Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by: Connectability

Check Your Bank Account DAILY

If you use a credit card for business you need to check your account **DAILY**. Scratch that. If you have a credit card period, you should be checking daily. Or better yet, set up your account so you receive alerts for EVERY transaction.

Over the past 2 months we've had 3 clients tell us that their credit cards were compromised. The scariest part: many of them didn't know until they got their monthly bill.

The faster you catch an issue with your account the easier it is to recover your funds.

Many banks have apps that send you a notification every time a transaction occurs. They can be a bit annoying, but the faster you're aware of a compromised card the better off you'll be in the long run.

March 2018

This monthly publication provided courtesy of Ted Shafran, President of Connectability.

5 Ways Your Employees Will Invite Hackers Into Your Network

Whether they're criminals or heroes, hackers in the movies are always portrayed as a glamorous group. When it comes down to the wire, these are the individuals who crack into the ominous megacorporation or hostile foreign government database, hitting the right key just in the nick of time. They either save the day or bring down regimes, empty the digital vault of the Federal Reserve or disable all the power plants in the country. It's always a genius up against an impenetrable fortress of digital security, but no matter what, they always come out on top.

In real life, it's rarely that difficult. Sure, if you look at the news, you might believe hackers are close to their Hollywood counterparts, stealing data from the NSA and nabbing millions of customer records from Equifax. But the majority of hacks aren't against the big dogs; they're against small to mid-sized businesses. And usually, this doesn't involve actually hacking into anything. A lot of the time – approximately 60% according to the *Harvard Business Review* – an unwitting employee accidentally leaves the digital front door open.

The biggest threats to your company aren't teams of roaming hackers; they're your employees. Here's why.

1 They'll slip up because they don't know any better.

With the proliferation of technology has come an exponential rise in digital threats of such variety and complexity that it'd be impossible for the average person to keep track of it all. Each of your employees' lives are a labyrinth of passwords, interconnected online accounts and precious data. If their vigilance slacks at any point, it not only leaves them vulnerable, but it leaves your company vulnerable as well. For this reason, most cyber-attacks come down to a lack of cyber security education.

Continued on pg.2

Continued from pg.1

2 They'll let you get hacked on purpose.

It's a sad fact that a huge portion of digital attacks are the result of company insiders exposing data to malicious groups. Whether it's info vital for your competitive advantage, passwords they can sell to hacker networks to make a quick buck or sensitive data they can make public simply to spite your organization, it's difficult to protect against a double agent.

3 They'll trust the wrong person.

For many hacks, little code is needed whatsoever. Instead, hackers are notorious for posing as a trusted member of your own team. And if you believe that you'd be able to spot an impostor from a mile away, you may want to think again. Not only is it easier than ever to crack individual users' e-mail passwords and login credentials, but personal info is now littered throughout social media. A simple visit to Facebook can give a hacker all they need to know to "social hack" their way into the heart of your business.

4 They'll miss red flags while surfing the web.

Clickbait is more than a nuisance plaguing your social media feeds. It can be a powerful tool for hackers trolling for easy prey. If an employee doesn't understand what exactly makes a site or link look dubious, they may open themselves – and your company – to browser exploits or other types of attacks.

5 They're terrible at passwords.

According to Entreprenuer.com, "3 out of 4 consumers use duplicate passwords, many of which have not been changed in five years or more." Even more of those passwords are simply weak, inviting easy access for unsavory elements. Many people brush off the importance of strong passwords, but the risks posed by the password "123456" or "password" cannot be overstated.

"It's a sad fact that a huge portion of digital attacks are the result of company insiders exposing data... But there is one way you can make a concrete change that will tighten up your security more than you realize: educating your people."

When it comes to defending your precious assets against digital threats, it can seem impossible to protect yourself at every turn. But there is one way you can make a concrete change that will tighten up your security more than you realize: educating your people. Through a comprehensive security training program, including specific examples of methods hackers use – particularly phishing – you can drastically minimize the risk of an employee accidentally opening up a malicious e-mail or posting sensitive info. When you make a concerted effort to make the entire organization vigilant against cyber-attacks, you're much less likely to be targeted.

Free Report: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

This report will outline in plain nontechnical English common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, as well as providing an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at www.connectability.com/protect or call our office at (416) 966-3306

Shiny New Gadget Of The Month:

FIXD

When was the last time you turned on your car, pulled out of the driveway and suddenly noticed the engine light pop up on your dashboard? You probably just ignored it and drove to your destination. Maybe the next day you spent some time trying to get to the bottom of the issue, only to come up short. Everything seems fine, so what's going on?

A new device called FIXD aims to figure that out. After plugging in the $59, palm-sized widget into your car's onboard diagnostics port – the same one mechanics use to find potential issues – it can communicate with a free app to tell you precisely what's wrong with your vehicle. You can determine why your engine light is on, how serious the problem is, and whether it requires emergency repairs, all without risking being ripped off by shady mechanics. If necessary, the device can actually turn off your engine light right from the app, making it a nuisance of the past.

So You've Been Breached… Now What?

The effects of a data breach can't be overstated. Even with all the prevention in the world, a good hacker can sometimes find their way into your network. Security is asymmetrical, while you need perfect defenses, a cybercriminal only needs a tiny hole to get into your network.

Unfortunately, because of the asymmetric nature of security, sometimes breaches do occur. So you've been breached. What should you do now? Here are 5 things you should do ASAP:

1) Determine what was stolen

You'll need to pin down exactly what information was in the data breach. Sensitive information falls into three general categories:

Least sensitive: names and addresses. You can find most of this data online so this is pretty harmless.

More sensitive: email addresses, dates of birth, and payment-card account numbers

Most sensitive: social insurance numbers, online-account passwords, financial account numbers and payment security codes

A password combined with an email address can easily be used to hijack online accounts, and with your SIN and name almost anyone can pose as you. Unfortunately, it's also very difficult to replace your SIN.

2) Change all affected passwords

If any of your accounts are compromised, change your password RIGHT AWAY. And if you used the same password for any of your other accounts, change those as well, and create a new, strong password for each and every account.

If you're concerned about forgetting passwords there are many inexpensive or free password management systems with military grade security. You can save your passwords there so you only need to remember one.

One more tip, if any accounts offer two-factor authentication use it! Even if a thief has the right password they can't get in because they won't have the code that is sent to your phone.

3) Contact Relevant Financial Institutions

If a bank-card number is stolen, contact the bank or institution that issued the card immediately. Make sure you speak to a live human representative. Explain the situation and ask them to alert you if they detect suspicious activity.

As long as you notify the bank or card issuer before fraudulent transactions take place, or very soon afterwards, you're covered. The longer the fraud goes on the less likelihood you have of recovering your funds, especially with debit cards since they carry less protection than credit cards.

4) Contact a credit-reporting bureau

Contact the major credit-reporting agencies and ask each to place a fraud alert on your name. That way is someone tries to use your identity – for example by taking out a mortgage in your name – you'll know. Equifax and TransUnion are the largest and most well-known credit-reporting bureaus in Canada.

5) Sign up for credit-monitoring

Canada's credit bureaus, as well as many credit card issuers, offer credit monitoring services. These services provide you with a notification every time there is an update to your credit file, such as a credit card application. There is usually a small cost associated with these services.

One final consideration:

Most people only find out about a breach after they receive a fraud alert from their bank, or notice a strange charge on their statement. Unfortunately confidential information is often on the Dark Web, just waiting to be snatched up by a cybercriminal.

There are a number of scanning tools that constantly monitor the Dark Web for stolen credentials and will notify you right away if any of your information is found. That way you can change passwords, and check you accounts immediately to reduce the effect of any leak.

Consumer grade solutions may be acceptable for an individual, but if you run a business we highly recommend using something enterprise-grade. In the wake of some major cyber breaches we've determined these tools are critical to holistically protecting your network.

We offer **Dark Web monitoring** to all of our clients. The cost is very reasonable and it could end up saving you a lot of money AND time. As they say "an ounce of protection is worth a pound of cure".

The 5 Chrome Extensions We Can't Live Without:

Almost two-thirds of internet users choose Chrome for their browsing needs, but many don't take advantage of the add-ons that take it from good to great. If you're new to the extensions game check out this list to learn about the 5 Chrome extensions we can't live without:

The Great Suspender: Are you a "tab hoarder"? If so this is the extension for you. It "suspends" any Chrome tabs you've left unchecked for a certain amount of time. As someone who has over a dozen tabs open at any time *The Great Suspender* is something I use daily. Without it my computer would be slow as molasses. When you want to revisit a page just click the tab and it springs back to life. You can also whitelist tabs you don't want suspended.

HabitLab: Almost everyone has some type of media addiction. It could be Twitter, Facebook, Netflix or YouTube. With HabitLab you select "Goal" sites you want to spend less time on, then choose "nudges" to reduce your dependency. One nudge called "1Minute Assassin" kills tabs after 60 seconds, another "Scroll Freezer" prevents scrolling after a certain number of scrolls, while "The Supervisor" displays the time spent on a goal site. HabitLab also includes metrics so you can track your improvement. If you want to regain control of your browsing give HabitLab a try!

Pocket: If you travel a lot you probably spend lots of time listening to music, reading books, or watching TV/Movies, but there is a better way. I regularly come across an article or video that sound interesting, but I don't have time to read or watch immediately. Pocket allows you to save articles, videos, or pretty much anything so it's visible from your phone, tablet or computer later. Plus Pocket recommends articles based on your interests. You can even select a font type and size. The best part: you don't need an internet connection!

Honey: Every time I buy something online I inevitably end up scouring the web for a coupon code. It takes time, and I often find nothing. Honey takes care of all of that. Simply checkout and Honey will let you know if coupons are available. It doesn't always find one, but when it does you can often save between 5% and 30%. Not bad for doing nothing.

1Password: If you don't have a password manager you need one. Some options include LastPass, Dashlane and 1Password. Without a manager, most people use the same easy-to-crack password for every account. If just one account is breached a hacker has access to all of your confidential information. All the major managers have Chrome extensions which make them easier to use. You can do all the same things with the desktop application, but it's often easier to use the extension rather than switching back and forth to the application.

Want To Win A $25 Gift Card?

Answer the following question to win a $25 gift card to The Keg. Now, here's the trivia question.

What does SSL stand for?

A) Superuser System Login
B) Secure Socket Layer
C) System Socket Layer
D) Secure System Login

Call now with your answer! 416-966-3306

MYELOMA CANADA

In honour of Ted's beloved cousin Tom Guttmann, we will be donating to **Myeloma Canada** this month.

Their mission is to improve the lives of Canadians impacted by myeloma by accelerating access to care through awareness, education, advocacy, community engagement and clinical research.

If you're interested in contributing we'd love to hear from you. Email us at **info@connectability.com** or call our offices at **(416) 966-3306**