WHAT YOU MUST KNOW ABOUT PROTECTING YOUR BUSINESS AGAINST ONLINE THEFT

How to prevent your client, personal, and business data from being stolen

DATACORPS
TECHNOLOGY SOLUTIONS

In this e-book we're going to teach you something you don't already know.

We're going to show you how, in non-technical terms, you can avoid putting your client, business, and personal information and identity at risk of being stolen. In this e-book you'll learn:

- The top 3 tactics used by online thieves which allow them to gain access to your information.
- 10 shady ways that thieves get your data using email.
- The one surefire way to keep your network and computers safe.
- What you need to know about scams being used to steal personal information via social media platforms.
- Best practices to implement that prevent your employees from giving away passwords and other sensitive data.

What Every Business Needs To Know About Protecting Against Online Theft

Contents

What Every Business Needs To Know About Protecting Against Online Theft 3

Chapter 1: Identity Theft Defined 4

Chapter 2: How Thieves Steal Your Information 7

Chapter 3: Four Must-Do's To Protect Your Company 10

Step #1: Encrypt Your Backups 10

Step #2: Make Sure Your Managed Anti-Virus Protection Is Up-To-Date 11

Step #3: Crate and Update a Corporate Firewall 11

Step #4: Update Your System With Critical Security Patches 12

Chapter 4: Easy Ways to Ensure Identity Theft Doesn't Happen 14

FREE Network Security Audit 15

Chapter 1:
Identity Theft Defined

Ever have a fraudulent charge appear on your credit card statement? That's identity theft. Ever have things like your social security number, tax ID, or business financials, get into the hands of people they shouldn't? That's identity theft.

Now imagine having things that are valuable to you, swiped right out from underneath your nose, without your even knowing about it until it's too late. What's worse is you could potentially lose your client data. Data that's important to your customers or clients could be compromised as well. That's identity theft.

Imagine what would happen if you had to invest time, money, and effort to restore your business credit and reputation. That's a lot of time spent that you won't ever get back. Now consider how much your business would suffer if the finances you use for payroll purposes was stolen, as well. What would you do if your company resources were gone, and you couldn't pay your vendors? Or worst case scenario, what if a cyber-criminal stole your identity and used it to pull off other nefarious acts? Could your business survive a bad season of negative PR from a story about how you, or your business, ripped off other innocent people? You might be innocent until proven guilty, but the media is ruthless and cruel. You'll be guilty the minute this nightmare story breaks.

The last question you need to ask yourself is could you survive, financially, if your business data were stolen? Many business owners ignore taking action to protect and secure their personal and company information. Often times, we've found that businesses are not prepared to properly prevent their networks from being exposed from online attacks. They often think 'that could never happen to me.' We meet business owners all the time that don't think about the big picture, and more importantly, how they'd survive if their business information was compromised.

Some eye-opening statistics about identity theft:

- Over 9 million Americans have their identities stolen every year, according to the U.S. Federal Trade Commission.
- Identity fraud cost consumers more than $100 billion dollars over the last two years, according to Javelin Strategy and Research.
- 11.6% of all identity theft occurs online, according to the same report by Javelin Strategy and Research.
- It takes more than 600 hours, on average, for someone who's had their identity stolen to clear their name and clean up the fraud conducted with their information. (Javelin Strategy and Research)
- 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 PCs rendered useless by spyware. (Source: Gartner Group)
- Over 60% of cyber attacks are aimed at small businesses

Why Your Business Is Vulnerable To Identity Theft

With changes to technology and the creation of new threats to steal your identity, you need to be vigilant. It takes a skilled technician many hours each day to secure even a few computers that are operating on your network. However, the cost of hiring an experienced technician on a full-time basis is just not feasible for most small business owners.

The DIY approach will kill a business when trying to secure their precious data. This is where we've seen businesses fail. They try to do it on their own, attempting to complete an in-house IT security process that just won't work out the way they expected. This inevitably results in a network that is not prepared, doesn't have the proper backups, is ill-equipped by a lack of virus updates, as well as security patches that are out of date ultimately giving everyone a false sense of security. It's only a matter of time before an online hacker finds a way into your network. If you're lucky, it will only cost you a little downtime.

Chapter 2:
How Thieves Steal Your Information

Some identity theft occurs through old-school methods, as opposed to some sophisticated means. Things like stealing your wallet, raiding your business files, taking payment data from your file cabinet, and overhearing you give a credit card number over the phone, do still happen. The best way to avoid these scams is through common sense. Avoid public conversations that involve your personal or business financial information. And put locks on your file cabinets so you don't end up a statistic.

Threats online, however, are more sophisticated. The following are 3 basic types of threats that cyber-criminals will use to gain access to your information over the web.

Phishing

Phishing is where scammers send spam or messages via email to try and get you to give them personal or sensitive business information. Cyber-criminals typically send carefully crafted email messages, or messages via social media sites that resemble legitimate messages from people you know and trust, such as your bank, a friend, or a business partner. These messages will attempt to "phish" banking information, credit card numbers, or other financial data. In the message, there's usually some sort of link that you're asked to click on. When you click this link, scammers have got you.

The thief who took your info can now use your information to gain access to other private accounts, raid your business, and potentially rack up thousands of dollars in fraudulent charges.

Another type of phishing scam is when cyber-criminals try to break into your computer, over the phone. They'll call you and pretend to be someone they're not. They'll claim to be a computer technician that's associated with well-known companies like Microsoft. They'll tell you that they've detected a virus or malware on your computer only to trick you to into giving them remote access of your pc, or trick you into paying for software you don't need.

Here's the catch: scammers take advantage of you. They take advantage of your trusting nature by stating reasonable concerns about viruses and other threats, so you ultimately get duped into their evil plan. Their goal the whole time is simply take your money.

E-mail Scams

Links to web sites are the most common way we see this happening. Here's how this works, first you get an innocent looking email in your inbox. What looks harmless is actually the makings of a crime, as the link in the email will ask you to unknowingly click on this link to update your information, buy this product, or something similar.

One of the most common, and widely publicized email scams, is the infamous Nigerian Email Scam. Con artists claim to be "officials" and ask those who receive their emails to give money for a certain cause. 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. Here's the catch: these emails are from crooks. They are trying to steal your money and your identity. In the end, there aren't any profits for you, and the scam artist vanishes with your money. 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.

Spyware

Spyware is software installed on your computer without your consent. This nasty software monitors or controls your computer use. Clues that spyware may be installed on your computer may include a barrage of pop-ups that randomly show up on your system, or a browser that takes you to sites you don't want to. Spyware may also mess with your toolbars, muck up the icons on your computer screen, and cause certain keys not to work. Spyware can also display random error messages on your screen while causing sluggish performance when opening certain programs.

Chapter 3:
Four Must-Do's To Protect Your Company

It's impossible to plan for every potential scenario. We know that, but by being proactive ahead of time you can avoid much of the negative impact of the vast majority of cyber-theft.

Step #1: Encrypt Your Data

Having data secured on a server at your business is one thing, but actually encrypting it is another. Most businesses don't have a good security process for encrypting their systems. Encryption takes very little time to do and adds tons of value by being proactive about protecting your data. Encrypting your data makes it nearly impossible for hackers to unscramble it, should they potentially access it. If a situation arises where a cyber-criminal gains access to your data, and you don't have encryption, you are opening yourself up to a huge risk of your identity and other important data being swiped. It's important. Take time to ensure your data is properly encrypted.

Step #2: Make Sure Your Anti-Virus Protection Is Managed and Up-To-Date

Not having a managed anti-virus solution can be devastating to your network. Whether you know it or not, attacks are coming from spam, downloaded data, and music files, instant messages, web sites and even emails. With potential attacks you can't afford to be without up-to-date virus protection that also alerts to potential trouble.

Not having an up-to-date anti-virus can put your data at risk for corruption and bring down your network. Additionally, it can hurt your reputation if an attack occurs and your customers or clients learned about it. So make sure you have a plan and process to deploy anti-virus and keep it up to date, indefinitely.

Step #3: Install and Maintain a Commercial-Grade Firewall

Small business owners tend to think they're immune to someone hacking their network and taking their data. But nothing could be further from the truth. We conducted an experiment where we connected a single computer to the internet with no firewall. Within minutes, over 13 gigabytes of data was taken by malicious code and files that we could not delete. The simple fact is that there are thousands of unscrupulous individuals out there who think it's fun to steal your information.

These individuals strike randomly by searching the internet for open, unprotected points of access. As soon as they find one, they delete files or download huge files that cannot be deleted, shutting down your system. 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. And if the malicious programs can't be deleted, you'll have to reformat the entire hard drive. This will cause you to lose every piece of information you've ever owned, unless you were backing up your files properly. Get a firewall. Test it. Make sure you're protected.

Step #4: Update Your System With Critical Security Patches

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. 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 don't discover these security loopholes on their own. Instead, they learn about them when Microsoft (or another software vendor) 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. 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 to allow an outsourced IT company to monitor and maintain their network.

Chapter 4:
Easy Ways to Ensure Identity Theft Doesn't Happen

If you're thinking, "This sounds great, but I don't have the time or the staff to handle all of this work," we've got the solution for you. We created a service designed with you in mind that can take over the day-to-day management and maintenance of your computer network. This packaged service frees you from expensive and frustrating computer problems. This product ensures you'll have little downtime and security threats. And it protects 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.

Here's the best part: we can cut your IT support costs by over 30% while improving the reliability and performance of your network. Here are some other benefits:

☑ Eliminate expensive repairs and recovery costs.

☑ Receive faster support through remote monitoring.

☑ Experience the nirvana of faster performance, fewer glitches, and little downtime.

☑ Get all the benefits of an in-house IT department without the high payroll cost.

☑ Receive discounts on software, hardware, and other IT services that you are already buying.

☑ Predictable monthly costs so you can effectively budget.

☑ Sleep easier by knowing your data is safe.

☑ Put an end to annoying spam, pop-ups, malware, and spyware.

FREE Network Security Risk Profile

Hopefully we educated you through this ebook by opening your eyes to all the technology challenges a small business owner faces.

And if you happen to be one of the many businesses not doing the steps outlined in this e-book, watch out because your network is an accident waiting to happen.

Because you took the time to read this e-book, we want to give you something in return. We want to offer you a world-class technology assessment for free.

It's called a Network Security Risk Profile and we typically charge $795 for this service. But as a prospective client, **it's yours for absolutely nothing**. It's a multi-point inspection of your network. In our proven process and multi-point audit, here's what you get:

- ☑ We come to you and complete an on-site evaluation of your technology and your network.
- ☑ Pinpoint any exposure to or risk from hackers, viruses, spyware, spam, data loss, power outages, system downtime and even employee sabotage.
- ☑ Review your system backups to make sure your data will be recovered in case of a disaster.
- ☑ Scan your network for hidden spyware and viruses.
- ☑ Look for hidden problems that cause error messages, slow performance and network crashes.
- ☑ Answer any questions you or your employees might have about your network or keeping it running problem-free.

Say goodbye to your computer problems, and start protecting your clients, business data and your identity. There's absolutely no obligation or pressure for you to buy anything, or to ever use our services again. As stated earlier, this is simply an easy way for us to demonstrate how you're exposed and what we can do about it.

Contact us and get your **free assessment** by emailing us at **safe@datacorps.com** with the words "Security Risk Profile" in the subject line. We'll take it from there.

What Your Peers Are Saying About Their IT Experience With DataCorps

"As a CPA, getting a great return on any investment makes a huge positive impact, particularly during these challenging economic times. If you are considering DataCorps Technology Solutions, consider no more. They are truly a partner in the success of my firm."

Stuart C. Angelo, CPA

"In order to maintain our competitive edge, we can't afford to be meddling in the day to day minutiae of managing the high utilization web application and hardware that is used to deliver it. We entrust the daunting task of managing the hardware behind our application to DataCorps, in addition to all of our office systems."

Vince Kudla, President, H2 Insight

"As we grew, we expanded our office and again relied on DataCorps to seamlessly move us into the new location, adding more of their services along the way! After this move, we began examining how our company was serving its clients and its employees and decided to make some fundamental changes to become more competitive. DataCorps adjusted their services and created custom offerings that complemented our changes to fit our budget, direction, and desire to be the very best Real Estate firm out there."

Sharon Michael, MREI Corporation

"We're a small firm that doesn't have the time or expertise to quarterback multiple technology consultants. DataCorps gives us several things we had not found in our previous technology support relationships. They respond quickly with real people who can solve problems without taking up much of our time. They look at issues globally, considering the impact on our other systems and equipment. And they get involved in one-off challenges and projects where we just need help from someone who knows the broader word of business technology. DataCorps support allows us to focus on the thing we do well - serving our own customers."

W. Michael Montgomery, Principal, Montgomery Retirement Planning Associates

“When we began our relationship with DataCorps back in 2009, they quickly identified several failure points that were already either on their way out or would soon become a problem. They had a plan and their ability to leverage resources at their data center helped us resolve those failure points at a much lower cost than if we had to re-build our infrastructure on our own!”

Todd Atkinson, CFO, Bayshore Health & Homemaker Services

DATACORPS
TECHNOLOGY SOLUTIONS