Quick Cyber Security Tips for Local Businesses

Target Audience

These cyber security tips are aimed at small businesses that do not have their own IT staff, do not fully outsource their IT operations to an MSP (Managed Services Provider) or do not otherwise have a mature cyber security infrastructure. Many of these tips will also be valid for home networks and personal smartphones.

Caveat

This information is not a substitute for years of IT security experience, professional training or well-designed IT infrastructure. The tips in this document are meant to be quick wins for those businesses that identify as being representative of the above target audience. Again, this is not comprehensive or best practice guidance, these are emergency measures to help you in a pinch. If your business does have IT support, please reach out to them before implementing any of these tips.

Why Provide These Tips Now?

Society's response to Covid-19 presents some acute challenges that many businesses may not have foreseen or prepared for. Essentially, bad actors see opportunity whenever there is confusion, significant change or when people feel a strong desire to help.

During any major humanitarian event, businesses should expect to see an increase in email phishing attacks, scam calls, wire fraud, fraudulent social media requests for charitable donations and more.

This sudden, dramatic and unplanned shift to having staff work from home is a massive opportunity for bad actors. During any major IT change event, businesses will often disable, bypass or poorly configure security tools/features. The thinking seems to be, "get people working and then we'll figure it out later". Unfortunately, it's far too common that many of these holes never get patched, because everyone is busy, and no one remembers they're there.

The following tips were selected to help small businesses focus on just a few things that can provide the biggest bang for their buck.

Cyber Security Tips in Order of Priority

Slow Down, Think and Document

This tip applies to you and every member of your staff. The biggest risk to your business is not keeping a cool head, doing some basic planning and having a record of the change. Writing out simple point form plans will organize your thoughts, check your logic and provide you with some record of what was done.

Planning doesn't mean trying to figure out absolutely everything at the beginning. Instead, follow a process of writing out the next two or three things you need to do, then do them. Once you've accomplished those two or three things, plan the next couple of changes. Take small manageable steps and take notes as you go.

The overwhelming majority of security failures are related to human error, so being methodical and writing as you go can save you a lot of pain now and in the weeks and months ahead.

Apply Updates!

I know you've been hearing this for years, but I still run into so many businesspeople who don't apply updates on their computers or their smartphones. Think of security updates as being like vaccines. This is how immunity is spread amongst computers. Granted not all updates are security updates, but unless you're going to review each update, you're better off just applying all of them.

Updates aren't just for your operating system. The applications (apps) that you use also need to be updated. By far the most important apps to update are your browser (Chrome, Firefox, Edge, Safari) and your email program (typically Outlook).

Protect Your Email Account Credentials

This might sound strange, but your email account has become a high value target for bad actors. Your email account is the centre of your online identity and it used as a conduit for resetting passwords on other accounts. This means that if an attacker can gain control of your email account, they can impersonate you (send phishing emails to your staff or coworkers) and they can change the passwords and security settings of most of your online accounts (think banking, cell phone, Office 365, G Suite, online accounting software, social media accounts, etc).

You can protect your email account by enabling 2 factor authentication (2FA) and choosing a unique and strong password or passphrase.

- Google G Suite
- Microsoft Office 365

If you are using your ISP's email service (@shaw.ca, @telus.net) or most of the low-cost hosting providers, you're not going to be able to set up 2FA. Some of these providers don't even support encrypted connections, which makes them dangerous. The best you can do with these providers is to set a unique and strong password and change it often. Changing email providers is a big job and not something you want to do during other major changes.

Do Not Operate Your Computer as an Administrator User

The strongest defense you have, against a wide range of threats, is to not login to your computer as an administrator user. Sadly, this is still the default whenever you create your first account on a Windows or Mac computer… And, it's not easy to change… Some small business owners may be able to work through this process without technical assistance, but it's not for the faint of heart. We only included this tip, because it's just so effective. Please only attempt this process if you have a really good full machine backup and you know how to use it. Otherwise, it's probably wise to pay for professional assistance.

- Windows
- Mac

Set Up a DNS Firewall on All Your Devices

DNS is like a phonebook for the Internet, which converts names to IP addresses. A DNS firewall can help to protect you from falling victim to many scams. We recommend the non-profit service Quad9 for its mix of strong security and zero cost.

A DNS firewall is different than your hardware router/firewall or the software firewall on your computer. At this point, absolutely every business should be using regular firewalls, so we're not going to spend any more time on them here.

- **Windows**
  - video instructions
  - or written instructions with screenshots
- **Mac**
  - video instructions
  - or written instructions with screenshots
- **iPhone/iPad**
  - I couldn't find a simple way to do this that works seamlessly across wifi and cellular. The closest I could find was an app called DNSCloak. Unfortunately, while DNSCloak does work, it's not easy to configure and beyond the scope of this article.
  - If you do decide to try DNSCloak, search for and use the option **quad9-doh-ip4-filter-pri**
- **Android smartphone/tablet**
  - Install the Quad9 Connect app
- **Advanced option** - Change the DNS servers in your modem or router/firewall
  - There are too many makes and models to provide specific instructions. If you know how to login to your modem or firewall, you can change your DNS forwarder IP addresses to **9.9.9.9** and **149.112.112.112**

Check your backups

Backups are your last line of defense against destructive attacks such as ransomware. There are many backup tools, methods and services, so we won't attempt to cover the setup of any particular solution. However, this tip provides guidance that should apply to all backup systems. You do have a backup system, right? Of course you do 😊

- Backups need to happen regularly in order to be a useful safety net
  - Backups should be done at least daily if not more often
  - Automated backups make achieving this goal realistic
- Backups to attached drives will not protect you against ransomware
  - If your backup system uses a USB drive or a network share, then you really must be careful about detaching it whenever your backup is complete
- Multiple backups are a great idea
  - Your main backup routine should be really solid, but you should also have a second backup system just in case the main one fails
  - This second backup system can be something as simple as just copying your most critical files to a USB stick (label it!) and put it in your home safe
- Check your backups periodically to make sure you can read important data
  - Especially if you're using a USB drive for your backups, you should frequently check to ensure that you can read important data from the drive

Working from Home

If you normally work in an office and you and your staff are suddenly going to shift to working from home, there are only a few options that are reasonably secure and possible without professional IT assistance. There are many, many insecure ways to enable working from home, so if you're uncertain, the best and simplest recommendation is to get professional help. If you feel confident doing this yourself, I'll outline two viable options you can implement on your own.

First, some ground rules

All the same rules that you're learning about good hygiene, social distancing, self quarantine, etc., apply to computers (see the appendix for the full analogy).

Three viable options for working from home

1. Use a work computer to view the screen of your desktop computer at work
2. Use a home computer to view the screen of your desktop computer at work
3. Talk with an IT professional if you want to do something different

Option 1 – More expensive, but more secure – Use a work computer

If your business has a small staff and you have business owned and managed laptops that can be handed out, then this may be a viable option for you.

- Create an account with one of the following companies - Teamviewer, Splashtop, GoToMyPC or Google. Be sure to use a unique and strong password and ideally also set up 2FA.
- Install their software on each laptop and on each desktop computer in the office
- When you login to the app on the laptop, you should be able to click on your work desktop and then moments later see your desktop

Option 2 – Cheaper, but less secure – Use a home computer

If you don't have work laptops, then using a home computer to access your work desktop computer is going to be your only viable option. To be clear, **this is not your most secure option**, because we assume that home computers are much more likely to be infected with something.

The process for setting up remote access is exactly the same as in Option 1.

Option 3 – Work with a professional

Your best option will always be to work with an IT company that has a strong and credible security focus. They can help you navigate all the available options and propose and/or implement the right solution for your specific circumstances.

A Quick Note on Cloud Services

Many companies are beginning to use cloud services, with Microsoft's Office 365 and Google's G Suite, being very common choices. Many businesses think that the cloud provider is taking care of all the security stuff, so they don't have to worry about it. Unfortunately, this this is a false sense of security. The current cloud service security model places the burden of security on the weakest links in the whole cyber security system, namely people, PCs and password choices. If your business chooses to use cloud services, you must be even more diligent about protecting people, PCs and passwords and you should absolutely enable 2FA whenever it is available.

Conclusion

If you are a small business owner that does not currently have IT professionals actively managing your business IT infrastructure, it is still possible for you to significantly improve your cyber security preparedness and even to enable yourself and your staff to work from home. Again, these measures are intended as quick, low cost wins in the midst of a crisis.

Once you emerge from the crisis (hopefully unscathed!), I highly recommend that you speak with a Managed Services Provider. A good MSP will be able to provide expert IT guidance, support and active management of your entire business IT environment.

Appendix: Analogy showing how cyber security follows similar rules to Covid-19 response

- You can't see the virus/malware without testing, so any computer that is not professionally managed should be a presumptive case
- You don't want your work computers to be infected through contact with your home computers, so avoid having the two "touch" each other
    - Transferring/sending a file from a compromised computer to an uncompromised one is a form of "touching" and can spread the infection
    - Connecting home and business networks directly together is a form of touching
- If you have multiple people working from home, you don't want their home networks to be able to touch the home networks of other staff. This violates socials distancing.
- If a work device, like a laptop, is going to be used from home, it needs to practice good security hygiene, just like if you were visiting a sick relative in the hospital. This means the work laptop should have:
    - Software firewall enabled
    - DNS firewall enabled
    - All updates applied
    - Not used by family members for general web surfing or playing games
    - Antivirus software enabled and up to date
    - Not logged in as an administrative user
    - Backups working
- If a work device becomes infected, it should immediately be "quarantined". This means detach it from all networks and shut it down. Don't let it back onto any network until it has been treated by a professional. Please don't try home remedies, you'll likely to either give yourself a false sense that you've fixed the problem, or you could make it worse.