Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by: Connectability

Welcome Lucy To The Team!

We thought it was time to introduce you to Lucy, the friendliest, happiest, and most enthusiastic Customer Service Rep we've ever had!

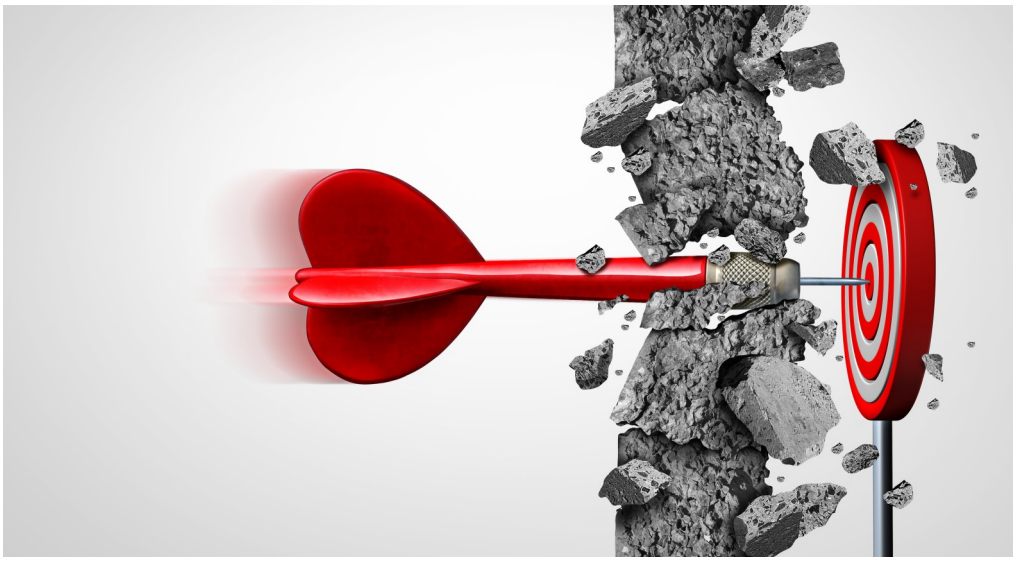
Lucy just turned 2 and is really getting the hang of the job! She's only part-time, but her main duties include:

1) Fetching tennis balls
2) Catching ZZZZZ's
3) Searching for crumbs
4) Greeting visitors with kisses
5) And of course, going for walks in the park

We hope you'll join us in welcoming Lucy to the Connectability team!

July 2018

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



Top 4 Ways Hackers Will Attack Your Network

And They Are Targeting You RIGHT NOW

Most small and midsize business (SMB) owners exist in a bubble of blissful ignorance. They focus on the day-to-day operations of their organization, driving growth, facilitating hiring and guiding marketing, without a single thought given to the security of the computer networks these processes depend on. After all, they're just the little guy – why would hackers go to the trouble of penetrating their systems for the minuscule amount of data they store?

And eventually, often after years of smooth sailing through calm seas, they get hacked, fork over thousands of dollars to malicious hackers, and collapse beneath the weight of their own shortsightedness.

The facts don't lie. According to Verizon's annual Data Breach Investigations Report, a full 71% of cyber-attacks are aimed squarely at SMBs. And while it's unclear exactly how many of these attacks are actually successful, with the sad state of most small businesses' security protocols, it's a safe bet that a good chunk of the attacks make it through.

But why? As Tina Manzer writes for Educational Dealer, "Size becomes less of an issue than the security network … While larger enterprises typically have more data to steal, small businesses have less secure networks." As a result, hackers can hook up automated strikes to lift data from thousands of small businesses at a time – the hit rate is that high.

Today, trusting the security of your company to your son-in-law, who assures you he "knows about computers," isn't enough. It takes constant vigilance, professional attention and, most of all, knowledge. Start here with the four most common ways hackers infiltrate small businesses:

1. PHISHING E-MAILS
   An employee receives an e-mail directly from your company's billing company, urging them to fill out some "required" information before their paycheck can be finalized. Included in the very professional-looking e-mail is a link your employee needs to click to

Continued on pg.2

Continued from pg.1

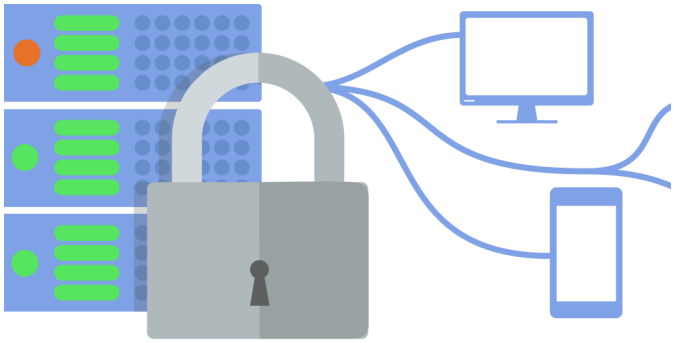
complete the process. But when they click the link, they aren't redirected anywhere. Instead, a host of vicious malware floods their system, spreading to the entirety of your business network within seconds, and locks everyone out of their most precious data. In return, the hackers want thousands of dollars or they'll delete everything.

It's called Ransomware and it's nasty. Getting people to open a link is one of the oldest tricks in the hacker toolbox, but today it's easier than ever to gather key information and make a phishing e-mail look exactly like every other run-of-the-mill email you receive each day. Train your employees to recognize these sneaky tactics, and put in safeguards in case someone messes up and clicks the malicious link.

2. BAD PASSWORDS
According to Inc.com's contributing editor John Brandon, "With a $300 graphics card, a hacker can run 420 billion simple, lowercase, eight-character password combinations a minute." What's more, he says, "80% of cyber-attacks involve weak passwords," yet despite this fact, "55% of people use one password for all logins."

As a manager, you should be bothered by these statistics. There's simply no excuse for using an easy-to-crack password, for you or your team. Instead, it's a good idea to make a password out of four random common words, splicing in a few special characters for good measure. To check the strength of your password, type it into HowSecureIsMyPassword.net before you make it official.

"...hackers can hook up automated strikes to lift data from thousands of small businesses at a time — the hit rate is that high."

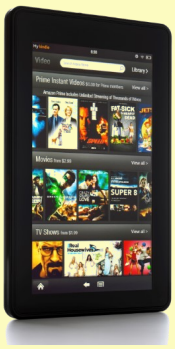


3. MALWARE
As described above, malware is often delivered through a shady phishing e-mail, but it's not the only way it can wreak havoc on your system. An infected website (such as those you visit when you misspell sites like Facebook.com, a technique called "typo-squatting"), a USB drive loaded with viruses, or even an application can bring vicious software into your world without you even realizing it. In the past, an antivirus software was all that you needed. These days, it's likely that you need a combination of software systems to combat these threats. These tools are not typically very expensive to put in place, especially considering the security holes they plug in your network.

4. SOCIAL ENGINEERING
As fallible as computers may be, they've got nothing on people. Sometimes hackers don't need to touch a keyboard at all to break through your defenses: they can simply masquerade as you to a support team in order to get the team to activate a password reset. It's easier than you think, and requires carefully watching what information you put on the Internet – don't put the answers to your security questions out there for all to see.

We've outlined some of the simplest ways to defend yourself against these shady techniques, but honestly, the best way is to bring on a company that constantly keeps your system updated with the most cutting-edge security and is ready at a moment's notice to protect you in a crisis. Hackers are going to come for you, but if you've done everything you can to prepare, your business will be safe.

Help Us Out And Get A Brand-New Kindle Fire Tablet Your Trouble



We love having you as a customer and, quite honestly, we wish we had more like you! So instead of just wishing, we've decided to hold a special "refer a friend" event during the month of July.

Simply refer any company with 8 or more computers to our office and get $100 off your support bill. If they become a Managed Services customer we'll even give you a free month of service! PLUS the business you refer will receive a FREE network assessment (a $397 value). Once we've completed our initial appointment with your referral, we'll rush YOU a free Kindle Fire as a thank-you (or donate $100 to your favorite charity ... your choice!).

Simply call us at 416-966-3306 or email us at info@connectability.com with your referral's name and contact information today!

Shiny New Gadget Of The Month:

Be A Better Chef With Anova's Precision Cooker

These days it seems like cooking for yourself is going the way of the dinosaurs.

We are increasingly reliant on delivery services and premade meals because of simplicity. The problem is that these meals are more expensive, less nutritious, AND you lose the satisfaction of preparing a delicious meal.

What if there was a way of cooking delicious and healthy food without the added work?

The Anova Precision Cooker does just that! It uses sous vide technology to cook food at the same temp throughout, and with Anova's mobile app you can wirelessly start the device, adjust the temp, and turn it off when your food is ready. That way when you get home your food is ready to eat!

You can get an Anova Precision Cooker for just $129 at: https://ca.anovaculinary.com/

5 Things You Should Know Before Investing In Cryptocurrency

Since Cryptocurrency came into the general consciousness, vague interest has steadily snowballed into a frenzy. The exponential growth of Cryptocurrency and the subsequent new market for investment have also generated a lot of questions and uncertainty.

In recent months Bitcoin reached a high of $19,000 USD, generating serious interest in the investment community. It's since dipped, but the fact remains: investing in Crypto has become a real consideration for the average investor.

With that in mind, here are the top 5 things you should know before investing in Cryptocurrency:

1) Do you research

This might seem obvious, but not every company involved with Cryptocurrency has the knowledge & understanding to continue growing once the market dies down.

Ensure they have a legitimate team, that they aim to solve a specific problem, and that they have some proof of concept or beta.

2) Be Responsible

Cryptocurrency can be part of any investment portfolio, but should still be treated as high risk. Because of the potential for very high returns, people tend to invest heavily in Crypto, but keeping your portfolio balanced is crucial. Crypto should make up only 10-20% of your overall portfolio.

3) Be Realistic

Because Crypto investments receive the most attention when they peak, many people have the false perception that these investments are "sure things". They may seem that way, but think back to the dotcom boom—many companies that seemed infallible no longer exist today.

4) Be Vigilant, borderline paranoid

Most concerns surrounding hacks and security, while well-founded, are also avoidable, even for people who aren't tech savvy. If you're investing on your own make sure you stay up-to-date on industry best practices and news. If that seems overwhelming, invest through a publicly traded blockchain investment vehicle like Block X. But make sure you choose a reputable organization.

5) Track gains and losses

Crypto is still in it's early days, so it doesn't classify as a real investment. That's largely because it's a global, decentralized entity. Regardless, it's still important to track gains and losses on crypto investments. This will help you understand how investments are doing, AND ensure you're in a position to pay your share of taxes if/when regulations change.

TechVibes.com, 5/14/18

Apple Takes Aim At Big Brother

You probably already know this, but Facebook (and many other apps) collects your private data and sell it to targeted advertisers. Unfortunately, to many consumers that just sounds like more of the same. It may be common place, but it doesn't make it right.

That's why Apple is working on a new feature for the next version of iOS, Mojave. The feature will alert you when Facebook or other apps attempt to collect data on you. The update will block social media "like" or "share" buttons from tracking users without permission. That won't always stop them from getting the data they crave, but it does notify you when you're being tracked.

The moral of the story is this: the more information you publish online the more information advertisers will have on you. So be careful about what you disclose. Remember: **big brother is watching**

What To Do BEFORE You Go To Starbucks

You're in the car on the way home from Starbucks, basking in the glow of your triple-shot, low-foam, extra-hot pumpkin spice latte when you suddenly realize your laptop has gone missing. You drive back to the store like a caffeinated lunatic, only to discover no one has turned it in. What do you do?

Well, first you should notify your IT department (us!) immediately to tell them your device has gone missing. That way, we can change passwords and lock access to apps and data. We can also remotely wipe the device to make sure no one will be able to gain access — a key reason it's critical to back up your data daily.

Next, change the passwords to ALL websites you regularly log in to, starting with any sites that contain financial or company data. If your laptop contained others' medical records, financial data, or other sensitive data (social insurance numbers, birthdays, etc.), you should contact an attorney to understand what you may be required to do by law to notify the affected individuals.

An ounce of prevention is worth a pound of cure, so make sure you have our email encryption and back up solutions as well as remote monitoring software on all your mobile devices. Put a pin-code lock or password requirement in place to access your devices after 10 minutes of inactivity, and get in the habit of logging out of websites when you're done using them.

Surefire Ways To Protect Yourself From Data Leaks, Hacks, And Scandals

1. Reconsider what you put online. This goes beyond social media posts. Even sharing your phone number with a store associate can bite you later.
2. Use password managers. This way, you can use different, random passwords for all your sites without forgetting them.
3. Use two-factor authentication. It's a no-brainer.
4. Encrypt the information on your drive. It's easier than it sounds!
5. Read privacy policies, otherwise you may be signing away more than you think.
6. Monitor your credit. That way, if someone tries to use your info to make a big purchase, you can stop them in their tracks.

Inc.com, 4/26/18

The Work Revolution

According to a 2016 study by *Randstad*, 20-30% of the workforce is made up of "non-traditional" (remote) workers. Estimates predict that by 2020 nearly 50% of the workforce will work remotely.

This presents a unique opportunity. It allows businesses to reduce overhead and increase productivity, while improving their ability to attract and retain top talent.

But opportunities often involve risk. If you allow people to work remotely you need a cybersecurity plan that your team is trained on. One more tip: supply company-owned machines. It's much easier to control security on a company-owned device than someone's personal machine.

If you don't have a cybersecurity plan in place, we can help! Just call us at 416-966-3306.

Parkinson Canada

This month we'll be making a donation to **Parkinson Canada!**

Since 1965, **Parkinson Canada** has been providing support services and education to people living with Parkinson's disease, their families, and the health care professions who treat them.

Many of us know someone suffering from Parkinson's and since it doesn't get enough media attention we felt this was too important to ignore.

If you'd like to contribute to this worthy cause we'd love to hear from you! Email **info@connectability.com** or call us at **(416) 966-3306!**