



TECHLORE

"Insider Tips to Make Your Business Run Faster, Easier and More Profitable"

INSIDE THIS ISSUE:

Security Alert! Is Your Cyber Protection Up-To-Date? Up-To-Date?	page 1	Two-Factor What?	page 2
Shiny New Gadget Root Robot	page 1	NeoTip of The Month	page 2
4 Steps to Finding Your Company's Diamonds In The Rough	page 2	Free Report Download	page 2
4 Ways Technology Can Make Your Business Meetings More Productive	page 2	Monthly Trivia Question: Win a \$25 Tim's Card!	page 2



"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"
- Jim Stackhouse
NeoLore Networks Inc.

Security Alert! Hackers and Cybercriminals Are Now Concentrating Their Attacks on Your Business! Is Your Cyber Protection Up-To-Date?

Technology exists in a state of constant flux. The most popular gadgets turn obsolete within a

hapless victims than ever before. We read about the most costly of these breaches in the news each

penetrate your business, it's well within the means of most businesses to implement comprehensive security solutions to give your organization a fighting chance.

need to be low-hanging fruit for well-funded and highly organized cybercrime rings. Hackers assume that a business like yours is too tiny and ill-informed to prepare for even a simple phishing scam, and they're usually right. But if every business owner put just a little more effort into securing their data, you can bet attacks would be curbed. And if every small business pledged to implement a professionally managed security protocol, we would see the frequency of these hacks diminish drastically.



It's vital to realize that, unfortunately, security protocols aren't a set-it-and-forget-it proposition. To respond to the evasive and increasingly sophisticated tools being shared throughout the enormous hacker community, you need an equally sophisticated and regularly updating security system. For nearly every one of the 978,000 fresh new malwares developed daily, there are patches and updates designed to address them – strategies and techniques to outsmart even the most devious of criminals.

There's a lot for business owners to think about during a year as chaotic as 2018, but your top priority should be the basic security of your company. Invest your time and resources into building a foundational blockade for potential threats, and you can rest assured that your livelihood is safe from digital collapse.

year or two, the sophistication of the hardware and software we use increases exponentially with each passing month and the digital foundations of modern society are almost continuously supplanted. Every day, there's a new device to contend with, a

morning, including Equifax, J.P. Morgan, Home Depot, Yahoo!, Verizon, Uber and dozens more.

Just because you don't have the resources of a massive corporation doesn't mean you

fresh update and an addendum to the already dizzying array of features at our fingertips.

But these high-profile incidents don't even comprise the majority of attacks. According to Verizon's 2017 Data Breach Investigations

Shiny New Gadget Of The Month: Root Robot

Root is the ideal robot to teach coding to young children. It engages youth by giving them interesting, fun and engaging problems to solve, rather than just flat images and puzzles on a computer screen. This robot has more abilities than other coding robots such as the ability to draw by lifting and roping pens, it erases whiteboard surfaces by lifting and dropping an eraser pad, it can scan, and climb up, down, and around magnetic surfaces (such as whiteboards). As a result of the ease of use, this robot has been popular in schools. To learn more, please visit www.codewithroot.com



It's a thrilling world full of possibility and potential, but our dependence on these ever-changing technologies comes at a price. The overlay of the Internet on all aspects of our lives is fraught with vulnerabilities that criminals are eager to exploit. Though new protective measures are developed at the same breakneck speed as the software they guard, so are new ways to penetrate and circumvent these defenses. It's estimated that 978,000 new malware threats are released with each passing day. It's clear that "up-to-date" can no longer be an accurate descriptor; it always describes a system one step behind the newest development.

Today, cybercriminals are casting a wider net and catching more

Report, 61% of breaches occurred at small businesses, with half of the 28 million small businesses across the United States succumbing to a digital strike. Even scarier is the fact that UPS Capital reports that 60% of these businesses shut down within six months of a breach.

It's a bleak reality to come to terms with if you're a business owner. The truth is that it's almost a statistical certainty that hackers will come for your data, and when they do, they'll likely be using techniques nearly unrecognizable from today's malicious flavor of the month. How can you possibly prepare for something that is constantly changing?

The answer is sustained attention, vigilance and resources directed toward protecting all that you've worked so hard to build. While it may be impossible to foresee exactly how hackers will try to



4 Steps to Finding Your Company's Diamonds In The Rough

Executives are always looking to inject "fresh blood" into their teams. They're on the hunt for shiny new talent to be that secret ingredient their organizations are missing. But in my numerous coaching sessions with entrepreneurs and leaders across the country, I found that an external search should usually not be the first step. Instead, I suggest that businesses look internally for hidden, untapped assets within the company. Here are four steps to start uncovering your diamonds in the rough.

1. DON'T HIRE TO FIT A TITLE.

It may be the way business has been done for half a century, but that doesn't mean it's right. You need to look at the individual strengths of each candidate and determine if he or she is right for your company and culture.

Make sure that you have a process in place to make hiring efficient. And as a part of that process, take time to identify

those creative and out-of-the-box individuals you already have on your team. Ask pointed questions of everyone you consider for a



given role, because this allows you to get a sense of how they think.

2. MINE FOR THE GEMS.

As you refine your hiring methods, you'll likely discover that the talent you're looking for might be right under your nose. Dig into your roster of existing team members. Create a company-wide survey for those interested in taking on creative or challenging initiatives, and give

them the opportunity to be considered. The true innovators know what they can bring to the table, even if they're currently not in a role that's a perfect fit. If you give them the opportunity to shine, they'll come forward.

3. REFINE AND POLISH.

Once you've identified your gems, spend some additional time with them. Find out what inspires and motivates them. You may decide to modify your team member's role or transfer some responsibilities to others in order to better utilize your talented individual's strengths and unleash their creative prowess. Just make sure to set clear expectations with each person, explain why you're making the change and empower them to do what they do best.

4. FORMALIZE YOUR PROCESS TO FIND MORE GEMS.

This isn't a one-and-done process. It's important to meet regularly with people to find these hidden assets.

Consider handing out surveys and holding brainstorming sessions regularly as part of your company culture. That way, new team members will come on board knowing there's an opportunity to shine in new ways, even if it's not what they were originally hired to do.

Focus on embracing and developing internal individuals with relevant skill sets before hiring. I guarantee there is a huge number of underutilized assets within your organization. Give them the space to shine brightly.

As the founder of Petra Coach, Andy Bailey can cut through organizational BS faster than a hot knife through butter, showing organizations the logjams thwarting their success and coaching them past the excuses we all use to avoid doing what needs to be done. Andy learned how to build great organizations by building a great business, which he started in college. It then grew into an Inc. 500 multimillion-dollar national company that he successfully sold and exited.

4 Ways Technology Can Make Your Business Meetings More Productive

Every entrepreneur knows how difficult it can be to run an efficient meeting. But most of them aren't leveraging new technologies designed to do just that. Rather than treating meeting participants like audience members, use a tool like GoWall to empower your team to contribute without disrupting your meeting's flow, keeping them engaged and on topic. Meanwhile, solutions like ParticiPoll equip any meeting with a poll that can provide useful feedback to implement at your next gathering. This is especially valuable for organizations that frequently host remote events, providing a quick breakdown of your meetings' strengths and weaknesses.

Speaking of remote contacts, Google Hangouts has made it easier than ever to set up video conferences where participants can move from chat to file sharing to

video chat with no fuss whatsoever. And if you're unable to stand in front of your team with a whiteboard, consider implementing a whiteboard app like Cisco Spark Board, which uses shared screens to create a cohesive brainstorming session between you and your team. SmallBusinessTrends.com, 2/21/18

GoWall®

participoll.



Cisco Spark

Two-Factor What?

Two-factor authentication (2FA for short) is a system in which you must verify your identity in two separate ways to access an account. Sound confusing? It's not. Here's an example:

After enabling 2FA on a Gmail account, you have to enter your password each time you log in. Then you are asked to enter a six-digit code that you pull from your phone, a jump-drive-sized key fob or a program on your computer.

Only then do you have access to your account. That way, if someone steals your password, they still can't get in.

If you aren't currently using two-factor authentication with your most sensitive data and systems, look into whether it might be an option. The extra 15 seconds it takes to pull up that second code is laughably short compared to the time you'd spend dealing with a hacked account.

NeoTip: What is the difference between Phishing and Spear-Phishing?

Phishing is a broad term that covers any attempts to trick victims into sharing sensitive information. The goal is to send a spoofed email that looks as if it is from an authentic organization to a large number of people, hoping that someone will click on that link and provide their personal information or download malware. These attacks are not personalized.

Spear-Phishing is a targeted attempt to steal sensitive information such as account credentials or financial information from an individual. Messages, and other forms of contact, are modified to specifically include personal details on the victim; such as their friends, hometown, employer, and even items they recently purchased online. This is the most successful form of acquiring confidential information and accounts for 91% of attacks.

Free Report: FREE Report: The 7 Most Critical IT Security Protections Every Business Must Have In Place Now To Protect Themselves from Cybercrime, Data Breaches and Hacker Attacks



978,000 NEW malware threats are being released every day, and businesses (and their bank accounts) are the No. 1 target. To make matters worse, a data breach exposing client or patient information can quickly escalate into serious reputational damage, fines, civil lawsuits and costly litigation. If you want to have any hope of avoiding a cyber-attack, you MUST read this report and act on the information we're providing.

Download your FREE copy today at <https://www.neolore.com/free-stuff/reports/> or call our office at (613) 594-9199.

Who Else Wants To Win A \$25 Tim's Card?

The Prize Winner of last month's Trivia Challenge Quiz is Mark P! Mark correctly answered last month's quiz question:

Question: What are the three standards you need to demand from your team of IT experts before disaster strikes?

Answer:
1. Constant monitoring of your network
2. Rapid response times
3. A real investment in your success

Now, here's this month's trivia question. The winner will receive a \$25 Tim's Card!

Question: What is the best way to verify your identity while accessing accounts?

Call (613) 594-9199 right now with your answer! Or email contact@neolore.com.

Knock, Knock. Who's there? Yeah. Yeah Who? No thanks, I Google.