INDEVTECH

TECHMinutes

Your Small Business Technology Information Source!

This Issue:

Update Your Chrome Browser, But Be Wary of Fake Alerts

Google Chrome has been pushing a lot of important updates over the last few weeks. Fortunately, updating Chrome is pretty seamless, and it's important that users do so. Users also need to be wary of fake Chrome errors that insist on installing malware. You don't want to fall for this scam!

Keep Google Chrome Updated

Google has been issuing some...

Read the Rest Online!
https://bit.ly/3XoxGtS

About Indevtech Incorporated

We are the IT department for many small businesses in Hawaii, across different verticals such as healthcare, legal, financial, and manufacturing concerns.

Visit us **online** at:
newsletter.indevtech.com

Hackers Will Tear Your Business Down, Brick by Brick

If you have the guts to start a business, having it succeed is a massive reward, especially considering how much work you've had to do to make that a reality. Unfortunately, for businesses worldwide, all that hard work and dedication could be destroyed after a cyberattack. This month, we'll discuss how exactly cyberattacks ruin an otherwise successful business.

They Can Steal Critical Data and Money

Hackers can steal important information, like customer details or money, and sometimes they demand businesses pay them to get things back, which is called ransomware. Businesses might also have to pay legal fees or fines because their customers' information got stolen. This can make it really hard for them to recover if they don't have strong security in place.

They Can Ruin Your Brand

People expect businesses to protect their information, and when that trust is

(Continued on page 3)

Cybersecurity Scam Artists Aren't Always Super Technical

Cybersecurity covers a broad range of risks and threats. You've got the basics like your computer viruses and malware, to the business-crippling ransomware and data breaches. You have threats that cause stress and downtime, and others that steal information and money, and others still that don't even have clear understandable objectives. The point is, cybersecurity isn't simple, but sometimes the threat actors and cybercriminals who target you will use low-tech methods to get what they want.

First off, let's start with the **Two Golden Rules of Being a Potential Cybersecurity Victim** (I know it's not catchy, I just made it up, but maybe it will catch on).

Rule #1: Nobody is Too Big or Too Small or Has Too Little to be Immune from a Cyberattack.
Plain and simple, there's no business too small, there's no person too humble, and there's nobody who doesn't have something worth the small amount of effort it takes to scam them.

Rule #2: Cybercrime is a Streamlined Business, and It's Thriving.
While there are plenty of lone scammers and hackers out there, the vast majority

(Continued on page 2)

4 Powerful Professional Services Technology Solutions

Professional services include a lot of the "experts" people depend on. Today's professional services firms rely heavily on technology to enhance efficiency, client service, and overall operations. This month, we thought we'd go through four technologies professional services firms depend on. Let's get into it.

Project Management Software

Project management software is one of the most commonly used technologies in professional services. These tools allow teams to collaborate on projects, track progress, and effectively meet deadlines. These platforms provide a centralized space for assigning tasks and managing resources, both of which are important for firms that rely on a steady stream of client engagement. Using project management software, professional services firms can ensure that projects are completed on time and within budget, leading to higher client satisfaction.

Customer Relationship Management

Another essential technology for professional services is customer relationship management (CRM) software. CRMs help firms manage their interactions with current and potential clients. The CRM allows businesses to store detailed information about client history, preferences, and communications, enabling firms to tailor their services to meet specific client needs. CRMs also have a lot of automation options. They automate various aspects of client communication, such as follow-ups and marketing campaigns, which are important for customer engagement. Relationships are the name of the game in professional services and CRM technology is indispensable for maintaining strong, long-term client connections.

Document Management Systems

The document management system (DMS) is a critical tool that professional services companies use to ensure that they have access to important documents on demand. DMS provides secure storage, easy access, and efficient sharing of documents within the firm and with clients. These systems often include version control, e-signature capabilities, and features that allow businesses to maintain compliance. For law, consulting, and accounting firms...

Read the Rest Online!
https://bit.ly/3MNc59H

Cybersecurity Scam Artists Aren't Always Super Technical

(Continued from page 1)

of cybercrime comes from very active groups of people who more or less work like a business. These organizations perfect the art of cybercrime, and they get to continuously repeat and hone in their tactics and treat it like a numbers game, and they are always looking to increase their ROI.

Low-Tech Social Engineering

It's expensive to write a virus or malware. It takes a lot of effort and a lot of intelligence and education. It's not expensive to exploit malicious software that is readily available and just requires a little scam artistry to deploy.

These low-cost, low-effort types of attacks are effective, and in a world where more and more businesses are deploying strong cybersecurity defenses, non-technical scams like social engineering simply allow the bad guys to be let right in beyond the security gate.

Social engineering is manipulation. It exploits human psychology to gain access to enough information or access to cause harm. Scammers target human weaknesses, such as trust, curiosity, or fear.

A good example of this is the **grandparents scam**. This, as its name suggests, often targets parents and grandparents. The scam is complex, but relatively easy for a clever scam artist with few morals to conduct. They learn a little information about their target, and then call them, claiming that a loved one is in jail or the hospital with a broken nose. They play the part of the loved one's attorney, and weave a story about how the one was in an accident involving a pregnant woman. This story can change a little, but the long and short of it is they need a large sum of money for bail, and they will send a driver to come pick it up...

Read the Rest Online!
https://bit.ly/3N5oB4F

Hackers Will Tear Your Business Down, Brick by Brick

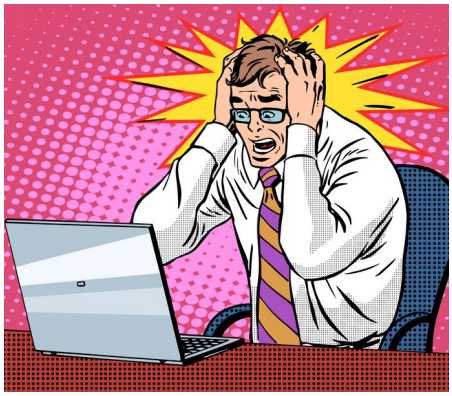
(Continued from page 1)

broken, customers don't want to deal with that business anymore. Even future customers might avoid the company because they think their information won't be safe. It's hard to earn back trust once it's lost, and in some cases, this can make the business fail.

They Can Create Chaos

When a hacker breaks into a business' systems, it can shut everything down for hours, days, or even longer. This means the business can't sell products or help customers, which makes it lose even more money.

Fixing the problem takes a lot of effort from IT experts and other staff, which means less time to focus on their regular work.



They Put Pressure on Everyone

Employees might have to work harder to fix things, worry about losing their jobs, or even be afraid that their own personal data has been stolen. This can make people feel unhappy and less productive at work, which can cause some employees to leave the company altogether. Trust us; you don't want to deal with cyberattacks if you can help it. To do everything you can to avoid them, you will need a comprehensive strategy that covers all elements of your business' technology.

Share this Article!
https://bit.ly/3DxVgOu

Innovations Made in Security Work to Protect Businesses

Cybersecurity is a major part of business computing today, mainly because there are so many threats. Cybersecurity professionals and network administrators must innovate to confront these threats. This month, we thought we would review three of these innovations to give you an idea of what is being done to help businesses handle the rough-and-tumble cybersecurity landscape.

Advancements in AI-Powered Threat Detection

One of the most significant innovations in cybersecurity is the integration of artificial intelligence (AI) and machine learning into threat detection systems. These technologies enable security systems to analyze a lot of data in real-time, identifying patterns and finding anomalies that could indicate a cyberthreat. AI systems learn and adjust to new threats. This allows them to offer a more proactive defense. In contrast, traditional methods rely on fixed rules. This AI capability is especially crucial as cyberattacks become more sophisticated, with hackers using AI to craft more convincing phishing attacks or bypass traditional security measures.

Zero Trust Architecture

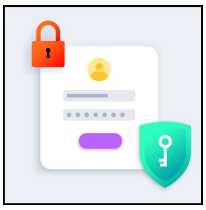
Zero Trust Architecture (ZTA) is reshaping how organizations approach security. Instead of assuming that everything inside a network is safe, ZTA operates on the principle that nothing can be trusted and everything has to be verified. This model requires continuous verification of every user and device attempting to access data and other computing resources, regardless of their location within the network. By implementing strong access controls and ensuring that only authorized users can access specific resources, ZTA significantly reduces the risk of internal threats and the spread of malware like ransomware inside a compromised network.

The Rise of Cybersecurity Automation

Automation is increasingly becoming a cornerstone of business, which also goes for cybersecurity strategies. As cyberthreats' number and overall complexity continue to grow, manual response efforts are often insufficient. Cybersecurity automation leverages AI, machine learning, and other advanced technologies to automate routine tasks such as threat detection, incident response, and vulnerability management. This speeds up response times and reduces the likelihood of human error, which can be the most prevalent factor in a security breach. By automating repetitive tasks, cybersecurity professionals can focus on more complex issues, improving the overall cybersecurity profile of a business.

Share this Article!
https://bit.ly/4e1FgSf

Tip: Choosing the Right Password



Whether you like it or not, the password is the most important part of your cybersecurity policy. That's saying something with all the tools and strategies out there designed to keep unauthorized users from accessing your accounts. Maybe they aren't the most comprehensive security solution, but they are by far the most frequently used and there are some things every user should know to help them build successful passwords. This month, we'll go into four things every computer user should know about building strong and reliable passwords

The Longer, the Better

When you are talking about passwords, the longer, the better. The more characters that need to be guessed to crack into an account, the less likely hackers will be able to. A good rule of thumb is to make a password over 12 characters long. One way to do this is to consider using a passphrase. Instead of 12 random characters, you would never be able to remember, try creating passwords that combine random words. This ensures that it is not easy to guess but much, much easier for you to remember.

Use a Variety of Characters

Many password platforms will require you to use various characters, but even if they don't, you should. This means creating passwords with a combination of upper and lowercase letters, numbers, and special characters. Another good tip is to not just add special characters at the end if they are required. Use them as a substitute for another character so they are less likely to be guessed. If you mix them in throughout a password, the sophisticated password-cracking tools will have many more variables to guess, reducing the chances they'll guess your password.

Keep It Impersonal

Surprising as it may be, hackers can glean significant information from social media accounts. If you use personal information for your password, whether because you can't help yourself or simply wouldn't be able to remember your passwords without a tidbit of personal info in there, you need to stop. You won't want to use your name, easily accessed information about you or simple passwords to try and protect your accounts. So even if you think the password "12345" is funny, don't use it. Don't use single words, as many hackers can conduct what are called dictionary attacks. You will need to use complex passwords. Using a password manager can be a great solution as they can provide you with unguessable and utterly random passwords and keep them encrypted for you...

Read the Rest Online!
https://bit.ly/47oeX6r

Indevtech has been serving Hawaii since 2001, providing end-to-end managed IT services to small- and medium-businesses. Our philosophy is very simple: we strive to be the best at what we do, so that you can succeed at what you do. We have a proven framework that, when deployed with a solid commitment from our clients, provides an unshakable foundation on which our clients can build their businesses.

Tech Trivia
40% of adult users check their mobile device within five minutes of waking up.

Indevtech Incorporated

Pacific Guardian Center, Mauka Tower
737 Bishop Street, Suite 2070
Honolulu, Hawaii 96813-3205
Phone: (808) 529-4605

newsletter@indevtech.com

blog.indevtech.com

Visit us **online** at:
newsletter.indevtech.com