Simplicit Tech News

It's the **New Year** and that means a fresh start. Whether you have personal resolutions or business goals in mind that you want to achieve, there is no better day to start than today!

Here at **Simplicit Technologies,** we can help you achieve some of that! Whether you are looking to upgrade your hardware, or increase Cyber Security awareness, we are here to help.

Learn how 14 Canadian banks were **spoofed** and their **customers credentials compromised** in a span of 2 years!

We are running a **FREE iPad** promotion! For more details, see bottom of **page 2** of this newsletter.

January 2020

This monthly publication provided courtesy of **Eyal Bishri**, CEO of Simplicit Technologies.

Our Mission :
"Helping people by simplifying their use of technology"

The Shocking Truth Behind the Growing Cybercrime Threats you Face...

and What You Can Do NOW to Protect your Company

One of the biggest challenges that the world is facing right now and will be a much bigger threat in the future is **Cybercrime**.

Cybersecurity Ventures stated that by 2021, digital crime will **cost businesses a total of $6 trillion,** up from $3 trillion in 2015.

In 2018, Marriott hotel's reservation system had been compromised. Millions of clients records, credit cards and passport information were captured by hackers, **costing Marriott hotel $28 million**.

Cybersecurity Ventures predicts 75 percent of the projected world population of 8 billion will be on the internet by 2022. The internet connection is growing so fast, faster than it takes to properly secure it.

It's not just monetary. Cybercriminals have the ability to control multitude of things, and that includes medical devices, home appliances, and even cars. In 2015, hackers got into a 2014 Jeep Cherokee and were able to control the steering wheel, disable the brakes, and shut down the engine.

Right now, the Internet is flooded with sensitive data. From passwords to financial information – it's out there. Some of it is secure, some of it isn't. Either way, because of the sheer amount of data floating out there, **cybercriminals have a greater chance to get what they want**. And over time, it becomes harder to protect that data.

Harvard Business Review looked at the reasons behind **why many businesses don't take cyber security seriously**. The results were interesting.

It turned out, businesses don't treat cyber security as "the ongoing process that it is."

Continued on pg.2

Continued from pg.1

Instead, it's typically treated as a "finite problem that can be solved."

In other words, if you do the bare minimum for security today, the thinking goes, you'll be protected tomorrow.

The problem is as the Internet changes and evolves, so do the threats against its users. It's pretty much impossible to set up a one-and-done security solution. If you were to set up something like an SMB "quick fix" and walk away, there's a good chance your business would be the successful target of an attack within a matter of months. This kind of thinking is far more costly than many business owners realize. A study by Akouto and Alpha Logistics found that **businesses that underinvest in cyber security end up spending more on cyber security in the long run** as they deal with attacks – up to 58% more. These costs don't even include downtime or lost wages caused by data breaches. In short, recovering from an attack is FAR more expensive than investing in security now.

So what can you do to protect your business? You can start with changing the way you think about cyber security. You have to accept that the threats are out there and will always be out there. But there are things you can do to minimize those threats.

Start with your people. For many businesses, especially those smaller than Fortune 500 companies, **your biggest threat is right inside your organization**. For those of us who are Internet-savvy, most would never dream of clicking on a scammy link or responding to a phishing e-mail. We've been around the cyber block and we know what to look for.

However, people still fall for even the most basic scams.

There will always be someone on your team who isn't informed about these kinds of threats, or those who use obvious passwords. *ZDNet* points out that "only 26% of workers know what to do in the event of a breach" and that "7% openly acknowledge that they ignore or go around security policy."

It pays to invest in a thorough and ongoing training program. It's crucial to outline clear and firm security protocols so your team knows EXACTLY what to do. No one's left guessing or clicking on anything they don't recognize.

It's also crucial to not go it alone. The single best way to stay on top of all things cyber security is to hire a highly experienced managed services provider who is up-to-date on the threats you're facing. Having a partner means you don't have to assume your business is protected. You'll *know* your business is protected.

Help Us Out and We'll Give You a Brand-New iPad as a Token of Our Appreciation

If you're happy with **SimplicIT** services we want to give back to you. A huge part of our goal is to grow the **SimplicIT** family and offer our services to other companies. Finding an IT provider that is the right fit can be difficult for any organization. When you refer our services, they will get the peace of mind for choosing a trusted IT provider. When our services are recommended by you, we want to make sure that you're rewarded for helping our family grow.

Simply refer any company with 10 or more computers to our office to receive a **FREE computer network assessment**. If the company signs a 12 month contract, we will **rush YOU a free iPad** as a thank-you.

Simply call us at **800-245-5210** or e-mail us at **contact@simplicit365.com** with your referral's name and contact information today!

Are Hackers Selling your Credentials?

Are you aware of the **Dark Web**? The **Dark Web** refers to a portion of the internet that is intentionally hidden from search engines.

On the **Dark Web**, people operate anonymously. This allows hackers to hold a wealth of people's credentials and perform illegal activities.

The Risks are Real!

- 150 Million is the average cost of a single data breach in 2020
- 60% of businesses shut their doors after a cyber-attack.
- 50% of small businesses have already experienced data breach in the past 12 months!

Get the peace of mind that your credentials, company financials, and customer records are 100% SAFE!

Simplicit Technologies offers a FREE initial scan to our customers! Contact us for more details at (800) 245-5210.

2 Year Phishing Attack on Canadian Banks

Recently, customers of Canadian banks have been attacked by cybercriminals in a large-scale phishing campaign. The attackers spoofed the banks' website , replicated the landing page , and created a domain very similar to the original site that only differed by a few letters.

The link to the fraudulent website was sent on a mass email to all the bank customers. When the users clicked on the link, it directed them to the fraudulent website. The users were then instructed to enter their log-in and password information, which were captured by the scammers.

The credentials captured were used to transfer funds to scammer-controlled financial accounts.

In this phishing campaign, the emails that were sent to customers contained a PDF attachment, which have the tendency to be trusted more at a higher level than those of Word documents and spreadsheets, which are editable.

Specifically, the PDF attachment contained a hyperlink, which the users were instructed to click. Email security solutions usually scan these type of hyperlinks, but since it's located inside the document instead of the body of the email, it was not detected. The users were advised that they are required to update their digital certificate if they want to continue using their bank's online services.

The attachment also contained a security code, that were required when they log in. A warning prompted users that they only have (2) days to enter the code or it will expire, effectively locking them out of their account. Messages of this type create a sense of urgency with the user.

These tactics are very common. It is surprising, but not uncommon, that this specific phishing campaign had gone undetected for two (2) years. There were 14 Canadian banks victimized including: TD Canada Trust, Royal Bank of Canada, and BMO Bank of Montreal.

The fraudulent websites have since been taken down. Similar scams in the future conducted by cybercriminals can be avoided if the proper precautions are taken, and users are brought up to speed regarding these threats.

From:

Simplicit Technologies
22222 Sherman Way
Suite # 200
Canoga Park, CA 91303

Postage

To:

3 Tips You Need To Know To Protect Your Small-Business Data So You Don't Get Hacked

Change passwords every 90 days.

If you use the same password for everything (and you've been using that password for years), there's a good chance that passwords and related usernames have been stolen. When you don't change your password, you put yourself at HUGE risk. Thankfully, password managers like LastPass and 1Password make it easy to keep your passwords updated and secure.

Use two-factor authentication (2FA).

Many services offer 2FA as an optional login feature. The problem is, they can't work if you don't use them. There are many types of 2FA, such as SMS text verification, PINs and biometrics, such as fingerprint or facial recognition.

Invest in employee education.

Your team should always know what's going on in the world of cyber security. They need to be very aware of phishing e-mails, fraudulent links and the importance of keeping their password updated. Understanding these topics means your team is better equipped to deal with these issues as they arise.