TECHNOLOGY TIMES

Insider Tips To Help You Run Your Business **Better, Faster, Easier** And More **Profitably**

IN THIS ISSUE

WHAT'S NEW?

Well, folks, Cyber Security Awareness Month has been shelved once again until next year! Thank you for following along with our month's long CSAM campaign. We had a lot of fun doing what we do best on social media - sharing all of the best cyber-security tips to help keep you safe.

An extra special thank you goes out to those who attended our grand finale: the Avenir IT Spooktacular Webinar. It was not only fun, but it was also a resounding success! Viewership was at a record high thanks to Paige, for its great organization. Not only did she plan a fun afternoon, she also turned out to be a fang-tastic host! Mathieu was just as awesome as our presenter.

For those who may have missed the webinar and would like to see it, it can be found in full on our YouTube channel Avenir IT Inc.

avenirit

WHAT IS THE "DARK WEB"?

The Dark web is a common term that we hear a lot these days on the news or TV shows we watch. It's a term often used to describe the source of all online cyber-crime – but what does it actually mean?

Think of the dark web as an online black market. You can purchase drugs, counterfeit bills, credit card numbers, hacked login credentials to web applications, fake ATMs and so much more. The term "Dark Web" has become a catchall term used for any illegal online activity that is not generally accessible through a normal web browser and internet searches.

So – if you can't access the dark web through a typical web browser, how can you access the dark web? Typically – this is done using a free anonymizing browser called TOR. TOR stands for "The Onion Router" and it uses multiple connection relay to keep your connection as private and secure as possible. Using TOR is not illegal – if you are not using it for malicious purposes. In fact, TOR's mission is to help their users protect themselves online from prying eyes, malicious surveillance and maintain your privacy online. Unfortunately, these tools work so well that it also enables cyber-criminals to anonymize themselves and complete illegal activities for profit.

It is important to note however that not everything on the dark web is necessarily bad. In fact – many individuals in foreign countries will access the "dark web" to share information or opinions that could have them persecuted by their own government. Even the BBC has an online presence on the Dark Web for this exact reason.

Understanding a data breach

A data breach is typically perpetrated

avenir it

with

The Chamber

The Winnipeg Chamber of Commerce

Last month, we were fortunate to set up a booth at the 2021 Small Business Summit, hosted by The Winnipeg Chamber of Commerce in honour of Small Business Week. Our Marketing Assistant, Paige, had an awesome time mixing and mingling with fellow small businesses. She says the day could not have gone better! A big thank you goes out to The Chamber for hosting and for having us.

by a single or a group of cyber-criminals. Often, the cyber-criminals that steal your data or that are responsible for large data breaches will not use this data personally – but instead will sell it to make a profit. This is where the dark web comes in.

Using an anonymous marketplace on the Dark Web, cyber-criminals can list their stolen information for anyone to purchase. When your information is stolen or compromised in a data breach, it's not just one cyber-criminal you need to worry about using your data, it's thousands from around the world that purchase your data and use it as they wish.

Different data sells for different prices

A conservative estimate in 2018 reported that cyber-crime generated at least $1.5 trillion dollars and that number is quickly growing every year. Individual hackers may earn around $30,000 for one job.

Here are other valuations of stolen data:

- Bank cards valued at $1000: $79.
- Personal information: $13
- Forged passport: $700
- Driver's license: $800
- PayPal account worth up to $12,000: $1,200.
- The entire database of over 50,000,000 records of MyFitnessPal: $4,218

Protecting yourself from the Dark Web

Information such as passwords purchased on the dark web can be the cause of your company's data breach.

Unfortunately, we cannot stop all data breaches, especially when many times these breaches are caused by other companies with no fault of our own. So how can we protect our information?

The key is to always be one step ahead. Rather than reacting to a breach, take a proactive approach to protecting your data. Always use strong passwords and never reuse them across other sites. If you're not planning on applying for a loan anytime soon, consider putting a credit freeze or credit lock on your account.

Finally, additional tools are available to monitor your information on the dark web. Work with your IT provider to learn about how they can help monitor your information so if it is found on the dark web, you will be the first to know.

Everything Avenir IT has assisted us with and suggested has been perfect for us! We are very happy that we made the decision to engage with Avenir IT. A good friend of ours, Nathan at Imperial Cabinets, put us onto them and we are thrilled.

Dr. Kelly Enns
Optometrist
Sage Creek Eye Centre

Business Email Compromise (BEC) is not a new term. BEC scams have been growing in popularity for some time now. If you're not familiar with BEC, it's when a fraudulent email is sent to a company or individual, and the email appears to be from a legitimate business resource or person, often varying from the legitimate email address by just a letter or two. There may be instructions within the scam email for the recipient to transfer money, purchase gift cards, click on a malicious link, or perform some other activity at the behest of the sender. Unfortunately, BEC scams often put the recipient at a disadvantage because they see the name or title of the sender and react quickly, or are hesitant to question authority.

So, what's the secret sauce that cybercriminals use across the board when launching their attacks on unsuspecting victims? According to report from Barracuda, it's surprisingly simple and straightforward: legitimate email accounts.

Let's elaborate on that. Barracuda found that hackers launched 100,000 BEC attacks on over 6,000 organizations by using 6,170 legitimate email accounts (which of course, were created with malicious intent). We're talking Gmail, AOL, and other verified email services.

The report further outlines the details of the attacks, identifying that 45% of the BEC attacks were carried out with these email accounts. It appears that Gmail is the platform of choice with 59% of the accounts originating there. This may be a result of the cost to create an account (it is free), the ease of registration of a new account, and the solid reputation that a company like Google carries – meaning it is much more likely to pass through security filters.

Change in Identity

While the email account will remain the same, the sender name does get updated from time to time by the cybercriminal in order to go unnoticed by the recipient. These accounts are not often used for more than a 24-hour period and then will go dormant for a while to lessen suspicion or if it has been flagged already, to reduce the likelihood of being detected by another server. That doesn't mean it goes away forever. Like your MySpace account, it stays out there in cyberspace waiting to be revisited.

Phishing for… Anything

Again, BEC scams are not new and they are just a small 'subdivision' of the much bigger issue of phishing – the single most used point of entry to a company in order to breach the data contained within the business infrastructure. And with the cost being minimal (basically it is free to do) and return on investment being potentially huge, the risk far outweighs the benefits.

Ongoing training is one of the best ways to arm employees and clients with the right tools to catch the phish.

Hottest Holiday Tech

The holidays are on the horizon and Black Friday will be here sooner than you think! We all know that gifting the latest and greatest tech is sure to make you a holiday hero, so we thought we'd take this opportunity to share some of 2021's coolest gadgets.

Modern Sprout Smart Growbar - For the plant mom or dad in your life, the Smart Growbar Supplemental LED light can allow you grow lush plants in even the darkest corners of your home.

Drinkworks Home Bar by Keurig - Everyone knows about Keurig Coffee Pods, but did you know that they also make Drinkworks Cocktail Pods? No more need for you to be a skilled mixologist with a stocked bar to thoroughly impress your next dinner party guests.

Roborock S6 Pure Robot Vacuum and Mop - You've heard of Roombas taking the hassle out of sweeping, but have you heard of the Roborock? Not only is this app controlled robot, a vacuum, it also works as mop! Now who doesn't love the sound of that?

Meural Canvas II - Why invest good money in a single art piece when you can purchase the Meural Canvas digital art frame instead. This inconspicuous, high quality wireless frames allows you to change your home's art with your mood! Bonus: no need to reinvest in art if you redecorate.

3 Tips To Help You Avoid Leadership Burnout

As a leader, you must be proactive about managing your stress, because when it is left unchecked, it can lead to burnout. Burnout is a workplace "phenomenon" that occurs due to chronic stress. Fortunately, there are many ways you can avoid burning out as leader. Here are some tips, and while they may seem like common sense, you'd might be surprised at how many leaders pay the price for waving them off.

1. As a leader, you need to get used to delegating. Too many leaders assume that they are the best ones to every task. This mindset will inevitably lead to burnout. Instead of assuming you are the best person for every job, train your team members to take on some of your responsibility. There should only be a handful of tasks that must be done by you, and that's where you should focus the majority of your efforts.

2. To avoid burning out, you must make your mental and physical health a priority. When you don't feel good, you're more likely to feel stressed. You're also less likely to perform well. So, instead of sacrificing your health for the sake of work, start thinking of yourself as a business asset.

3. Lastly, be sure to take regular time off from work. When you have days off, avoid every temptation to continue working, such as answering emails or taking work calls. Rather, use this time to enjoy some of your favorite activities and to see the people you care about. You should also prioritize regular vacations, even if you can't travel. Vacations are an opportunity to recharge and return to your work feeling refreshed, so don't make excuses to avoid them.

Adapted from "Avoiding Leadership Burnout" by Keithen Washington

8 Tips To Protect Yourself When Holiday Shopping Online

1. Shop reliable websites and get there safely. Don't be fooled by the lure of great discounts by less-than-reputable websites or unknown sellers. Use the sites of retailers you know and trust and get to their sites by directly typing a known, trusted URL into the address.

2. Beware of seasonal scams. Fake package tracking emails, fake e-cards, fake charity donation scams, and emails requesting that you confirm purchase information are common this time of year.

3. Conduct research. Read reviews and see if other customers have had positive or negative experiences with them. Verify the website has a legitimate mailing address and a phone number for sales or support-related questions, if the site looks suspicious, call and speak to a human.

4. Always think twice before clicking on links or opening attachments -- even if they appear to be from familiar sources. Messages can easily be faked.

5. Keep clean machines! Before searching for that perfect gift, make sure your device, apps, browser, and anti-virus/anti-malware software are patched and up to date. Never make purchases using public WIFI.

6. Protect your passwords. Make them long and strong multi-factor authentication (MFA, also called two-factor or 2-step authentication) wherever possible.

7. Look for https:// (not http) in the address bar before using your credit card online. The 's' tells you the web page has privacy protection installed and will mask any data shared. Ensure the lock symbol is present as well.

8. Check your credit card and bank statements regularly. These are often the first indicators that your account information or identity has been stolen. If there is a discrepancy, report it immediately.