take a look at the full list of MSP benefits on the following page!

# A complete list of MSP benefits:

- **You'll prevent 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.

- **You'll avoid unneeded service travel 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 and fewer glitches" 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 help your computers stay in tip-top shape for speed, performance and reliability.

- **You will have the benefits of an in-house IT department without all of the costs.** As a Managed Service Plan customer, you'll have access to state-of-the-art ticketing system for a fast response to your IT requests, and all calls to PCPC are answered by our friendly in-office team.

- **You'll receive substantial discounts** on IT services that you are already buying. Pay an affordable rate at the tier you select, and get the support right for your business size.

- **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. Once-a-day backups will not avoid losing a full day's work!

- **You'll finally put a stop to annoying spam, pop-ups and spyware** taking over your computer screens 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 right now?

## Get our FREE network security audit today!

Hopefully this e-book has been an eye-opener about adequately protecting your organization's data and computer network.

If your organization is not doing the four steps outlined here, your network may be an accident waiting to happen, and the next step is to take immediate action toward protecting yourself.

Because you have taken the time to request and read this informational booklet, we would like to offer you a **Free Network Security Audit**. Normally, we charge for this service, but as a new MSP client, you're eligible at no cost, as a way of introducing our MSP offerings to your organization.

## During this audit one of our experienced technicians will...

- ✓ **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" 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. We can also give you a second opinion on any projects you are considering.

# We're offering our Free Security Audit for a limited time only!

We'd like to extend this offer for this limited time, to give NYC organizations and businesses a chance to meet our team and experience our time-tested customer service, firsthand.

## There's no obligation to purchase our services to participate.

**Three ways to sign up today:**

1. Online form - Follow this link to register now.
2. Email us - info@pcpc.tech and let us know your interested.
3. Call us direct - Dial **212-315-0809** and mention this booklet!

**Take me to the sign-up form!**

# What our clients are saying about PCPC:

## Thoughtful

PCPC's dedicated staff and unique team coverage enabled us to realize a smooth move and to upgrade our infrastructure in line with the exciting changes at BTQ.

***David Terrio,***
*President, BTQ Financials*

## Reliable

In 33 years, we encountered a number of problems of course - and - our system was never down for more than 24 hours. Mike and his staff were on call and ready, willing and able to get us back up and running quickly.

***Bob Dellacona,***
*CEO, Maid*

## Trustworthy

PCPC's response was immediate as we'd come to expect. It confirmed our choice to be their client for 20 plus years.

***Pat Lynch,***
*General Manager, Lynch, Rowin, Esq.*

## Adaptive

We have maintained our relationship with PCPC, becoming early clients, and relying totally on Michael and his capable staff to keep us functional and operational in the ever-changing cyber world.

***Mary Ann Rothman,***
*Executive Director, CNYC Inc.*