# CTTS TECH TALK

## YOUR TECHNOLOGY NEWSLETTER

**OCTOBER 2024**


JOSH


SARA


KURT


MICHELLE


KEN


CHRISTINE


EVAN


KURT


CHAIM


WILSON


You may think you've taken every possible precaution to shield your business from cyber threats. You've invested in the most advanced security solutions, fortified your defenses against hackers, and locked down your systems. But have you considered the threat that might already be inside your organization?

## WHAT'S INSIDE THIS ISSUE?

TECH NOTES

# FROM CEO, JOSH WILMOTH

## Cybersecurity Awareness: Myths Debunked

**Hello and happy Cybersecurity Awareness Month!**

October is a perfect time to reflect on the health of your business's digital defenses. With 2025 around the corner, the evolving nature of cyber threats isn't slowing down. As businesses grow—adding employees, devices, and expanding operations—the risk of a cyberattack grows with them. Unfortunately, cybercriminals don't take holidays, and they're constantly refining their tactics to target vulnerabilities. But don't worry, we're here to help you sort through the noise and arm your business with the right knowledge.

Let's kick off by debunking some common myths about cybersecurity. The truth is, many businesses fall victim to misconceptions that leave them exposed. By understanding and dispelling these myths, you can make informed decisions to better protect your company.

**Myth 1: Small Businesses Aren't Targets**

Many business owners believe that cybercriminals only go after big corporations. This couldn't be further from the truth. Small and medium-sized businesses (SMBs) are prime targets because hackers know that SMBs often lack the sophisticated security measures of larger companies. In fact, a significant percentage of cyberattacks are aimed at businesses with fewer than 500 employees.

**The Reality:** No business is too small to be a target. In fact, cybercriminals see SMBs as easy prey because they often assume they're not at risk. Prioritize your security and don't wait until it's too late.

**Myth 2: Cybersecurity Is All About Technology**

Yes, firewalls, antivirus software, and encryption are essential tools. But a successful cybersecurity strategy is much more than that—it's about people, processes, and education. You can have the best technology in place, but if your employees aren't trained on best practices, your business is still vulnerable. Human error remains one of the leading causes of data breaches.

**The Reality:** Cybersecurity isn't just about having the latest tech. Regular employee training, developing clear policies, and creating a culture of security awareness are just as crucial. Make cybersecurity a company-wide effort.

**Myth 3: I'm Covered by My Basic Security Measures**


If you think that having a basic antivirus or firewall is enough to keep hackers at bay, think again. Cyberattacks have become far more sophisticated, and relying on outdated or minimal defenses leaves your business at risk. Hackers are constantly evolving their methods, using tactics like social engineering, ransomware, and zero-day exploits to bypass traditional security systems.

**The Reality:** Basic security measures are no longer enough. You need a multi-layered approach to cybersecurity that includes advanced threat detection, response strategies, and regular updates to your systems.

**Myth 4: Cybersecurity Is Expensive**

Many business owners hesitate to invest in comprehensive cybersecurity measures, assuming that the costs are too high. However, the cost of a security breach far outweighs the investment in prevention. A single breach can lead to data loss, legal fees, reputational damage, and downtime that can cripple your business.

**The Reality:** While investing in cybersecurity might seem costly upfront, it's far more affordable than recovering from an attack. Cybersecurity is an investment in the future of your business, and there are scalable solutions that fit businesses of all sizes.

**Myth 5: If I've Never Been Hacked, I'm Safe**

Cyberattacks can happen at any time, and just because you haven't been targeted yet doesn't mean you're in the clear. Cybercriminals are always looking for new victims, and their tactics are becoming more advanced. Relying on luck to protect your business is not a strategy.

**The Reality:** Cybersecurity is about being proactive, not reactive. Don't wait for a breach to happen before taking action. Regularly assess your security posture and make sure you're staying ahead of potential threats.

**Taking Action: How to Strengthen Your Cybersecurity**

**- Invest in a Strong Cybersecurity Framework:** Layered defenses, such as firewalls, intrusion detection, and multi-factor authentication, help minimize the risk of a breach.

**- Regular Employee Training:** Ensure your team knows how to identify potential threats like phishing and ransomware attacks.

**- Partner with Experts:** Work with a trusted IT partner like CTTS to continuously monitor and assess your cybersecurity defenses, ensuring your business stays protected.

This Cybersecurity Awareness Month, take time to evaluate where your business stands. At CTTS, we're here to help you navigate the complex world of cybersecurity and ensure that your company is safeguarded from threats, both now and in the future.

Stay safe, stay proactive, and reach out to us if you have any questions or need assistance with enhancing your cybersecurity strategy.

**Wishing you a secure and successful end to the year!**

# ADVANCED TECH

## Is Your Biggest Cybersecurity Threat Already Inside? How to Defend Against the Danger You Didn't See Coming


You've invested in top-tier security to protect your business from outside threats—firewalls, encryption, and monitoring tools. But what if the biggest danger isn't an external hacker? What if the threat is coming from someone inside your organization?

It's a difficult truth to face, but many cybersecurity breaches happen from within. Whether intentional or accidental, your employees, vendors, partners, or even yourself could unknowingly be creating vulnerabilities. In this article, we'll dive into the most common insider threats and provide actionable steps to safeguard your business from within.

**The Common Insider Threats You Should Be Watching**

Insider threats come in many forms, and they can happen at any time. Understanding these risks is the first step to protecting your business.

**1. Data Theft**
This is when an employee or trusted insider steals sensitive information for personal gain or to harm your business. It can involve physically stealing company devices or digitally copying data.

**Example:** A healthcare employee downloads and sells patient records on the dark web, violating confidentiality and risking the company's reputation.

**2. Sabotage**
A disgruntled employee or someone with an agenda deliberately damages your business by deleting files, introducing malware, or even locking you out of critical systems.

**Example:** An ex-employee tampers with internal systems, causing operational downtime and significant financial loss.

**3. Unauthorized Access**
Employees may access confidential information intentionally or by accident. Either way, this opens the door for data leaks or malicious activity.

**Example:** A low-level employee gains unauthorized access to proprietary information and leaks it to a competitor.

**4. Negligence & Error**
Simple mistakes can be just as dangerous as malicious actions. Clicking a malicious link or misplacing a device with sensitive information can lead to significant data breaches.

**Example:** An employee accidentally downloads malware, compromising the company's entire network.

**5. Credential Sharing**
Sharing passwords or login details, even innocently, creates unnecessary risks. It's like leaving the door to your business wide open.

**Example:** An employee logs into their work account on a friend's laptop and forgets to sign out, allowing a hacker to gain access.

**Red Flags: How to Spot Insider Threats Before They Happen**

Early detection is key to preventing an insider threat from escalating. Watch for these warning signs:

**- Unusual access patterns:** An employee suddenly accesses confidential data unrelated to their role.

**- Excessive data transfers:** Large volumes of data being moved or downloaded unexpectedly.

**- Repeated authorization requests:** Employees asking for access to sensitive information they don't need for their job.

**- Use of unapproved devices:** Personal devices used to access company data.

**- Disabling security tools:** Employees disabling antivirus or firewall protection.

**- Behavioral changes:** Sudden shifts in behavior, missed deadlines, or signs of stress can indicate something is wrong.

**Strengthen Your Defense: 5 Steps to Prevent Insider Threats**

It's essential to take proactive steps to prevent internal threats before they occur. Here's how to build a robust defense system:

**1. Strong Password Policies & Multi-Factor Authentication:** Require complex passwords and implement multi-factor authentication (MFA) to limit unauthorized access.

**2. Limit Access Based on Roles:** Ensure employees only have access to the data necessary for their work, and regularly review these permissions.

**3. Ongoing Education & Training:** Make insider threat awareness part of your regular cybersecurity training. The more employees know, the better they can protect your business.

**4. Regular Data Backups:** Keep secure, up-to-date backups of your data to ensure quick recovery in the event of a breach.

**5. Develop a Response Plan:** Have an incident response plan in place that details how to detect, respond to, and recover from insider threats.

**You Don't Have to Face Insider Threats Alone**

It can feel overwhelming trying to guard your business from both external and internal threats, especially when the risks are so varied. But you don't have to do it alone. Partnering with an experienced IT provider like CTTS ensures that you have the right tools and expertise to detect and prevent insider threats before they damage your business.

We can help you monitor potential risks and set up a comprehensive plan to respond to any incidents. Reach out today, and let's safeguard your business from the inside out.

# BIZTECH

## Phishing Attacks Are More Sophisticated Than Ever: Here's How to Protect Your Business

You start your day, coffee in hand, ready to dive into work. An email from what looks like a trusted partner appears in your inbox. Without thinking twice, you click the link. In that moment, you've just walked into a phishing trap—one set by cybercriminals.

**Unfortunately, this scenario is becoming a daily occurrence for businesses of all sizes.**

Phishing scams are no longer the amateurish, easily recognizable threats of the past. These attacks have evolved, becoming highly sophisticated and often indistinguishable from legitimate communications. As a business leader, it's crucial to stay informed, so you don't fall victim to the ever-growing threat of phishing.

**The Myth: Phishing Is Easy to Spot**

There's a common misconception that phishing emails are riddled with obvious red flags—bad grammar, suspicious links, or direct requests for sensitive information. While this may have been true years ago, today's phishing scams are much harder to detect.

Cybercriminals now use cutting-edge technology like AI to create emails and websites that mimic legitimate brands and trusted partners with startling accuracy. Logos, language, and even email signatures can all look identical to the real thing. This level of deception is why even tech-savvy individuals fall for these scams.

Simply put, phishing scams aren't as obvious as they used to be.

**Understanding Different Types of Phishing Attacks**

To protect your business, it's important to recognize the different types of phishing scams that are out there. Here's a breakdown of the most common ones:

**1. Email Phishing:** The classic scam where attackers pose as reputable companies—think banks or well-known brands—asking you to click a link or provide personal information.

**2. Spear Phishing:** This attack is personalized, targeting specific individuals or organizations. Cybercriminals research their targets to make the emails look as real as possible, often bypassing standard security measures.


**3. Whaling:** This is spear phishing with a twist—it targets high-profile individuals like CEOs and executives, making it even more dangerous. The goal is usually to extract confidential information or authorize large financial transactions.

**4. Smishing:** Similar to email phishing, but through SMS messages. These messages usually contain malicious links or prompt recipients to share personal details.

**5. Vishing:** A voice-based attack where scammers call posing as credible organizations (e.g., tech support or banks) to obtain sensitive information over the phone.

**6. Clone Phishing:** Cybercriminals take legitimate emails you've already received and replace the links or attachments with malicious ones. Because it looks familiar, you're more likely to trust it.

**7. QR Code Phishing:** Attackers use QR codes to direct you to harmful websites. These codes can appear in emails, flyers, or even on posters. Once scanned, they can lead you to malicious websites that steal your data.

**How to Defend Your Business Against Phishing Scams**

Phishing attacks are increasingly sophisticated, but there are practical steps you can take to minimize the risk:

**- Employee Training:** Regularly educate your team on how to spot phishing attempts and conduct simulations to test their knowledge.

**- Advanced Email Filtering:** Use tools that automatically detect and block suspicious emails before they reach your inbox.

**- Multi-Factor Authentication (MFA):** Require MFA for all logins to add an extra layer of security.

**- Regular Updates:** Keep your software and systems updated to ensure you're protected against the latest threats.

**- Cybersecurity Tools:** Firewalls, antivirus programs, and intrusion detection systems can provide robust protection against unauthorized access.

**Don't Wait Until It's Too Late**

Phishing scams are evolving fast, and it takes continuous vigilance to stay one step ahead. If you're unsure about the effectiveness of your current defenses, now is the time to act.

At CTTS, we specialize in helping businesses strengthen their cybersecurity strategies. Contact us today to ensure your organization is protected from phishing and other digital threats.

Your business is too important to leave vulnerable. Let's work together to create a safer environment for your team and clients. Reach out now!