Employee education: your #1 defense against cyber threats

Shaw Business

5 easy ways to strengthen your company's "front line"

Cybercrime continues to rise and is costing Canadian businesses an estimated $3 billion per year.[1] From small retailers and restaurants to service-based professional firms, no organization is immune or "too small" to have their network attacked.

Where is the weakest link in your company's security chain? Unfortunately, it's likely one of your employees or contractors. More than half of all cyber attacks are the result of actions from "insiders", those trusted people who have access to your company's systems, according to a recent global report.[2]

That means you could significantly reduce your organization's risk of cyber attacks simply by taking steps to ensure your employees are better trained to prevent them. Here are five ways to do that:

1. Provide guidance with a clear computing use policy

According to Get Cyber Safe (getcybersafe.gc.ca), a national public awareness campaign program, **83% of SMBs (small and mid-size businesses) don't have a cyber security plan in place**.[3] IT World Canada, an online resource for IT professionals, recommends that computing policies be clearly stated in writing, with penalties for violations that can involve performance evaluations and may even lead to termination.[4] All employees and contractors should review and sign the policy.

Get Cyber Safe says business policies on Internet usage should, among other things: [3]

- Address the types of websites employees are allowed to visit
- Establish guidelines for social media
- Limit the amount of personal e-mail employees send or receive at work
- Advise employees to seek permission when downloading new programs
- Advise employees to avoid opening e-mail attachments unless they're from trusted contacts

The HR Council of Canada (hrcouncil.ca) provides a sample policy[5] on Internet and e-mail use, as do various professional IT organizations.

Security experts also say it is wise to have any policy you want to implement reviewed in advance by a human resources and legal professional.

To help employees do their online work safely, your business should install the latest security

software, and update browsers and operating system to defend against viruses and malware. To learn more about these security terms read our Small Business Cybersecurity Toolkit article here.

2. Emphasize physical safety for devices

Sophisticated cyber attacks make headlines, but many cyber breaches are low-tech crimes of opportunity. You can mitigate some risk by encouraging the care and physical protection of business devices, mobile and otherwise.

Some of these measures involve using common sense and developing better habits. For example, a report on cyber security best practices by the Investment Industry Regulatory Organization of Canada (IIROC) recommends companies follow a "clean desktop" principle by: [6]

- Putting away sensitive information
- Engaging screen lock when employees are away from their desks
- Password-protecting all mobile devices

Caution is especially important if your company is integrating Internet of Things, or IoT, technology. Just about any WiFi-enabled device, from POS (point-of-sale) systems to thermostats and cameras, can be susceptible to hacking if not physically protected.

Allowing employees to use their own phones, tablets or laptops for remote work—known as BYOD, or "bring your own device"—is a common practice among small businesses, and for good reasons. The practice empowers employees and relieves the company of the expense of providing mobile devices for them. In fact, more than three quarters of Canadian companies support BYOD, according to one recent study. [7]

However, caution is warranted. A recent survey found that **one in five organizations had suffered a mobile security breach**, primarily driven by malware and malicious WiFi (for example, a "public" network that was actually set up by a hacker). [8]

Best practices for BYOD security include implementing a formal company policy. In addition to mandating strong passwords (see #3, following this paragraph), security experts recommend to consider requiring two-step authentication (the use of an additional piece of information beyond username and password) for personal devices that are used for business, in case they're lost or stolen. The Office of the Privacy Commissioner of Canada recently released a comprehensive whitepaper on these and other issues for BYOD.[9]

3. Require strong passwords that are changed every 90 days

Weak passwords are an all-too-common problem. In fact, some Canadian companies, including banks, have weaker password requirements than those for Google and Twitter accounts, according to reporting by The Globe and Mail.[10]

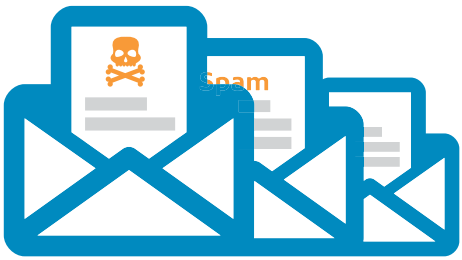
Meanwhile, a recent international survey of employees found that **49% admitted to sharing their login details with coworkers** at some point.[11]

While no one enjoys changing (and re-memorizing) passwords, experts say that even the smallest business needs to take this basic step to protect itself. They recommend:

- Passwords that are at least eight characters long, with a combination of lowercase and uppercase letters, and at least one number and one character
- Password protection for all company devices
- Different employee passwords for different devices and portals, none of which are stored on their computers or mobile devices

To make the process a bit less onerous, many servers can be set to require new passwords at certain intervals, and employees can use widely available password managers such as LastPass and Dashlane to securely store and organize login information.

4. Teach employees to spot "phishing" attacks.



Even with advanced spam filters, about 10% of phishing e-mails get through.[12] However, your employees can't defend against potential attacks if they're not able to recognize them. **A 2015 survey, tested 19,000 computer users and found only 3% could recognize all of 10 phishing scams presented**.[13]

Phishing scams can be done by phone, but they usually come in the form of an e-mail or website in which an attacker poses as a trusted source or company—a government agency, a financial institution, even the owner of the business. The hacker then uses the platform to solicit information or convince recipients to click on a link, which in turn automatically downloads malware on their device.

Employees should always hesitate to click on a link, or open an attachment, from an unknown source. Teach employees to recognize red flags like:

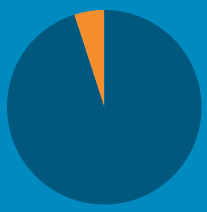
- A mismatch between the purported sender's e-mail address and the organization's URL
- Misleading domain names, such as the company website name with a different extension (e.g., ".net")
- A request for information that the company should already have, such as birthday or SIN (social insurance number)
- Poor grammar and misspellings
- Any request to transfer large sums of money, or an urgent call to immediate action
- When in doubt, an employee should call the source of the message to ensure the request is legitimate, and to double-check before giving out information or credentials.

5. Hold regular security meetings.

Because hacking strategies and attacks are constantly changing, ongoing training is required to increase awareness. Regular training not only mitigates the risks of human error, but also serves as a reminder for employees to follow policies. These meetings should reinforce basic security protocols and identify any new threats or vulnerabilities. Time-pressed business owners can also communicate these messages through updates to the computing use policy. Have employees sign updates to verify they've read them.

Such training and education about best practices to avoid cyber threats should also not be solely for front-line workers. An IIROC best practice guide notes that because hacking attacks often target executives, it's essential they also take part in all cyber security meetings.[14]

Protect your business with good practices



95% of all data breaches involve human error.[2]

83% of small businesses don't have even an informal cybersecurity policy.[12]

63% of employees say they **use the same password** in multiple locations.[15]

49% of employees say they have shared passwords with coworkers.[9]

More than 40% of employees report having **access to corporate accounts** even after leaving their job.[15]

We know security can be a big task for small businesses, but you don't have to do it alone.

Let us help manage it for you with SmartSecurity from Shaw Business.

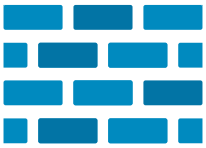
SmartSecurity by Shaw Business

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

Advanced threat protection

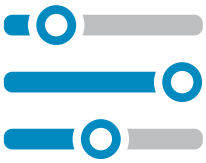
Help protect your business against the latest viruses, malware and malicious hackers - with automatic updates.

Business grade firewall



Permit or deny traffic at the network level.

Content filtering

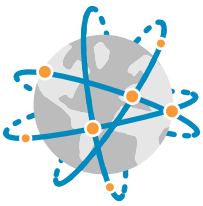


Control types of content that are allowed on your network.

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: 1-855-280-9555 | **Visit:** business.shaw.ca/smartsecurity | **Follow us:**

Shaw Business

Sources

1. Canadian companies have a big new ally in the fight against cyber crime, Financial Post, December 11, 2015 http://business.financialpost.com/fp-tech-desk/canadian-companies-have-a-big-new-ally-in-the-fight-against-cyber-crime

2. IBM 2015 Cyber Security Intelligence Index, IBM, 2015 https://www-01.ibm.com/marketing/iwm/iwm/web/signup.do?source=ibm-WW_Security_Services&S_PKG=ov36858&S_TACT=C405016W&dynform=19041

3. Get Cyber Safe Guide for Small and Medium Businesses, Get Cyber Safe, 2016 http://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-en.aspx#s3-3

4. IT World Canada, 2016 http://www.itworldcanada.com/

5. HR Policies & Employment Legislation, 2016 http://hrcouncil.ca/hr-toolkit/internet-email-use.cfm

6. Investment Industry Regulatory Organization of Canada (IIROC), 2016 http://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf

7. Canadian firms leading world in BYOD: Study, 2013 http://www.itworldcanada.com/article/canadian-firms-leading-world-in-byod-study/47616

8. BYOD and Mobile Security 2016 Spotlight Report, Crowd Research Partners, 2016 http://www.crowdresearchpartners.com/portfolio_item/byod-mobile-security-report/

9. Is a BYOD Program the Right Choice for Your Organization? 2016 http://www.crowdresearchpartners.com/portfolio_item/byod-mobile-security-report/

10. Why Canada's banks have weaker passwords than Twitter or Google, 2013 http://www.theglobeandmail.com/technology/digital-culture/why-canadas-banks-have-weakerpasswords-than-twitter-or-google/article18325257/

11. A Study of Insider Threat Personas, IS Decisions, 2016 http://www.isdecisions.com/insider-threat-persona-study/

12. Get Cyber Safe Guide for Small and Medium Businesses, Get Cyber Safe, 2016 http://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-en.aspx#s3-3 Get Cyber Safe http://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-en.aspx

13. McAfee Phishing Attack Quiz, 2015 https://blogs.mcafee.com/consumer/phishing-quiz-results/

14. Cybersecurity Best Practices Guide, 2015 http://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf

15. 2016 Market Pulse Survey, Sailpoint, 2016 https://www.sailpoint.com/identity-governance-market-pulse-survey/