CYBER SECURITY 101 eBook
FOR CANADIAN SMALL BUSINESSES

WW WORKS

IT services & consulting
Greater Toronto Area, Canada

Contents

Take Online Scams Seriously

Although news of large corporate websites being hacked is reported on a regular basis, many small businesses fail to realize that they too are a possible target for online scams.

Even if your business is small, don't move forward with the philosophy that an online scam 'won't happen to us'. That was the casual attitude of a Canadian financial services company that recently had a rude awakening. They believed that since they were 'small fish in a big sea' that they were basically invisible online. No scammer would bother targeting them, right? Wrong. Their website was hacked and the reason was embarrassing. Not only was their server unsecure but all of the computer passwords at the office were 'password1'. Ouch.

Be prepared in the event that online thieves come looking for your sensitive information which may include credit card information, email IDs and passwords. Did you know that within minutes hackers can turn your little website into a spy bot, scooping up personal information without you ever realizing? Or even worse, they can hack into your website databases and manipulate or destroy important information.

Here are a few simple ways that you can discourage online scams:

1) Avoid common passwords.

Hackers try all the easiest passwords (like *password)* so use strong passwords and change them often. **Learn more about passwords on page 7.**

2) Switch to HTTPS.

Hyper Text Transfer Protocol Secure is a secure communications protocol that is used to transfer sensitive information between a website and a web server. Moving your website to HTTPS adds an encryption layer of SSL (Secure Sockets Layer) to your HTTP making your users' and your own data extra secure from hacking attempts. **Learn more about HTTPS and SSL Certificates on page 10.**

3) Be aware of common phishing scams.

It's in everyone's best interest to understand the common types of phishing scams online criminals use including pharming, session hijacking and malware based phishing. Prevention is the key to protecting your IT security and identity from online scams. No matter how small your business and online footprint, it's important to put preventative measures into place. **Learn more about phishing scams on page 11.**

4) Hide Admin Directories.

Hackers use scripts that scan directories on your web server for obvious names like 'admin'. They'll enter the folder to compromise your website's security. Many CMS's allow you to rename the admin folders to any name you choose. In order to avoid a potential breach pick an innocuous name for your admin folders and don't let anyone know (except your webmaster!).

5) Keep All Software Updated.

Make sure that every piece of software you run on your website is up to date. CMS providers like WordPress regularly release patches and updates that make their software less vulnerable to attacks. Run these updates and always have the latest version supporting your site. If your site uses third party plugins, keep track of their updates too and ensure that these are updated as well.

Be Proactive About Cyber Safety

Prevention is the key to protecting your IT security and identity from cyber criminals.

When you read that, don't you just want to push that thought aside and say, "It won't happen to me!" Remember the Canadian financial services business that was hacked because of using one of the most common passwords, 'Password1'? Avoid putting your business at risk by putting preventative measures in place.

We're living more and more of our work lives online including banking, payroll, and ordering supplies. With technology evolving so quickly we don't always know how we're leaving ourselves open to online fraud, scams or identity theft. The majority of small businesses in Canada are not adequately prepared to ward off the interest of a cyber criminal.

Canada's ongoing **Get Cyber Safe** public awareness campaign brings attention to the fact that cyber criminals are now 'actively targeting' smaller businesses because they believe their computers are vulnerable.[1] In fact, the largest growth area for targeted cyber attacks in 2012 was businesses with fewer than 250 employees — 31% of all attacks targeted them.[2] The campaign aims to help Canadians become more educated about Internet security and provide the steps they can take to protect themselves online.

Cyber security at work is a shared responsibility.

Several people within a business — co-owners, managers and employees — should become familiar with the importance of security safeguards in terms of operations.

A fraudster can assume the identity of a business and steal client lists, assets and credit information, or use the company's identity to obtain business or payments. The cyber criminal could be a completely unknown third party, an employee, a competitor or even a supplier.

According to *The Globe and Mail's Report on Business* article:

> *"The average cyber attack can cost a Canadian small business just over $3-million – a hefty price tag that factors in loss of client trust and non-compliance fines of up to $1-million."*[3]

No wonder the majority of small businesses that experience a cyber attack fold within six months! So, what proactive steps can you take to protect yourself and your business?

Consider outsourcing your IT and cyber security needs to a specialist with a good reputation, knowledge and expertise to protect your business from cyber criminals. Given what a small business has to lose (i.e. everything) it doesn't seem a waste to invest in cyber security. According to industry guidelines, a small business should be spending anywhere from 3 to 7% of its operating budget on security.[4]

It's important to be proactive and prepare to face a cyber attack with up-to-date antivirus software and firewalls, smart passwords, secure servers and regular backups.

About Passwords

Change Them.
And, while you're at it, choose new passwords that are *not* so common.

Some of the most commonly-used passwords according to the security group SplashData, are 'password', 'qwerty', '12345' and'welcome'. Predictably, they are all terribly easy to guess. You can see the whole list below.

The security group which collects and sorts passwords from data breaches in North America and Europe said "123456" and "password" were, for the 6th year in a row, the most common passwords. Groan.

The latest report was compiled from more than 2 million leaked passwords. Some new and longer passwords made their debut on the list which shows some kind of an effort – by both websites and web users – to be more secure. Nevertheless, the longer passwords are so easy that their being longer does not mean safer.

The data gives some insight into the minds of internet users. People love sports as both 'football' and 'baseball' are in the top 25 most popular passwords. Others choose to use the most basic office references like 'admin' as their work computer's password.

So now that you see how easy it is to hack your password, what else should you know?

Top 5 Internet Password Do's

1. Create unique passwords that use a mix of words, numbers and both upper- and lower-case letters.
2. Choose a long password such as a phrase that has personal meaning (for easy recollection). Probability means that a longer password will be harder to crack.
3. Think in terms of phrases. Use the first letters of a memorable pangram, such as 'Pmbw5dlj' – which equals "*Pack my box with five dozen liquor jugs.*"
4. If you're not a creative type, use a password manager like 1Password [5], which can generate secure passwords and store them for you.

Ideally, protect yourself best by using two-factor authentication (2FA), which will send a text with a code or use an app to verify your log-in. Find out which websites support 2FA at TwoFactorAuth.[6]

Top 5 Internet Password Don'ts

1. Don't use easily guessed passwords, especially anything that could be guessed by a look at your Facebook profile. Big fan of dragons (Game of Thrones "likes")? Big fan of Football (NFL "likes")? Don't use that as your password. You know better now.
2. Don't use your network username as your password.
3. Don't choose passwords based upon personal details that are not top secret, such as your birth date, phone number, or names of family members and pets.
4. Don't use words that are found in the dictionary. Free online password-cracking tools come with dictionary lists that will try thousands of common names and passwords.

Never use your email password at any e-commerce site. If you do and a site at which you are registered gets hacked there's a very good chance someone will be reading through your e-mails.

Obviously a secure password is only a piece of the puzzle. Other pieces include installing strong firewalls, plugging up network holes, user education and physical security – all things with which a great IT company can help to bring peace of mind.

The 25 most common passwords

1. 123456
2. password
3. 12345
4. 12345678
5. football
6. qwerty
7. 1234567890
8. 1234567
9. princess
10. 1234
11. login
12. welcome
13. solo
14. abc123
15. admin
16. 121212
17. flower
18. passw0rd
19. dragon
20. sunshine
21. master
22. hottie
23. loveme
24. zaq1zaq1
25. password1

Remember that financial services company that got hacked? Did you notice that their password was the 25th most common in North America? *You* now know better.

(courtesy of https://www.teamsid.com/worst-passwords-2016/)

About SSL Certificates

Secure Socket Layer Certificates are used to establish an encrypted connection between a computer browser and a web server.

Basically, SSL technology activates a lock and the https protocol which allows for secure connections that protect sensitive information. Once that connection is established all web traffic between the web server and the computer browser will be protected.

Usually, an SSL is used to secure credit card transactions, logins, data transfer and social media sites.

There are other benefits as well. SSL Certificates not only keep data safe between servers, they enhance customer trust and improve conversion rates and your Google Rankings. No wonder the number of organizations using SSL Certificates – for secure search – has grown so quickly. In June 2014 Google called for 'HTTPS Everywhere' at its I/O conference. Google's Webmaster Trends Analyst Pierre Far told a room full of developers that, "We want to convince you that all communications should be secure by default." Google followed up with an official announcement almost two months later. Of course, all of Google's properties are encrypted.

HTTPS stands for Hyper Text Transfer Protocol (the 'HTTP' before a site's domain) with the addition of 'S,' for 'secure'. As you would guess, the 'S' means that the site's data is encrypted.

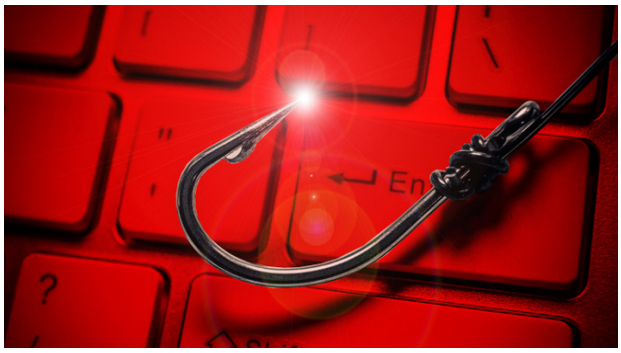
We're doing our part to help create a more secure and safer Internet. SSLs are bundled with our Managed Services package. Well, maybe 'bundled' isn't the best way to describe it. Let's just say we've seamlessly integrated the very best security services. No need to opt in as we now consider it a standard within ServiceWorks, our all-in managed services plan. Learn more about our managed services on page 10.

We provide the most comprehensive type of SSL Certificate (Extended Validated) and make it simple for our clients. There's no involvement necessary on your end. And, there are no long term commitments or additional invoices to worry about!

Expect automatic, transparent, open and cooperative, 'security by default' SSL Certificates.

About Phishing Scams

It's in your best interest to have a basic understanding of the types of common online phishing scams. Help avoid a cyber crime attack by recognizing the signs. Here are the types of phishing scams of which you need to be aware:



Deceptive Phishing

Deceptive Phishing is the most common type of scam. Fraudsters impersonate a legitimate company and try to steal people's personal information or login credentials. Often, they include a sense of urgency or a threat to scare users. For example, a PayPal scammer would send an email that instructs you to click on a link in order to correct a discrepancy with your account. The false link would lead to a fake PayPal login page that would collect your credentials for the attackers.

Malware-Based Phishing

Malware is software written to harm and infect a user's PC. This includes viruses, spyware, adware, trojan horses and worms. Ransomware, an advanced form of malware, is used to execute financial fraud and extort money from computer users. Your screen may show a pop-up warning that you have been locked out of your computer and that you can have access only after paying the cyber criminal. One particularly infamous type of ransomware is Cryptolocker, a trojan that targets computers running Microsoft Windows.

Session Hijacking

Session Hijackers monitor your activities online until you sign in to a target account or purchase something online. They then can use your credentials to undertake unauthorized actions such as transferring funds without your knowledge. This is why we include SSL certificates with our fixed-fee managed IT services plan, ServiceWorks, as encryption helps prevent any hijacking attempts.

Pharming

Pharming is when a hacker modifies a company's website host files and covertly hijacks your computer and directs it to a fake site. There's a good chance you won't realize that the website isn't legitimate. In most cases, a faux-site where you enter confidential information looks identical to your bank or online shopping sites like eBay or Amazon. The faux-site is controlled by hackers who gain access to your credit card numbers, account password, etc.

This is why we always ensure our ServiceWorks clients use an up-to-date anti-virus program which protects them from unauthorized alterations of the Host file. It's also important to always download the latest security updates or patches for your Web browser and operating system to stay protected. Just to be sure, always check the 'HTTP' address. When you visit a site where you're asked to enter personal information, the 'HTTP' should change to 'HTTPS'. The 'S' stands for secure.

Keyloggers

This particular variety of spyware tracks keyboard input and then sends relevant information to your cyber stalker via the Internet. Keyloggers can be installed on your computer by a virus, worm or Trojan. Fraudsters capture your account numbers and passwords as you type which gives them enough information to empty your bank accounts and set up credit cards in your name. Thankfully, good anti-spyware will protect your computer against known viruses, worms and Trojans of all types. Resist the temptation to download 'freeware' such as free screensavers. Keyloggers can easily attach themselves to free software offered over the Internet so only download from reputable sources.

Business Data Theft

Cybercriminals don't care about the size of your organization, it's the type of data that matters. In fact, SMBs are much more likely to not be well protected online which makes the job easier. Too many small companies mistakenly think they can fly under the radar because they are not that lucrative and have hardly any assets.

62% of SMB's have been victims of a cyber breach.

Scammers steal confidential customer details, intellectual property, legal opinions, employee related records, credit card information and more. Small businesses shell out an average of $38,000 USD to recover from a single data breach. Avoid losing current and potential clients by investing in regular system checks to ensure your organization's data safety. Our ServiceWorks clients are secure in knowing that they are protected with Security Audits, Remote Monitoring, Data Backup and Business Continuity.

Content Spoofing

Content Injection Phishing or 'spoofing' is where the scammer changes a part of the content of the page of a reliable site. Users can be misled to go to a page outside of the legitimate website where they will be asked to enter personal information. A quality IT provider can ensure that your website is not vulnerable to a hacker's malicious code.

Search Engine Phishing

Search Engine Phishing occurs when cyber scammers create websites with irresistible offers and have them indexed legitimately with search engines. People find the sites while they're looking for products or services online and are fooled into giving up their information. Remember, if it seems too good to be true, it is.

It's incredibly important to protect yourself and your business as much as possible online. Be aware of current common phishing scams, use creative passwords, keep your operating system and software updated and always use exceptional security software.

About ServiceWorks

It's our fixed-fee Managed IT Services plan.

We make it easier for Greater Toronto Area businesses to succeed in today's tech-driven environment.

Included with ServiceWorks

- Cost-effective managed IT services
- Reliable technology with systems that perform at optimal speed.
- Protected technology including all of your IT networks, systems, and applications
- Cyber Security to ensure the business continuity you need

Keep in Mind

- No surprise IT expenses - We're affordable, with a monthly fixed rate.
- IT 'Know-It-Alls' that keep up with today's quickly-evolving technologies.
- Security Audits to identify vulnerabilities that could harm your IT and your business reputation.
- A comprehensive Cyber Security Solution that protects your data, email, and IT investments.
- Regulatory Support so that your technology promotes compliance with stringent privacy regulations.
- Customizable Cloud Services so you can add solutions or delete them as needed.
- Remote monitoring to catch IT issues and repair them before they create big problems.
- Mobile Device Management solutions so your data is safeguarded anywhere it goes.
- 24/7 Live Help Desk Services available any time of the day or night.
- Backup and Disaster-Recovery Solutions with secure onsite and offsite data storage, protection and recovery.

About WW Works

With our dedicated and certified team of technical experts WW Works is well positioned to meet all of your IT department needs. We have been serving the IT needs of our **client base around the Greater Toronto Area** for 27 years.

Get In Touch

Give us a call to learn more about our Cyber Security Solutions. We can talk to you about locking down your systems and keeping your business safe and operational. We'll manage your technology and computer systems so they meet business cyber security standards.

Call Us:
905 332 5844

Email Us:
info@wwworks.com

Notes

1. **http://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-en.aspx**
2. **http://www.symantec.com/security_response/publications/threatreport.jsp**
3. **http://www.theglobeandmail.com/report-on-business/small-business/sb-managing/cyberattacks-an-ongoing-threat-to-canadian-small-businesses/article22653793/**
4. **http://www.theglobeandmail.com/report-on-business/small-business/sb-managing/cyberattacks-an-ongoing-threat-to-canadian-small-businesses/article22653793/**
5. **https://1password.com/**
6. **https://twofactorauth.org/**