Internet threats:

steps to security for your small business

Shaw Business

Proactive solutions for small businesses

A restaurant offers free WiFi to its patrons. The controller of an accounting firm receives a "confidential" email in which he is asked to provide tax details on employees. A lawyer loses his phone.

What do they all have in common? Their business' network security is at risk. And whether your business network consists of a fleet of servers and computers, or simply a laptop and a mobile phone, it, too, can easily be at risk.

We see headlines weekly about large, multinational corporations being hacked, but surprisingly it is small businesses that are the most in danger. 60% of targeted attacks in 2014 struck small and medium-size companies.[1] And those hacks can really hurt a small business by compromising critical data, exposing customer information, and costing organizations millions of dollars. The average cost of being hacked as a small business is $36,000.[2] This amount climbs an additional $8,000 once indirect expenses and damage to reputation are taken into account.[3]

Why are small businesses such inviting targets? The simple reason is that they often have less cyber security knowledge and fewer resources, which makes them easier to crack. Small businesses also sometimes serve as vendors to large companies, which may be the hacker's ultimate target.

It's no surprise, then, that more and more business owners are seeing network security measures as an essential way to "insure" their information's safety, just as they take measures to protect from property loss. In fact, Canadian law requires it. The Personal Information Protection and Electronic Documents Act (PIPEDA) requires organizations to devise policies and procedures for protecting personal information. For more information, see the user-friendly guide at www.priv.gc.ca/information/pub/guide_org_e.pdf

Fortunately, just as hackers develop more ingenious methods, so too do experts develop new methods for securing business data. There is no "one size fits all" solution, because specific needs vary by industry. However, here are some of the most important guidelines to know:

60% of targeted attacks in 2014 struck small and medium-size companies.[1]

1. Educate employees

Awareness is the best defense. Employees (as well as contractors or vendors who may have access to your network) are often the most vulnerable link in a network security chain. You can have a great network security solution in place, but one employee can directly or accidentally allow an intrusion if not educated properly. **Phishing**, for example, is a common means of invading a company's network, whereby a hacker masquerades as a trustworthy entity. An employee then clicks on an interesting or seemingly important link in an email, and a small piece of **malware** automatically downloads, with no one the wiser. Another example of targeting employees is a new trend known as "CEO fraud" or "fake president fraud," in which hackers mimic a top executive's email address.

Therefore, you'll want to inform your employees and contractors about **phishing**, and perhaps create a policy of double-checking via telephone when significant transactions are requested. Find resources and training for businesses and employees at StaySafeOnline.org (http://staysafeonline.org/business-safe-online/train-your-employees)

2. Step up your password game

To protect your business from intrusion it is important to create complex passwords, have a policy of changing a password frequently, and policies for changing passwords with employee departures.

With high-quality WiFi, employees are no longer confined to their desks to work while in the office; they can take a mobile device to a colleague's office, to a private space, or to a part of the business located on the other side of the building. With this changing work environment it is important to have separate networks for guests and employees and have passwords for each. A separate network for guests means employees do not have to sacrifice speed or bandwidth during times of heavy client usage.

3. Enable security safeguards

A **firewall**, which can be a software program or a piece of hardware, is a filter between a computer network and the Internet. It is the first line of defense that helps to block **malware** and other invaders. **Antivirus software**, which is installed on computers and devices, scans computers for malware "infections" that have reached the system, and cleans them up. Your business needs both, and needs to keep up with any updates or "patches" issued by the manufacturer. Avoid the temptation to disable a strong firewall because it requires an extra step—like reading a pop-up notification or double-checking a web address—to access certain sites. Look to managed security solutions that features both firewall and content filtering.

4. Embrace encryption

Simply put, encryption is a way of "scrambling" information (video, words, images) so that they no longer make sense. A "key," such as a passcode, is needed to restore the information to its original state. Your email provider, computer operating system, and much of the business software your company uses may have built-in encryption options; check with your provider or manufacturer. If not, consider purchasing additional encryption software from a reputable provider. Remember that removable media, such as USB drives, should be encrypted as well.

When you send information online, you'll want to make sure the network is secure. You'll know when a site is secure if you see "https" in the beginning of a web address, with the "s" at the end noting it's safe and encryption is at work.

As a small business, you should obtain an **SSL** certificate to secure your website so that customers can safely share sensitive information. You can purchase a certificate by contacting your web developer or hosting company. Your hosting company will have to install the certificate on your server, and your web developer will then configure your website to deploy the secure connection.

Utilizing an encrypted network is important for any business, but particularly for e-commerce companies and offices that handle highly sensitive client/patient information, such as doctors' offices, insurance agencies, or financial firms.

5. Be on top of the mobile security

Most of us bring our work with us wherever we go, often on personal mobile devices such as a smartphone, laptop or tablet. Remind employees regularly of the potential harm to the business if a device is lost or stolen. At the very least, all employees who use personal devices for work should have unique passcodes that lock those devices. There are also apps that provide a service known as “containerization” that separates corporate and personal data. Some even allow an IT technician to remotely wipe a device clean should it ever end up lost or stolen.

6. Don’t share your business network

Offering WiFi to your customers and guests can be a great move, but allowing them to use the same network your company uses is a big mistake. Be sure to ask your WiFi provider about ways to separate your customer-facing network from your business network. This will both alleviate bandwidth concerns and prevent that hacker in the parking lot from gaining access to your business data. Businesses should always ensure that their private WiFi network is encryption-enabled and password-protected.

7. Consider a security solution that leverages the cloud

A security system that leverages the **cloud** offers the advantage of easy access to the latest intelligence from around the world to continuously update its defenses. When data and applications are based in the cloud they are generally safeguarded by large enterprises that have the resources to provide multiple layers of security and backup—many more than the average small business could ever afford.

If any of the above seems overwhelming or simply too time-consuming for your small business, don’t hesitate to call in expert help. Managed security services can handle your business’s network security needs so that you don’t have to spend time on installation and regular updates.

It’s never too late, or too early, to start thinking about a network security solution. Regardless of the industry you’re in—service, retail, professional, and others—there’s no time like the present to protect your business.

Security terms decoded

Understand these terms to help you make decisions about security for your business

APT (advanced persistent threat)
A long-term targeted attack that breaks into a network in multiple phases to avoid detection.

Antivirus software
Software designed to detect and protect against computer viruses and malware.

Data breach
When sensitive or confidential data is accessed, copied or stolen by an unauthorized party.

Email authentication
Verification, by an email server, of the source of any given message. The process protects against spam and email scams.

Encryption
The process of converting data into a unique, unrecognizable code.

Firewall
A filter between a computer network and the Internet. It is the first line of defense that helps to block malware and other invaders. Firewalls can be implemented in both hardware or software, or a combination of both.

The cloud
Increasingly, software (such as Microsoft Office 365) and services (such as data storage) are delivered over the Internet. The data for these services is accessible from anywhere, but physically stored "in the cloud," which refers to massive data centers.

Malware
Malicious software designed to access or cause harm to a computer or network.

Phishing
A fraudulent request for sensitive data (like personal information, passwords, etc.) made via email.

Skimming
An attempt to steal credit or bank card information with a card-reading device, known as a skimmer.

Secure Sockets Layer (SSL)
The standard security technology for creating a link between a web server and web browser, which ensures the information passed between the two remains secure.

Ransomware
A software code that "kidnaps" data by encrypting it, then demanding payment for the decryption key. Ransomware can be delivered via email links or attachments, or through infected websites.

Cybersecurity by the numbers

71% of all data breaches are waged against companies with less than 100 employees.[4]

22% of small businesses say they don't know where to start when it comes to cyber security.[5]

83% of small and medium businesses **do not have a cyber security plan in place.**[6]

1 out of 10 people who receive a malicious email will click a link in it.[7]

Cybercrime costs roughly **$400 billion** annually across the globe.[8]

Is your business protected?

Take a moment to consider the following questions

- [ ] Do you keep, record and/or share critical data in the cloud?
- [ ] Do your employees and/or customers use the Internet at your place of business?
- [ ] Do you transmit sensitive information between employees online?
- [ ] Do you transmit sensitive information to customers and/or vendors online?
- [ ] Do you use multiple devices for business activities?
- [ ] Do you and/or your employees travel and use unknown networks?

If you answered yes to any of these above questions, your business can benefit from a managed security solution.

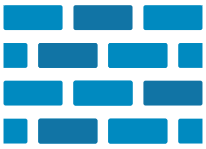
SmartSecurity by Shaw Business

SmartSecurity keeps your business secure so you can focus on growing your business.

Advanced threat protection

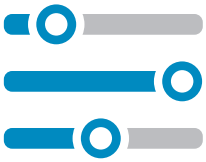
Help protect your business against the latest viruses, malware and malicious hackers - with automatic updates.

Business grade firewall



Permit or deny traffic at the network level.

Content filtering



Control types of content that are allowed on your network.

Application control

Control the applications that go in and out of your network.

Connectivity

Connects multiple sites securely and allows you or your employees to login to your network securely from anywhere.

Cloud managed

Cloud-based solution with automatic updates. You can manage it through an easy-to-use online portal or our experts can help manage it for you with 24/7/365 tech support.

Learn more about how SmartSecurity can help protect your business.

Call: 1-855-505-3023 | **Visit:** business.shaw.ca/smartsecurity | **Follow us:**

Shaw Business

1: Symantec Internet Security Threat Report 2015 http://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf
2. The Big Business of Hacking Small Businesses, Inc Magazine, 2016. http://www.inc.com/will-yakowicz/big-business-of-hacking-small-businesses.html
3. Damage Control: The cost of Security breaches, Kaspernsky Lab into the source, 2015. http://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf
4. Verizon 2012 Data Breach Report http://www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf
5. Towergate Insurance, "SMEs and Cyberattacks: What You Need to Know" 2015 https://www.towergateinsurance.co.uk/liability-insurance/smes-and-cyber-attacks
6. 2012 NCSA/Symantec National Small Business Study Government of Canada http://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-en.aspx#s2
7. 2015 Data Breach Investigations, Verizon http://www.verizonenterprise.com/DBIR/
8. "Net Losses: Investigating the Global Cost of Cybercrime," McAfee report, June 2014 http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf