CIOTECH
Networks | Computers | People

THE TOP 10

Ways to Prevent Your Business from Being Hacked

INTRODUCTION

If you've ever seen a friend's post for "really cheap Ray Bans" in their Facebook stream, you've seen what it's like to be hacked. While it can be comical to see someone's Facebook stream pics of puppies and kids get pre-empted for sunglasses, it's not funny when it happens to your business. That's why so many companies are turning to managed IT services.

When your business gets hacked, not only can embarrassing communications be published in your name, but your client's personal data is at risk. People are unlikely to forgive a data breach and your reputation can be permanently affected. Even so, it seems like hacks are happening on a regular basis to the point that customers and users are being asked to change their passwords every couple of weeks because of a new cyber-attack.

The National Cyber Security Alliance estimates that 20% of small businesses get hacked each year. The National Small Business Association was less conservative, estimating the number is closer to 43%.

COMMON TYPES OF CYBER-ATTACKS

Before addressing how to avoid getting hacked, it's important to talk about the most common types of cyber-attacks.

PHISHING

Phishers use emails and sites that resemble well-known businesses (or communications from your friends) to get you to enter key payment information and passwords for them or to click on their URL. Paypal, banks, Yahoo, and Amazon are popular "masks" they use. For instance, phishers might send an email about a recent Amazon order and redirect the recipient to log in for more information. When the person does, the phisher has their password, and their computer has likely been infected with malware. Malware is one of the most common hacking schemes out there currently.

RANSOMWARE

Ransomware has grown up. It used to be that it told users their computers were infected and they needed to purchase virus protection to rid themselves of these <fake> viruses. Now ransomware has become more sophisticated or more thuggish in locking a computer and its data, and demanding payment to release it. The FBI estimates $18 million has been paid out to these cyber criminals.

COMMON TYPES OF CYBER-ATTACKS

VIRUSES AND TROJANS

These types of attacks are often billed as the parents of today's phishing and ransomware but they're still very much out there. You can get them from clicking on an infected link or visiting an infected website. While most anti-virus software can protect you from these threats, new ones are discovered all the time, and software must be updated in order for them to be caught.

Luckily, in most cases, getting hacked is largely preventable. Businesses become more vulnerable as they grow their online presence. If your business is growing, and your online presence increasing, you need to start thinking about vulnerabilities. Here are the top ways you can avoid getting hacked:

TIP #1:
KNOW IF YOU'RE "MOST VULNERABLE"

While cyber-attacks and hacking can happen to any business, there are certain industries that are more vulnerable than others. Just as flaunting expensive jewelry might make you more vulnerable to theft, being in an industry where it's commonly known you have large amounts of personal data, will make you a more attractive target for hackers. Industries like healthcare, which have social security numbers and birth dates, make it easy for hackers to use that information for applying for loans and credit cards.

TIP #1: KNOW IF YOU'RE "MOST VULNERABLE"

Hackers also target companies they know save credit card information. "Borrowing" these numbers can give them a near endless stream of revenue. Most cyber-attacks occur in companies with low-hanging fruit.

While you may not fall into the most vulnerable industries, you still need to protect yourself from hackers. While data is what they are after, severe cyber-attacks monitor your every keystroke. You lose data, privacy, and they can have total access to your digital life. Knowing your business is vulnerable is the first step in avoiding being hacked.

TIP #2:

USE A VIRTUAL PRIVATE NETWORK (VPN)

Most companies use a VPN, but if you don't here's what you need to know. A VPN encrypts all information coming to and from your computer. This means your data is protected because hackers can't "understand" it. VPNs also mask your IP address, which makes it difficult for people to figure out your location. It's also an ideal situation if you find yourself accessing a lot of public WiFi points like in airports and hotels.

TIP #3:

KNOW YOUR BUSINESS COULD BE VULNERABLE THROUGH YOUR CONNECTIONS

Most companies use a VPN, but if you don't here's what you need to know. A VPN encrypts all information coming to and from your computer. This means your data is protected because hackers can't "understand" it. VPNs also mask your IP address, which makes it difficult for people to figure out your location. It's also an ideal situation if you find yourself accessing a lot of public WiFi points like in airports and hotels.

TIP #4:
LEARN OBSCURITY IS NOT SECURITY

Years ago a small business needn't worry about getting hacked because no one knew about the business and only large companies were targets. That's no longer the case. With cyber-attack apps and automated hacking tools, vulnerabilities are quickly discovered, and most companies have vulnerabilities. Don't assume that because you're not a Fortune 500 company you're safe. Cyber criminals aren't necessarily looking for companies with billions of dollars in revenue. They're looking for easy access. Unfortunately, small businesses often provide just that.

TIP #5:
CONSIDER THE WEAKNESSES OF BYOD

Bring Your Own Device (BYOD) is one of the biggest concerns most IT support companies will tell you about. Unsecured mobile and tablet devices with access to company files, or even the CRM, can wreak havoc on a business. That's why it's important to use protection on all employees' devices. Make sure every employee understands the need for this type of security and make it a part of employee education. Use encryption for the devices whenever possible.

TIP #5: CONSIDER THE WEAKNESSES OF BYOD

One of the most common weaknesses in personal devices (and small businesses for that matter) is not updating your operating system (OS) or your web browser. OS and web browser companies keep an eye on malware, worms, and viruses. Many of them have protection built in, but only if you have the most recent versions.

TIP #6:

KNOW THE DIFFERENCE BETWEEN PERSONAL PROTECTION AND BUSINESS PROTECTION

Personal antivirus apps are not robust enough to cover your business needs. One of the biggest differences between personal and business licenses is that most business licenses ensure that multiple devices are covered and patches are applied automatically. Outdated virus protection is a common vulnerability. Most people don't seem to understand the importance of the patches that come out and many leave their systems badly out of date. Business licenses ensure that won't happen.

TIP #7:
EDUCATE YOUR STAFF

In addition to the dangers of bringing your (possibly infected) personal device into the office, there are a lot of other points to cover with your staff as you create a culture that takes cyber security seriously. As a business owner it's important to educate them on the how and the why. Important advice includes:

- Don't open any emails or click on links from people you don't know.
- Not all emails are from the senders they claim to be. Beware of unexpected communications from large companies or emails from friends that share a link but no reason behind doing so.

TIP #7: EDUCATE YOUR STAFF

- Don’t use the exact same password on all of your accounts.
- Don’t use passwords that are obvious and easy to find in public records or on social media like anniversary dates, names of children, and other common ones like “password” or “1234.”
- Educate on the importance of using pin code protection for devices.
- Security questions should be secure. Even though companies give us questions to answer, don’t choose anything that can be figured out in a quick search. This includes mother’s maiden name and former addresses. If the security question is easily found, make up an answer, instead of answering it honestly, and remember it.
- Don’t keep a file of passwords under “passwords” on your computer.
- Don’t write passwords down.
- Before clicking on a link, hover over it to see where you’re really being directed.
- Lost devices that have access to the office’s computers should be reported right away to the service provider.
- If an employee has reason to believe they have just opened a bad link, or if they think their system has a virus, tell IT support immediately. It does not go away and even if everything seems fine, it often isn’t. Instruct them not to shut the computer down. Make sure every employee knows the protocol behind handling a possible infection in the same way that they know what to do in the case of a fire or a tornado. Quick response can save you thousands of dollars.

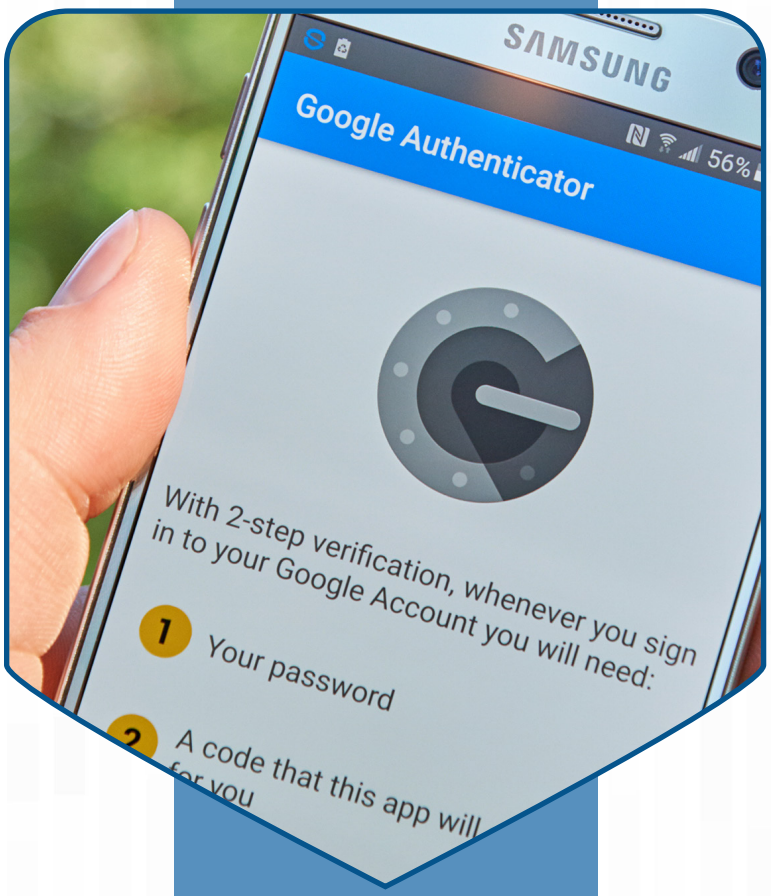
TIP #8:

DON'T BELIEVE EVERYTHING YOU READ IN EMAILS

While this could be another point in educating your staff, it's done so frequently that it deserves a tip of its own. When you get an email from a company you do business with or a social media provider asking you to change your password because they've been hacked, never click the link in the email. Sure it's convenient, but with today's graphic capabilities it is very easy for hackers to mirror another company's font and logo. Instead, go directly to that company's site and change it there. If it was a phishing scam, you've just avoided it and if it was legitimate, you changed your password like the company requested.

TIP #8: DON'T BELIEVE EVERYTHING YOU READ IN EMAILS

Another thing to keep in mind, the IRS never contacts you via email and Microsoft will never call you and ask you for personal information. That's simply not how they do business and any attempts to contact you in those ways are fraudulent.



TIP #9:
USE TWO-STEP AUTHENTICATION WHEN POSSIBLE

Lots of sites allow for global log-ins using Facebook or Google. While this is convenient and easy because you're only remembering one password, and that one is usually saved on your system, using a two-step authentication process whenever possible will ensure your security even when a cyber attacker has your password. These sites will text you a verification code if someone logs in from a new/unrecognized device. You will then need to key in the verification code to get access. Assuming your hacker doesn't have physical possession of your phone, this will most likely stop his/her attempts.

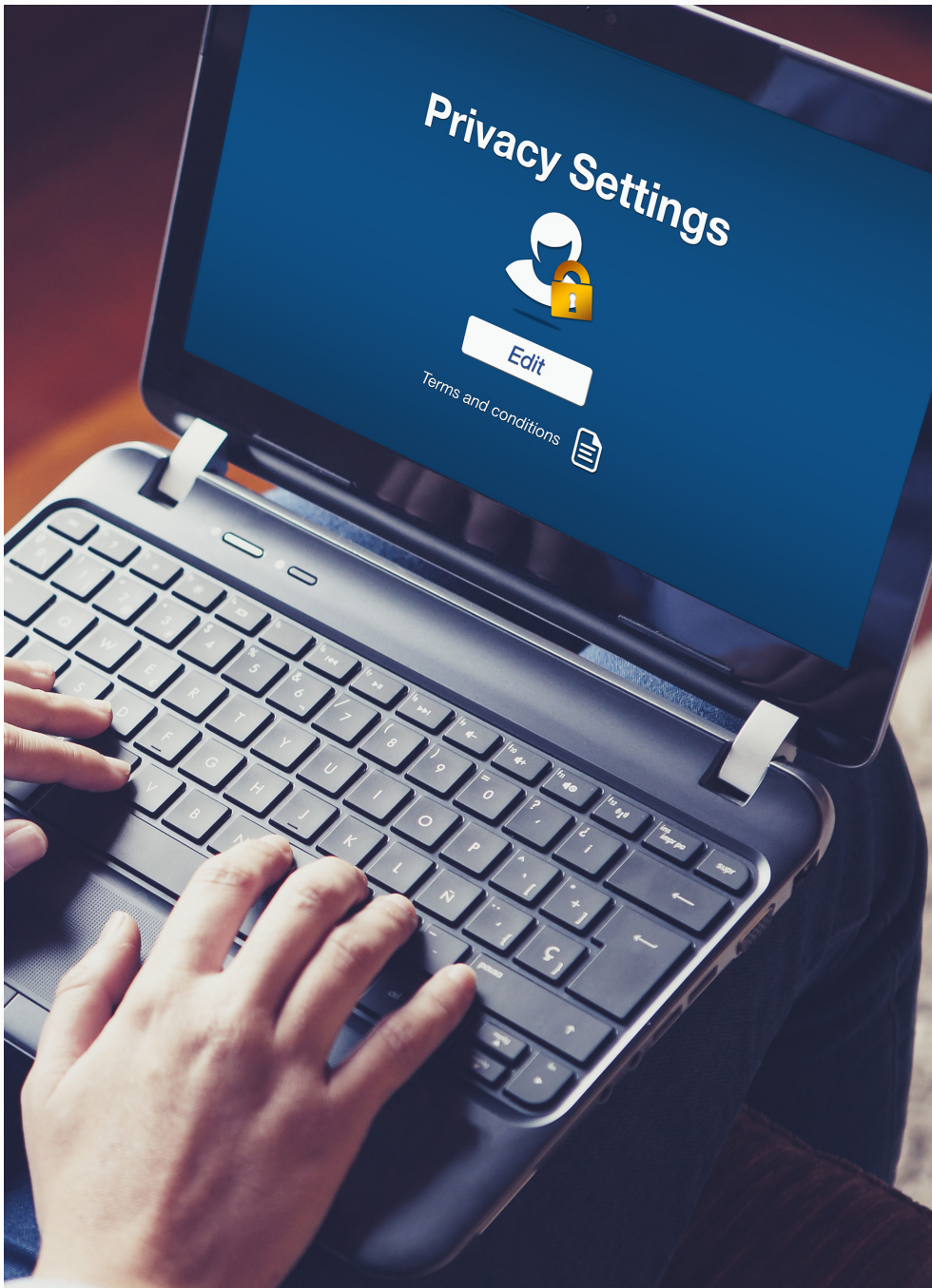
TIP #10:
TIGHTEN YOUR OWN NETWORK SECURITY

If you maintain your own network security and don't use managed IT services, there are a few best practices you should be aware of:

- Set your system to make passwords expire frequently.
- Put stipulations in place that employees can't use the same two passwords by using a system that remembers the past 3 or 4 most recent passwords.
- Require passwords be alpha numeric, with at least one character, and a capital letter.

TIP #10: TIGHTEN YOUR OWN NETWORK SECURITY

- Every device attached to the network should automatically be scanned for malware.
- Install a web application firewall.
- Install website security applications.
- Hide admin pages so they're not indexed. Here's how with a robots_txt file.
- Use SSL protocol to transfer clients' information between your website and your database.



BACK UP EVERYTHING...JUST IN CASE.

CONCLUSION

If all this seems too overwhelming, assign your business data a level of importance. The security of the most critical data to your company's existence should be prioritized above less important information like an employee newsletter, for instance. While this will buy you some time, it's just as easy to implement cyber security measures all at once than it is to roll it out in phases. It's important to note that your information is only as safe as your weakest link, so if you decide to address your security issues in phases, your information better be siloed or else a hacker can get in through a vulnerable area and go elsewhere.

A lot of the tips for avoiding hacks require an additional step and while it's inconvenient for you, a little inconvenience in logging in is a lot better than losing your business because of a data breach.

Also make sure every one of your employees understands why these precautions are necessary. This is about more than someone going to Target and using your credit card. A security leak could shut down your company. It can begin as simply as getting information from an employee's personal smartphone, and then using it to hack your client database. Once your client's data is in jeopardy, you can be assured the future of your business is as well.

Most employees don't understand the gravity of a cyber-attack. Just as you would help them with their professional development, you must educate them on cyber security. If you're not prepared to do that, consult IT support.

Cyber security must be one of your main concerns for your business and it's an ongoing one. You can't let it slip your mind. You need to keep up with it since cyber-attacks are constantly evolving. Often it's not a hacker that decimates a business but the damage to a firm's reputation, as well as financial restitution for clients, and paying to fix the problems caused by cyber criminals.

If you want to know what you can do to further protect your business, consult a Tampa managed IT support company such as CIO Tech at

813-649-7762

www.ciotech.us

CIOTECH

Networks | Computers | People