The Tech chronicle

What's New

COVID-19 (Coronavirus)

Cyber Criminals are on the rise more than ever capitalizing on the COVID-19 situation. There are more phishing attempts than ever. With Companies being forced to have employees to work from home has presented major difficulties in keeping security of information protected from these Cyber criminals. Everyone is facing a NEW challenge.

We are here to HELP! We are emailing ***WEEKLY COVID-19 TIPS*** with information to help protect you and your organization. If you are not receiving these, sign up **FREE**:

ESCOffer.com/COVID-19/

April 2020

This monthly publication provided courtesy of Eric Stefanik, President of Elliptic Systems Corporation.

Our Mission: Building and Implementing IT Security Awareness in the Everett to Seattle areas with protective services like Cybersecurity, Business Continuity, Backup Disaster Recovery, VOIP, Cloud Computing, Virtualization and Managed Services.

Employees Are Letting Hackers Into Your Network By Doing These 5 Things …Here Is What You Can Do To Stop It!

If you run a small business, you are a target for cybercriminals. At this point, it's just a fact of life. Hackers, scammers and cybercriminals of all kinds target small businesses because they are plentiful, and more often than not, they lack good cyber security (if they have any at all). Here's the kicker: these criminals don't need to use malicious code or advanced hacking skills to get what they want. In reality, many of them target your biggest vulnerability: your own employees.

It's a sad truth, but every day, employees of small businesses let hackers right in because they don't know better. They see an e-mail from the boss, open it and click the link inside. By the time they realize they've made a mistake, they're too embarrassed to say anything. From there, the problem gets worse. Actions like this can end in DISASTER for your business.

The problem is that most employees don't have the training to identify and report IT security issues. They aren't familiar with today's threats or they don't know to not click that e-mail link. There are many things employees are doing – or not doing – that cause serious problems for small-business owners. Here are five things people do that allow hackers to waltz in through your front door.

1. They don't know better. Many people have never been trained in cyber security best practices. While some of us may know how to protect our network, safely browse the web and access e-mail, many people *don't*. Believe it or not, people do click on ads on the Internet or links in their e-mail without verifying the source.

Continued on pg.2

Continued from pg.1

This can be fixed with regular cyber security training. Call in an experienced IT security firm and set up training for everyone in your organization, including yourself. Learn about best practices, current threats and how to safely navigate today's networked world.

2. They use bad passwords. Many people still use bad passwords like "12345" and "qwerty." Simple passwords are golden tickets for hackers. Once they have a username (which is often just a person's actual name in a business setting), if they can guess the password, they can let themselves into your network.

Many security experts suggest having a policy that requires employees to use strong passwords. Passwords should be a mix of letters (uppercase and lowercase), numbers and symbols. The more characters, the better. On top of that, passwords need to be changed every three months, and employees should use a different password for every account. Employees may groan, but your network security is on the line.

3. They don't practice good security at home. These days, many businesses rely on "bring your own device" (BYOD) policies. Employees use the same devices at home and at work, and if they have poor security at home, they could be opening up your business to major outside threats.

> **"The problem is that most employees don't have the training to identify and report IT security issues."**

How do you fix this? Define a security policy that covers personal devices used in the workplace, including laptops, smartphones and more. Have a list of approved devices and approved anti-malware software. This is where working with an IT security firm can be hugely beneficial. They can help you put together a solid BYOD security policy.

4. They don't communicate problems. If an employee opens a strange file in an e-mail, they might not say anything. They might be embarrassed or worry that they'll get in trouble. But by not saying anything, they put your business at huge risk. If the file was malware, it could infect your entire network.

Employees must be trained to communicate potential security threats immediately. If they see something odd in their inbox, they should tell their direct supervisor, manager or you. The lines of communication should be open and safe. When your team is willing to ask questions and verify, they protect your business.

5. They fall for phishing scams. One of the most common scams today is the phishing scam. Cybercriminals can spoof e-mail addresses to trick people into thinking the message is legitimate. Scammers often use fake CEO or manager e-mails to get lower-level employees to open the message. Criminals will do anything to trick people into opening fraudulent e-mails.

Overcoming these threats falls on proper training and education. Phishing e-mails are easy to spot if you take the time to do it. Look at the details. For example, the CEO's e-mail might be CEO@yourcompany.com, but the scam e-mail is from CEO@yourcompany1.com. It's a small but significant difference. Again, it's all about asking questions and verifying. If someone isn't sure if an e-mail is legit, they should always ask.

Free DarkWeb Scan! Are your companies credentials for sale on the DarkWeb? How much do you know about the DarkWeb?

We are here to HELP! Find out if your company credentials are on the DarkWeb with our **FREE DarkWeb Scan**. The Dark Web is a hidden universe contained within the "Deep Web"- a sub-layer of the Internet that is hidden from conventional search engines. We go into the DarkWeb for you and keep you out of it so you don't add the risk of getting compromised.

Request your FREE DarkWeb Scan here or share this link ($79 Value):

https://www.escoffer.com/darkwebscan/

Simply call us at **425-441-9500** or e-mail us at Info@EllipticSystems.com

We are Here to HELP!

Cyber Criminals are having a hay day with the 'Stay Home, Stay Healthy' order by our Government. Employers are faced with one of two things:

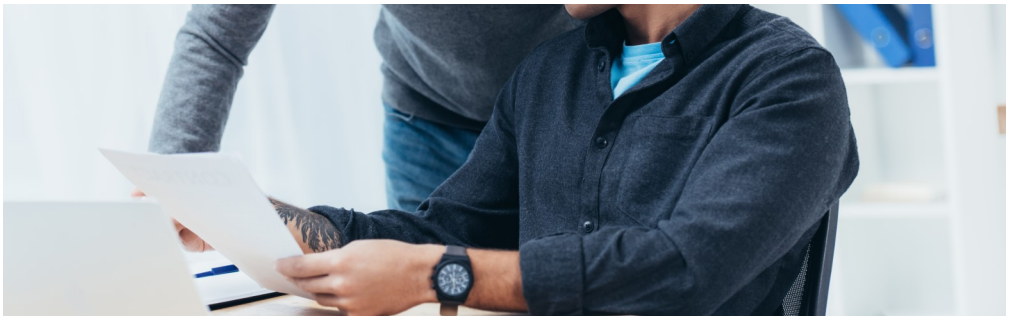
1. Close your business and lose Revenues hoping the Government will bail you out or you end up closed permanently!
2. Set up your Employees to work from home—which presents a massive breach in IT Security!!!

This is the last thing Elliptic Systems wants to see happen. Setting up Employees to work from home is not as simple as handing them a laptop or even worse have them use their personal computer to access company network and data. You **MUST** take precautions to protect your network and retain security protocols, especially if you must keep compliant with HIPAA, SEC, SOX, FINRA and others. I have put together a **'Work From Home Report'** and offering it for **FREE** to you. There is tons of valuable information you may not have thought about. I will also give you my **FREE 'Home Office Action Pack'** that contains customizable documents you must have in place for Employees to work at home.

Request your FREE Work From Home Report here:

https://www.escoffer.com/workfromhome/

The Benefits Of A Mastermind Group



I believe no man is an island. So, I offer this tip: if you're an entrepreneur, you need to be in a mastermind. Being in a mastermind group is one of the most powerful tools to help you increase profitability in your business.

1. What is a mastermind group?
If you aren't familiar with them, a mastermind is a group in which entrepreneurs can mentor each other and help each other grow their businesses. It can be an important catalyst for growth and shaping your business.

The mastermind I run is called the Edison Collective. We get together face-to-face every quarter to expand our business (and occasional musical) knowledge. We share our ideas, solutions, best practices, successes and challenges as entrepreneurs. Most of all, we motivate and inspire each other.

2. What are the benefits of belonging to a mastermind?
While some mastermind groups run on a digital platform, face-to-face meetings are important if they're an option. What I love about being in a mastermind is the connection. We are truly there to learn from each other. No one walks in with their ego. We gather to benefit ourselves and each other by sharing and learning from other entrepreneurial experiences.

To benefit from a mastermind, you must be willing to collaborate, share and learn from each other. At times, it's almost like free coaching. You get sneak peeks at how businesses run behind the scenes, and oftentimes, we take those ideas and implement them in our own practices. And remember, trust is imperative. There is total confidentiality, so feel free to not be a boss for a bit.

I have found that meeting with this group has raised the bar for me. My business is more profitable. I find support from my peers as well as education and resources I may not have been exposed to in the past. Even better, I have another venue for accountability (yup, even I need it!) and a place to share my goals. So next quarter when we meet, I better bring the results!

3. Who can be in a mastermind?
The beautiful thing is that you don't have to join an established mastermind. You can start your own. Find like-minded entrepreneurs who are driven to achieve the same goals and vision you are. Get together once a quarter face-to-face, have open discussions about your business and get your insights from each other.

That right there? Priceless!

MIKE MICHALOWICZ (pronounced mi-KAL-o-wits) started his first business at the age of 24, moving his young family to the only safe place he could afford – a retirement building. With no experience, no contacts and no savings, he systematically bootstrapped a multimillion-dollar business. Then he did it again. And again. Now he is doing it for other entrepreneurs. Mike is the CEO of Provendus Group. He is also a former small-business columnist for The Wall Street Journal, MSNBC's business makeover expert, a keynote speaker on entrepreneurship and the author of the cult classic book The Toilet Paper Entrepreneur. *His newest book,* The Pumpkin Plan, *has already been called "the next* E-Myth*!" For more information, visit MikeMichalowicz.com.*

4 Cyber Security Myths Business Owners Need To Know

Myth: Cyberattacks only come from external sources.
Reality: Upward of 60% of data breaches can be traced back to employee error. They may leave sensitive data on unsecured hardware rather than behind digital walls. They may open malicious files that copy and send data to an external location. Employee IT security training goes a long way to fix this.

Myth: Simple antivirus software or firewalls are enough to protect your business.
Reality: Cybercriminals use sophisticated tools to get what they want. The fewer security solutions you have in place, the easier it is. Antivirus software can't do anything to stop a motivated hacker, and firewalls should never be considered a primary line of defense. Web scanning and malware detection software can give you more protection on top of these.

Myth: Your business is too small or niche to be a target.
Reality: Cybercriminals don't care about the size or type of your business. They target everyone because they know they'll eventually break through somewhere. Small businesses are more appealing because they often lack serious cyber security solutions.

Myth: You don't collect payment or financial data, so you aren't worth targeting.
Reality: They aren't just looking for credit card details. They want usernames, passwords, e-mail addresses and other personal identifying information they may be able to use elsewhere because people have a bad habit of reusing passwords for other accounts, including online banking. *Inc., Dec. 16, 2019*

Top Tips For Making The Most Of Your Small-Business Technology

Embrace mobile. Your customers use mobile, so your business needs to work in the mobile space too. Optimize your website for a better mobile experience.
Good copy goes far. From blogs to social media posts, compelling, well-written copy can go a long way. Share personal stories and success stories and create a narrative for your business online.

Instagram it. If your business isn't on Instagram, it should be. Many of your current and future customers are there. It's a great place to share photos, tell stories and foster connections.

Get more out of SEO. Good header tags, for instance, are a must for good overall SEO. Learn how to get more out of headers and you'll be able to drive more traffic to your website or related webpages. *Small Business Trends, Dec. 1, 2019*

Things Mentally Strong People Don't Waste Time Doing

Overthinking – They look at their situation and take decisive actions. Some look at all the available information and go. Others rely more on their gut. Either way, they keep things moving forward.

Regretting – It's natural to want a different outcome than the one you got or to think, "I should have done X instead of Y." But these thoughts can hold you back and lead to second-guessing yourself later.

Complaining – It can be healthy to complain. It gets your thoughts into the open where they can be discussed. But you have to discuss and arrive at solutions. Complaining for the sake of complaining – or complaining to people who can't help – is unproductive. *Business Insider, Dec. 17, 2019*