1991 – 2021
30 YEARS OF EXCELLENCE
Computer Technologies, Inc.

TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's Inside

September 2023

Kim Nielsen, CISSP, CCSA
President & Chief Technology Strategist at Computer Technologies Inc.
(248) 362-3800

"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!"

How Well Do You Know Your Incident Response Plan?

The faster you can identify suspicious activity on your network, the faster you can respond to the threat actor. But then…do you know *what to do* to report the breach and kick start your company's incident response plan into motion?

Cybersecurity incidents are becoming more and more common, and it is **essential** to have an incident response plan in place. A plan can help organizations prepare for, spot, respond to and recover from a cybersecurity incident. This documentation will include useful information like the roles and responsibilities of personnel involved in the response process, the steps they should take when responding to a security incident, and what reporting and disclosure protocols need to be followed.

In short, why is it so important to have an incident response plan in place *before* a threat actor attacks? **It's a matter of *when*, not *if*, you are the target of a cyberattack these days.** Having a formal plan and training in place will help organizations prepare to notice, react to and deal with a security breach or other cybersecurity-related issue.

What to Expect From Your Incident Response Plan

Every organization will have their own personalized incident response plan because every business is different! Yours might include notifying Simon Sez down in I.T. to come up from Floor 2 and

Continued on pg.2

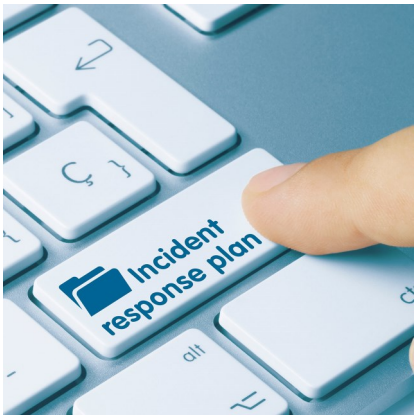
Continued from pg.1

have a look, or a number to reach a specialist during off-hours at (555) 555-1800.

Although the specifics may change, the main goal is to prevent you from making a mistake when you encounter suspicious behavior on your systems or network. If you don't react immediately, the threat actor has more time to dig deeper into your company's private files. If you try to stop them yourself, you could open new doors for them by accident. Knowing where to report odd activity lets the experts (that's us!) step in right away and chase the unauthorized user out, limiting/eliminating any exposed or stolen data.

Depending on your role in your organization, you might also be expected to carry out certain responsibilities after a security incident. Maybe you're on the team who drafts up communication to send out to any affected parties whose data might have been exposed in the breach, for example. Perhaps you're a manager who must come up with engaging ways to re-train your team in the areas in their security awareness training with which they're having trouble.

Each and every one of the people in your organization are gatekeepers of the private data that you handle. Depending on what you do and who you take on as a client, your incident response procedures



and cyber-defense protocols could be pretty complex! That's why you should become familiar with yours; you need to know what roles and responsibilities you play.

Conclusion

An incident response plan is an essential part of your security strategy. It outlines exactly what and when you need to take certain steps to shut down a security threat to your systems. It teaches you how to detect, respond, and recover from an incident. It also provides guidance on how to prevent more cyber-attacks like that from happening again.

Minimize the damage and disruption caused by security incidents by learning and relying on your incident response plan until those best practices come as natural to you as a reflex. How well do you know yours?

Free Executive Guide: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

This guide will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at
https://www.cti-mi.com/protectdata923/
or call our office at (248) 362-3800

Security Corner

Geotagging: What Is It And What Are The Security Risks?

Whether you're checking in to someplace on Facebook, or browsing posts made from a specific location on TikTok or Instagram, you've probably come across geotags before. It may shock you to hear this, then: Geotagging can pose cybersecurity and privacy risk.

How Does Geotagging Risk Your Data Privacy?

Geotagging involves embedding geographical location information (such as latitude and longitude coordinates) into digital media files. These can be photos, videos and posts!

This information reveals where the media was created, which could lead to some unintended consequences. If they can find out more about that "metadata," malicious actors would be able to track your movements or identify your habits, making it easier to spear-phish you.

At work, there's the additional risk of exposing the location of sensitive business activities to competitors, adversaries, and cyber-criminals.

Mitigating The Risks Posed by Geotags

1. **Review Settings:** Check the settings on your devices and apps to determine if geotagging is enabled.

2. **Disable Individual Geotags:** For sensitive media or posts, turn off geotagging before sharing.

For more information about staying safe while online and other cyber threats, call us at 248-362-3800 or visit: https://tinyurl.com/yswcss2v

Learn How To Spot Fake LinkedIn Sales Bots

LinkedIn has become an invaluable platform for professionals. People use it to connect, network, and explore business opportunities. But with its growing popularity have come some red flags. There has been an increase in the presence of fake LinkedIn sales bots.

These bots impersonate real users and attempt to scam unsuspecting individuals. This is one of the many scams on LinkedIn. According to the FBI, fraud on LinkedIn poses a "significant threat" to platform users.

In this article, we will delve into the world of fake LinkedIn sales bots. We'll explore their tactics and provide you with valuable tips. You'll learn how to spot and protect yourself from these scams. By staying informed and vigilant, you can foster a safer LinkedIn experience.

Identifying Fake LinkedIn Sales Connections

Social media scams often play on emotions. Who doesn't want to be thought of as special or interesting? Scammers will reach out to connect. That connection request alone can make someone feel wanted. People often accept before researching the person's profile.

Put a business proposition on top of that, and it's easy to fool people. People that are looking for a job or business opportunity may have their guard down. There is also an inherent trust people give other business professionals. Many often trust LinkedIn connections more than Facebook friend requests.

How can you tell the real requests from the fake ones? Here are some tips on spotting the scammers and bots.

Incomplete Profiles and Generic Photos

Fake LinkedIn sales bots often have incomplete profiles. They'll have very limited or generic information. They may lack a comprehensive work history or educational background. Additionally, these bots tend to use generic profile pictures. Such as stock photos or images of models.

If a profile looks too perfect or lacks specific details, it could be a red flag. Genuine LinkedIn users usually provide comprehensive information.

Impersonal and Generic Messages

One of the key characteristics of fake sales bots is their messaging approach. It's often impersonal and generic. These bots often send mass messages that lack personalization. There may be no specific references to your profile or industry. They often use generic templates or scripts to engage with potential targets.

Inconsistent or Poor Grammar and Spelling

When communicating on LinkedIn, pay attention to the grammar and spelling of messages. You may dismiss an error from an international sounding connection, but it could be a bot.

Fake LinkedIn sales bots often display inconsistent or poor grammar and spelling mistakes. These errors can serve as a clear sign that the sender is not genuine. Legitimate LinkedIn users typically take pride in their communication skills.

Unusual Connection Requests and Unfamiliar Profiles

Fake LinkedIn sales bots often send connection requests to individuals indiscriminately. They may target users with little regard for relevance or shared professional interests. Be cautious when accepting connection requests from unfamiliar profiles. Especially if the connection seems unrelated to your industry or expertise.

5 Small Business Tech Trends To Fuel Your Growth

In today's ever-evolving digital landscape, small businesses have more opportunities than ever. Many of these trends call for leveraging technology to their advantage.

Embracing the right tech trends can help businesses compete. It enables them to streamline operations, enhance customer experiences, and fuel their growth.

Here are 5 small business tech trends that have the potential to drive success as well as propel your business forward even in an increasingly competitive market.

1. Cloud Computing: Expanding Possibilities
2. Artificial Intelligence: Automating Efficiency
3. E-commerce and Mobile Commerce: Expanding Reach
4. Data Security: Safeguarding Trust
5. Automation and Workflow Integration: Streamlining Operations

Technologies To Help You Run Your Small Business Better

Running a small business can be challenging. But advancements in technology have opened a world of opportunities. Small business owners can use digital tools to streamline operations. As well as improve efficiency, and boost productivity.

But trying to navigate the options yourself can be confusing. Just buying apps because someone told you one was cool, might not be the best strategy. You need to focus on needs and target optimization.

Let's explore some game changing technologies for small businesses.

Cloud Computing for Scalability and Flexibility

Cloud computing has transformed the way businesses store, access, and manage their data. Apps like Microsoft 365 and Google Workspace allow small businesses to afford more including enterprise-class functions formerly enjoyed only by large companies.

Customer Relationship Management (CRM) Software

Spreadsheets can only take you so far. CRM software can help you improve your sales process. As well as personalize marketing campaigns and provide top-notch customer engagement and support.

Collaboration Tools for Seamless Teamwork

Efficient collaboration is crucial for small businesses. This is especially true when employees are in different offices or working remotely.

"I just feel fortunate to live in a world with so much disinformation at my fingertips."