Calibre Consulting

Contact us
403-980-8880
info@calibreconsulting.ca

# Busting the Most Common Cybersecurity Myths – Part One

*In Part One of this Two-Part article, we'll be busting four common myths about cybersecurity and how to correct them to ensure you and your company are protected.*

Most people like to think that they have a basic understand of how to keep themselves safe in an internet-dependant world: don't share your passwords, don't open links on spam emails, and don't give your credit card info to self-proclaimed royalty over the internet. Often times, however, all it takes is one mistake for someone to fall victim to a devastating cyberattack. There is also a lot of misinformation around about how to protect sensitive information online, and even when people know how to keep themselves safe, what they know is often not what they do in practice. After all, many of us are guilty of keeping a document full of increasingly difficult-to-remember passwords, even though we've been told to never write them down.

That problem of sporadic best practices on the internet can be compounded when people bring their spotty cybersecurity literacy to work, especially in small and medium-sized businesses. If you want to help dispel the myths and increase the literacy of you and employees, here are four common misconceptions and how to combat them:

## If I Use Password-Secured WIFI, My Information is Safe

Many of us have seen the warning signs from our banks: beware using open WIFI networks in public to do your online banking! Common sense tells us that using an unsecured WIFI network is like a personal information buffet for would-be hackers. However, since the emphasis is so widely (and rightly) placed on unsecured networks, many tend to assume that password-protected WIFI is much safer. This is simply not the case. While taking the extra step of needing a password to access a public network is safer in comparison to nothing at all, it's not much of a deterrent. If you can easily find the password for your local coffee shop, so can someone, either local or remotely, who wants to do you and your data harm.

Nothing will ever be entirely secure in a world with a digital landscape that is constantly changing year after year. However, a good option to increase your defenses while using public WIFI is a VPN (Virtual Private Network). There are many options on the market, both free to use and paid subscriptions, which work by redirecting your internet traffic through a remote server which encrypts all data you send or receive. It bypasses and protects you from an ISP which can see and record everything you do. Nothing is 100% safe, but adding the extra protection of encrypted data directed through a remote server, unattached to you or your location, is significantly more difficult to hack into versus an unprotected (either public or password-secured) WIFI network.

## Incognito Mode Can't Track Me

Private browsing, commonly known as 'incognito mode' for Chrome users, seems to imply that whatever you do while using it can't be tracked. It's 'private' and thus, far more secure than opening up a regular browser window. However, contrary to popular belief, private browsing doesn't actually protect you from much. Google, itself, reveals when you open a private window that "going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit." This revelation isn't any different for Firefox, Safari, Internet Explorer, or any other browser client.

So, what's the point of private browsing? Not much. If you want to invest in a way to fully hide your digital footprint from prying eyes, as much as one can hide on the internet, is by using a VPN. However, if you want to hide your internet history or any information you fill out online from the PC or Mac you're using, incognito mode is the way to go. Private browsing also doesn't allow cookies (small pieces of data that websites use to record a user's browsing activity) to be recorded. So, third party websites like Facebook and Twitter, who use them to track internet usage to better target ads, won't be able to see what you're doing.

## My Password is Strong Enough

If you've had to change your password or sign up to a new site recently, you've probably encountered the aggravating trend of being forced to enter something so complicated you have to write it down or you'll have no hope of remembering it. But surely by forcing everyone to use a password with at least 9 character, 1 number, 1 special character, and 1 uppercase letter means our passwords are impenetrable, right? Not so much. While a 28-digit password with a randomized combination of characters is certainty harder to break into, it isn't impossible. After all, anything can be hacked.

The most up-to-date method of protecting the safety of login credentials is Two-Step Authentication. The process works by confirming a user's identity by using something they know, like a password or pin number, and something they have, like a physical object or second email. A prime example would be the Two-Step Authentication needed to access an ATM machine; a user has a pin number (something they know) and a physical bank card (something they have). This two-step process helps to ensure the account is being accessed by its legitimate owner. Recently, websites have also been using this new process by requiring users to enter their email and password, as well as a randomly generated code sent to their phone upon login.

## My Business Won't Be a Target - We're Not a Big Corporation and We Don't Have Information Worth Stealing

Small and medium-sized companies often assume they're far less likely to be a target of cyberattacks, simply because they're not as well-known as larger businesses. Unfortunately, that is glaringly untrue. Smaller businesses are a favourite target of cybertheft; 43% of cyberattacks are aimed at small businesses, and more than 50% of small businesses suffered a data breach in 2018. The problem lies with access and

willingness to invest in cybersecurity. Small and medium-sized businesses often cannot afford to spend anywhere near as much money to protect its data as large corporations do. Therefore, they're a much more attractive target. When only 14% of small business are ready and willing to defend themselves from a cyberthreat, it's no wonder hackers love playing those odds.

Many businesses also make the mistake of assuming because they're not a bank or a big tech company like Facebook or Twitter, organizations which deals almost exclusively with personal information, they don't have data worth stealing. That is unfortunately untrue. Any business that deals with any sort of client information has a bullseye on its back. This was seen last year in the infamous WannaCry hack, which targeted hundreds of thousands of personal computers around the world, as well as organizations like FedEx, the Russian railway system, French car manufacturer Renault, a handful of universities in China, and many others. One of the scariest, and most unexpected targets, was the NHS; the UK's National Health Service. The ransomware hack lead to the cancellation of 19,000 appointments in the span of 7 days, and locked health care workers out of their computers until a cryptocurrency ransom was paid. Luckily the attack was stopped after emergency patches were sent out by Microsoft, and a kill switch was discovered that prevented further spread of the virus. In the NHS's case, and many others, the problem appeared to be the use of outdated Microsoft software; an unwillingness to spend money on upgrades that ended up costing the UK government "£72 million in subsequent cleanup and upgrades to the NHS's system."

What's the takeaway from all of this? Simple. No matter what type of business you run, you will always have data worth stealing. It's important to take the necessary steps to ensure your software is consistently up-to-date and both you and your staff are literate about cybersecurity. Spending the time and money to ensure you and your business is protected will help mitigate any disasters in the future and help to prevent you from joining the 60% of small and medium-sized businesses who go out of business within 6 months of a cyberattack.

*Are you guilty of any of these cybersecurity misconceptions? Join us next week, when we'll look at four more myths, including the internal threat of cyberattacks and the sneaky evolution of malware.*