September 2023

TechTidbit.com

brought to you by Tech Experts

Eight In 10 Businesses Were Targeted With Phishing In The Last Year. Was Yours?

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

Despite all the buzz about high-tech threats like ransomware and malware, good old phishing has held on to its title as the number one trick in a cyber criminal's toolkit.

Phishing is when someone tries to trick you into giving them your personal information, like your password or credit card number. They do this by sending you emails or text messages that look like they're from a real company.

According to the latest annual cyber breaches survey, 79% of businesses were targeted with a phishing attempt in the past year. And if your employees aren't trained in cyber security awareness, 1 in 3 of them are likely to fall for a phishing attack. Scary!

You might be thinking, "Sure, it's bad, but it can't be that bad, right?" Well, let's break down the consequences of a successful phishing attack.

The impact on your business

Let's set the scene: one of your employees clicks on a bad link in an email. Next thing you know, sensitive company data is in the hands of cyber criminals. You're looking at potential financial loss, damage to your reputation, and one giant headache.

The impact on your employees

There's more... it's not just your business that takes a hit. The employee who clicked that link? They're probably feeling as guilty as a dog caught stealing a steak from the dinner table. This can lead to stress, decreased productivity, and even increased employee turnover.

Turn lemons into lemonade

As a business owner, how you handle these incidents can make a big difference. Turn these incidents into learning opportunities.

This way, you're fostering a culture of understanding and open communication. Remember, everyone makes mistakes – it's how we learn from them that counts.

How can we show phishing who's boss? One word: training. Regular cyber security awareness training can significantly reduce the risk of phishing attacks being successful.

And it can help protect you from a whole host of other cyber security risks too. It feels like a no-brainer.

If it's something we can help you with, get in touch.

How can we show phishing who's boss? One word: training. Regular cyber security awareness training can significantly reduce the risk of phishing attacks being successful.

We Love Referrals!

The greatest gift anyone can give us is a referral to your friends and business colleagues. Referrals help us keep costs down so we can pass the savings to our clients.

If your friend ends up becoming a client - we'll give them their free first month of service (for being a friend of yours) AND we'll give you a $250 Amazon Gift Card.

Simply introduce us via email to sales@mytechexperts.com and we'll take it from there. We'll look after your friend's business with a high level of care and attention (just like we do with all our clients).

Planning Digital Transformation? Don't Forget Your Team

"Businesses often make the mistake of getting caught up in the whirlwind of "cool new tech" and forget about the human element. How many times have you heard of a company rolling out a major new software system, only for their employees to struggle with the change?

Have you heard of the term "digital transformation?" It's where you introduce new technology across every part of your business, to help you sell more, deliver better customer service and be more efficient/profitable.

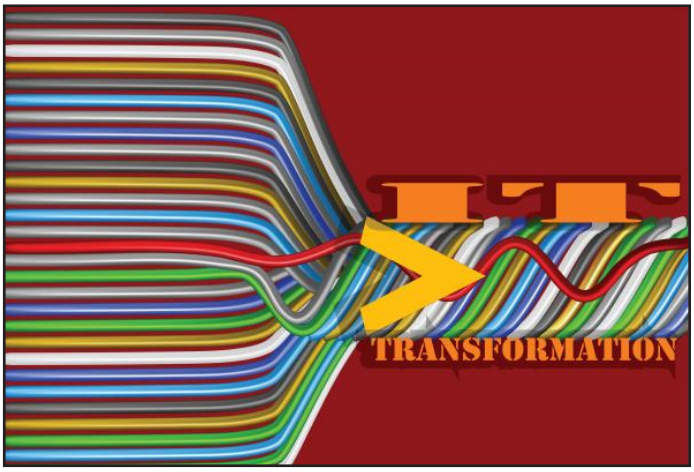
That word 'transformation' sounds impressive, doesn't it? It's like your business is a caterpillar, ready to emerge from its cocoon as a dazzling, tech-savvy butterfly.

But hold on a minute, let's not forget about the most important part of this metamorphosis – your people.

Yes, you read that right. It's not technology that should be at the heart of any digital transformation… it's people.

Businesses often make the mistake of getting caught up in the whirlwind of "cool new tech" and forget about the human element. How many times have you heard of a company rolling out a major new software system, only for their employees to struggle with the change?

The truth is, the success of any digital transformation hinges on your team's buy-in. You can have the most cutting-edge technology



in the world, but if your people hate using it, it's going to fail.

So how do we put people first in digital transformation? It starts with communication. Your team needs to understand why change is happening and how it will benefit them. This isn't just a one-time announcement, but an ongoing two-way conversation.

Next, you need champions. These are individuals at all levels of the business who are enthusiastic about the change and can help others get on board. Enthusiasm is contagious!

And finally, you need to break down silos. The digital world thrives on collaboration, and your business should too. If departments are working in isolation, you're not harnessing the full potential of your team or your technology.

Let's not forget about the role of AI in all this. Generative AI systems, such as ChatGPT, have been making waves in the media, highlighting the importance of the human element in the digital transformation debate. After all, technology should serve people, not the other way around.

The pace of technological advancement is dizzying, no doubt about that. But amidst all the change, one thing remains constant - the importance of putting people, processes and culture at the center of your digital transformation.

If we can help you with any kind of technology project, just give us a call.

- The Surface Web (the internet visible to search engines) only accounts for 10% of the internet. The rest lives in the Deep Web – where pages aren't indexed, or are encrypted, password protected or behind a paywall. This is normal, legal and very different to the Dark Web… where criminals do business.
- One of iTunes' terms and conditions states that you are not to use their devices to create "…nuclear, missile, chemical or biological weapons."
- Only 4.5 billion people around the world have a working toilet. More than 6 billion people have a cellphone

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.

Lets 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 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 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. They may be no specific references to your profile or industry. They often use generic templates or scripts to engage with potential targets.

Excessive promotional content

Fake LinkedIn sales bots are notorious for bombarding users. You'll often get DMs with excessive promotional content and making unrealistic claims. These bots often promote products or services aggressively. Usually without offering much information or value.

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.

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. They may be no specific references to your profile or industry. They often use generic templates or scripts to engage with potential targets.

Contact Information

Tech Experts Support Team
(734) 240-0200
support@MyTechExperts.com

Main Office
(734) 457-5000
info@MyTechExperts.com

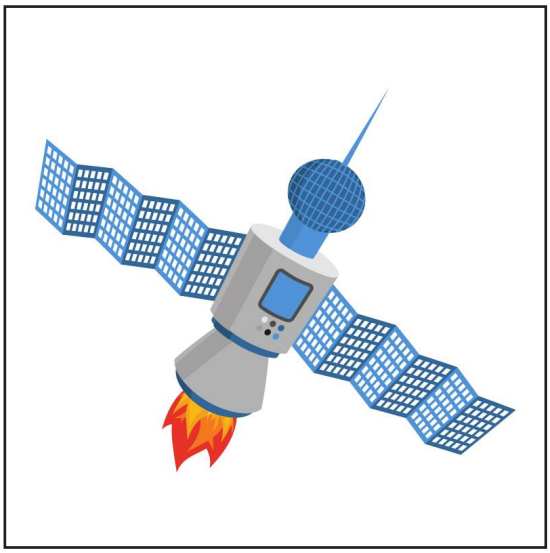
Sales Inquiries
(888) 457-5001
sales@MyTechExperts.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Satellites Are Safe In Space...But Not Cyber-Space!

Yes, satellites are indeed vulnerable to cyberattacks.



As sophisticated technologies, satellites are not immune to the risks posed by cyber threats. While they operate in space, they are still managed and controlled through ground stations on Earth, making them susceptible to various types of cybervulnerabilities.

Think about it...

Like any computer system, satellites can be infected with malware or viruses, affecting their functionality and data integrity. They can also be overwhelmed with excessive traffic, causing temporary or permanent disruptions, like any other DDOS attack.

Attackers can also send false signals or information to satellites, leading to incorrect data processing or navigation errors.

Imagine if a company's computer systems crash, or there's a big cyber-attack, or a natural disaster like aflood or fire strikes their office.

With a well-thought-out plan in place, you (and your coworkers) can quickly get back on your feet, minimize the damage and continue serving customers.

The disaster recovery plan includes things like data backups, so important information doesn't get lost forever. It also outlines who's in charge of what during the crisis, so everyone knows what to do.

If hackers gain access to the ground stations or satellite control systems, they may be able tomanipulate or disrupt satellite operations. Intercepting that communication signal could expose sensitive information!

While less common, physical attacks on satellites or their infrastructure in space can also occur, leading to a loss of functionality.

If someone successfully hacked a satellite, it could impact critical services such as communication, navigation, weather forecasting and national security.

For this reason, space agencies, satellite operators, government organizations and other stakeholders are continuously working to enhance satellite cybersecurity measures and stay ahead of potential threats!

Do you have a disaster recovery plan?

Having a disaster recovery plan might seem like extra work, but it's a smart and responsible thing to do.

It helps keep the company running smoothly even when bad things happen, and it shows that you're ready for anything! So, just like how we prepare for unexpected situations in our daily lives, companies need to have a disaster recovery plan to be ready for anything that comes their way.

It's like having an emergency kit ready for unexpected disasters. Just like how we keep a flashlight, some snacks, and first aid supplies handy for emergencies, a disaster recovery plan is a strategy for what to do when major problems occur that disrupt operations.

A disaster recovery plan also ensures that you have a safe place to work from in case their usual office is unavailable (like, say, if a global pandemic were to strike?).

When something major happens, it's normal for people to panic. A disaster recovery plan that has been routinely tested, updated and studied will save you from the panic, and headache, of what to do when the worst goes down.

Instead, you'll be back to business as usual in no time.