*Cybersecurity Awareness Month*

# the NetWork

LeadingIT

Chicagoland CybersecurITy Support

October 2024

GoLeadingIT.com ☎ 815-788-6041 in @goleadingit

# Understanding the Signs of a Phishing Attack and What to Do Next

**Phishing attacks used to be easy to spot — obvious, poorly written emails that practically screamed “fraud.” Now, not so much.**

**Over time, these attacks have evolved into sophisticated schemes that can deceive even the most cautious individuals. Today, phishing attempts often involve well-crafted messages that appear to come from legitimate sources, making them a major cause for concern.**

### *Recognizing the Signs of a Phishing Attack*

Understanding the signs of a phishing attack is crucial to protecting yourself and your organization. Here are some red flags to be on the lookout for:

• Unsolicited messages: Be cautious of emails or messages from unknown senders, especially those that seem out of the blue.

• Grammar and Spelling Errors: Professional organizations rarely send communications with obvious mistakes. Poor grammar or spelling should have alarms going off in your head.

• Sense of Urgency: Cybercriminals often create a sense of urgency to manipulate your emotions. By making you feel that immediate action is necessary, they aim to bypass your rational thinking and pressure you to make rash decisions–such as clicking on a malicious link or providing sensitive information–before you have time to step back and consider the risks.

• Suspicious Links and Attachments: Avoid clicking on links or opening attachments unless you are certain of their source. You may also try hovering over links to check their actual destination before clicking.

### *What Not to Do if You Suspect a Phishing Attack*

Knowing what not to do is just as important as recognizing the signs. Here’s what you should avoid at all costs:

- **Responding to Emails:** Engaging with the sender can confirm your email address is active, leading to more phishing attempts from various email addresses.
- **Clicking Links or Downloading Attachments:** If you receive a link or attachment you weren’t expecting, even if it seems legitimate, do not click on it. These could direct you to malicious websites or install malware on your device.

*Continue reading on page 7*

*Pictured on the cover: (Left to Right) Daniel, Jeremiah, and Kyle.*

# Cybersecurity on a Budget:

## Essential Tools and Practices for SMBs

In the world of small business, every penny counts. As small and medium-sized businesses (SMBs) are increasingly finding themselves on the radar of cybercriminals, so does every aspect of their operations. While the need for robust cybersecurity is clear, many SMBs struggle to implement comprehensive protection due to budget constraints and limited resources. But with the right approach and partner, it's possible to achieve strong cybersecurity without breaking the bank.

### *Understanding the Risks*

Cybercriminals are increasingly targeting small and medium-sized businesses (SMBs), with 43% of data breaches in 2023 involving these organizations. Due to their often less robust security measures, SMBs are vulnerable to common threats like ransomware, phishing attacks, data breaches, and insider threats.

A successful cyberattack can have devastating consequences, including financial losses, operational disruptions, reputational damage, and legal liabilities. A Cisco survey from 2021 found that 61% of SMBs experienced a decline in revenue and 66% suffered a negative impact on their reputation following a cyberattack.

### *The All-Inclusive Solution*

One effective approach for SMBs is to partner with a provider offering all-inclusive IT support, such as LeadingIT. This model provides comprehensive cybersecurity coverage along with broader IT management, ensuring that all aspects of a company's technology infrastructure are protected and optimized.

### *Key Components of Comprehensive Cybersecurity*

1. **24/7 Monitoring and Support:** Round-the-clock surveillance of systems and networks is crucial for detecting and responding to threats quickly. An accessible help desk ensures that any issues are addressed promptly.
2. **Proactive Maintenance:** Regular updates, patching, and dark web monitoring help prevent vulnerabilities before they can be exploited. A managed firewall provides an additional layer of protection against cyber threats.
3. **Advanced Security Measures:** Implementing threat detection tools, conducting regular security audits, and ensuring compliance with industry standards are essential for robust protection.
4. **Data Protection and Recovery:** Automated backups, including email, and comprehensive disaster recovery planning safeguard against data loss and minimize downtime in case of an incident.
5. **Network and Infrastructure Management:** Proper design, implementation, and maintenance of network infrastructure, along with performance optimization, ensure seamless and secure operations.
6. **Strategic IT Support:** Tailored IT roadmaps, technology recommendations, and procurement services align cybersecurity efforts with business goals and growth strategies.
7. **Employee Training:** Regular cybersecurity awareness training for staff is crucial, as human error remains a significant factor in many security breaches.

### *The Value of All-Inclusive IT Support*

Opting for an all-inclusive IT support model, like that offered by LeadingIT, provides several advantages for SMBs:

- **Predictable Costs:** A fixed monthly fee covers all IT needs, including cybersecurity, without surprise charges or hourly billing.
- **Comprehensive Coverage:** From daily operations to special projects, all IT aspects are managed under one umbrella.

*Continue reading on page 6*

# 6 Ways Cybercriminals Are Exploiting MFA Weaknesses

Multi-factor Authentication (MFA) has long been touted as a robust security measure, significantly enhancing account protection beyond simple password-based systems. In fact, MFA can block over 99.9% of account compromise attacks.

However, as cybersecurity evolves, so do the tactics of malicious actors. Cybercriminals are increasingly finding ways to exploit weaknesses in MFA systems, highlighting the need for continued vigilance and improvement in security practices.

### *Understanding MFA and Its Importance*

MFA requires users to provide two or more verification factors to gain access to a resource such as an online account. While MFA significantly improves security, it's not impenetrable. Let's explore some of the ways cybercriminals are exploiting MFA weaknesses.

### *1. Social Engineering and Phishing Attacks*

One of the most common tactics used to bypass MFA is social engineering, particularly through sophisticated phishing attacks. Cybercriminals create convincing fake login pages that not only capture passwords but also intercept MFA codes.

**Best Practice:** Implement robust phishing awareness training for all users. Use email filtering systems to detect and block phishing attempts. Encourage the use of password managers that can detect when a website's URL doesn't match the legitimate site.

### *2. SIM Swapping*

For MFA systems that rely on SMS or voice calls, SIM swapping poses a significant threat.

**Best Practice:** Move away from SMS-based MFA to more secure methods like authenticator apps or hardware tokens. Encourage users to set up strong security measures with their mobile carriers, such as requiring in-person verification for SIM changes.

### *3. Man-in-the-Middle (MitM) Attacks*

In MitM attacks, cybercriminals intercept communication between the user and the authentication server. They can capture both the password and the MFA code in real time, using them to gain unauthorized access.

**Best Practice:** Use strong encryption protocols (HTTPS) for all authentication processes. Implement certificate pinning in mobile apps to prevent interception. Educate users about the risks of using public Wi-Fi networks for sensitive transactions.

### *4. Exploiting MFA Fatigue*

Some cybercriminals exploit "MFA fatigue" by bombarding users with push notifications, hoping they'll eventually approve one just to stop the notifications. This technique, also known as "MFA bombing" or "push notification spam," takes advantage of user frustration and complacency.

In 2022, Uber suffered a significant breach where the attacker used MFA fatigue to gain initial access to their systems.

**Best Practice:** Implement number matching in push notifications, where users must enter a code displayed on the login screen into their authenticator app. Set limits on the number of push notifications sent within a specific timeframe. Provide clear, contextual information in push notifications about the login attempt.

*Continue reading on page 7*

# Evaluating the Total Cost of Ownership in Hardware Procurement Decisions

When it comes to hardware procurement, many executives focus on the initial purchase price. However, a comprehensive evaluation should include the Total Cost of Ownership (TCO) to fully understand the long-term financial impact. TCO considers not just the upfront cost but also the ongoing expenses related to maintenance, support, and eventual replacement. For organizations looking to optimize their IT investments, understanding TCO is critical—especially in the context of hardware-as-a-service (HaaS) solutions.

### *The Components of Total Cost of Ownership*

TCO is composed of several key factors beyond the initial purchase price:

1. Acquisition Costs: This includes the purchase price of the hardware, any shipping, installation, and configuration costs. For many businesses, these initial expenses are the most visible, but they represent only a fraction of the total cost.
2. Maintenance and Support: Hardware requires ongoing maintenance to ensure optimal performance. This includes routine updates, troubleshooting, and repairs, which can accumulate significantly over time. Additionally, support contracts or warranties may be necessary to mitigate unexpected failures, adding to the TCO.
3. Energy Consumption: Older hardware tends to be less energy-efficient, leading to higher operational costs over time. Upgrading to newer, more efficient devices can reduce energy costs, which is an essential factor to consider when evaluating TCO.
4. Downtime Costs: Hardware failures can result in downtime, which can be costly in terms of lost productivity, customer dissatisfaction, and potential revenue loss. Proactive replacement cycles, help minimize the risk of downtime.
5. End-of-Life Disposal: When hardware reaches the end of its useful life, there are costs associated with its disposal, including data wiping, recycling, and potential environmental fees. Choosing a HaaS solution can mitigate these costs, as the provider typically handles the disposal and replacement of obsolete hardware.

### *How LeadingIT's HaaS Solution Reduces TCO*

LeadingIT's Hardware-as-a-Service (HaaS) model offers a strategic approach to reducing the TCO of your IT infrastructure. By leasing hardware through a HaaS model, businesses can avoid large upfront costs and instead spread the expenses over a manageable monthly fee. This model also includes regular hardware refreshes, ensuring that your technology stays current and efficient without the burden of large capital expenditures every few years.

1. Cost Predictability: With HaaS, hardware costs are predictable and can be planned into your budget, reducing the risk of unexpected expenses related to hardware failures or emergency replacements.
2. Regular Upgrades: LeadingIT encourages the replacement of devices every three years, which aligns with the industry standard for optimal performance and security. Regularly updating hardware ensures your organization is using the latest technology, which is more energy-efficient and less prone to failure, reducing maintenance and downtime costs.
3. Comprehensive Support: HaaS typically includes maintenance and support in the service agreement, further lowering the TCO by eliminating the need for separate support contracts or unexpected repair costs.
4. Scalability: As your business grows, so do your hardware needs. HaaS allows you to scale your hardware fleet up or down with ease, ensuring you only pay for what you need, when you need it.
5. Environmental Responsibility: HaaS providers often manage the disposal of outdated hardware in an environmentally responsible manner, reducing the costs and complexity associated with end-of-life disposal.

*Continue reading on page 6*

# The Top 3 Cloud Security Challenges and How to Mitigate Them

### *1. Effective Management*

Cloud environments are dynamic and continually evolving, making them increasingly difficult to manage. As your organization grows, adds new services, or changes configurations, the complexity increases and often leaves security gaps.

**HOW TO MITIGATE:** Automated tools that adapt to the changing environment are a great way to ensure your cloud infrastructure is managed properly. Look for automation tools that can provide continuous monitoring and real-time assessments.

### *2. Lack of Visibility*

Without clear visibility into your cloud environment, misconfigurations can go unnoticed, creating security vulnerabilities.

**HOW TO MITIGATE:** Implement cloud security posture management tools to detect and correct misconfigurations.

### *3. Regulatory Compliance*

Maintaining compliance with industry standards like GDPR, HIPAA, and PCI DSS is a significant challenge due to something called the shared responsibility model. This is where both your organization and the cloud service provider play crucial roles in protecting data.

**HOW TO MITIGATE:** Ensure your cloud service provider offers built-in compliance tools and regularly updates you on changes to regulations. Compliance audits and staff training also play a crucial role in this process.

## *Cybersecurity on a Budget*

continued from pg 3...

- **Focus on Core Business:** With IT needs handled by experts, SMBs can concentrate on their primary business activities.
- **Scalability:** As the business grows, the IT support scales accordingly without the need for significant additional investments.
- **Industry-Specific Compliance:** Expertise in ensuring your business meets all relevant regulatory requirements.
- **Cyber Insurance Support:** Reviewing policies to ensure compliance.
- **Project Work:** In-house project management from planning to execution, with no additional costs.
- **Software and Hardware Procurement:** Vendor management and procurement services to ensure you have the right tools and technology.

### *Conclusion: Implementing a Budget-Friendly Strategy*

Cybersecurity is a crucial investment for SMBs, not a luxury. By partnering with a comprehensive IT support provider like LeadingIT, SMBs can access affordable and effective cybersecurity solutions. This approach not only safeguards against evolving threats but also provides the technological foundation for growth and success.

## *Evaluating the Total Cost of Ownership in Hardware Procurement Decisions*

continued from pg 5...

### *Conclusion*

Evaluating the TCO of hardware procurement decisions is essential for making informed, strategic choices that align with your business goals. While the initial cost of hardware is a critical factor, it's important to consider the long-term costs associated with maintenance, downtime, energy consumption, and disposal. LeadingIT's HaaS solution not only helps to reduce these costs but also ensures that your business is always equipped with the latest technology, providing a competitive edge while optimizing your IT budget.

By focusing on TCO and leveraging HaaS, executives can make smarter, more cost-effective hardware decisions that contribute to the overall success and sustainability of their organizations.

## 6 Ways Cybercriminals Are Exploiting MFA Weaknesses continued from pg 4...

### *5. Bypassing MFA Through Account Recovery Processes*

Many MFA implementations have account recovery options that can be exploited. Attackers might use publicly available information to answer security questions or exploit vulnerabilities in the recovery process itself.

Here's something to think about: An attacker would have up to a 43% chance of successfully guessing a user's security answer within ten attempts, depending on the language and question asked.

**Best Practice:** Strengthen account recovery processes by requiring multiple forms of verification. Avoid using easily guessable security questions. Consider implementing a waiting period or manual review for MFA disabling requests.

### *6. Exploiting Weak Second Factors*

Not all second factors are created equal. Email-based MFA, for instance, can be compromised if the email account itself isn't adequately protected. Similarly, security questions often rely on information that could be easily researched or guessed.

**Best Practice:** Phase out weaker MFA methods like SMS or email in favor of stronger options like FIDO2-compliant hardware keys or biometrics. If using software tokens, ensure they are protected by device encryption and biometric unlock.

### *Conclusion: MFAs Are Only Part of the Solution*

While MFA remains a crucial layer of security, it's clear that it's not a silver bullet. As cybercriminals continue to evolve their tactics, organizations must stay informed about potential vulnerabilities and adopt a multi-layered approach to security. This includes using the strongest MFA methods available, regularly updating security protocols, and providing ongoing education to users about emerging threats.

## Understanding the Signs of a Phishing Attack and What to Do Next

continued from pg 2...

- **Giving Out Personal Information:** Legitimate organizations will never ask for sensitive information via email. Do not share personal or financial details in response to an email. In fact, many organizations, like title companies, have a fraud warning in their email signatures reminding people not to share confidential information.

### *What You Should Do Instead*

Once you've identified a potential phishing attack, take these steps to protect yourself:

1. Report the Phishing Attempt: Most email providers offer tools to report phishing. For example, in Gmail, you can:
   a. Open the suspicious email (avoid clicking links or attachments).
   b. Click on the three vertical dots in the top right corner of the message.
   c. Select "Report phishing" from the dropdown menu.
   d. Follow the on-screen instructions to complete the report.
2. Delete the Email: After reporting, immediately delete the email from your inbox and trash the folder.
3. Update Your Security Software: Ensure that your antivirus software and other security tools are up-to-date to protect against future threats.

Alternatively, if you think you've been the victim of an attack that you already responded to, take the following action ASAP:

- Change your passwords
- Contact the affected Institution
- Monitor your accounts
- Run a security scan with your antivirus software

### *Stay Vigilant*

Phishing attacks are a growing threat, but with the right cybersecurity solutions, education, and tools, you can significantly reduce your risk. Remember, cybersecurity is a shared responsibility. So, make sure your team is aware of how dangerous these insidious attacks are.

# LeadingIT Core Values Victor of the Month

This month, we are thrilled to honor not one, but two outstanding individuals as Values Victors for Chasing Excellence: Mark and Scott.

Every day, Mark and Scott push boundaries, set high standards, and lead by example, consistently striving to deliver the best outcomes for our company, our team, and our clients. Their dedication to excellence not only elevates the quality of our work but also inspires all of us to reach higher. Congratulations, Mark and Scott!

## LEADINGIT VALUES:

- We Are Driven
- We Chase Excellence
- We Are Humbly Confident
- We Are Accountable
- We Have A Positive/Fun Mindset

*Continue reading on our blog at goleadingit.com/blog*

LeadingIT

Serving the Chicagoland area with
offices in Woodstock, Downtown Chicago,
and now in Manteno, IL.

LeadingIT

# $1000 REFERRAL PROGRAM

**WE LOVE REFERRALS!**

Do you know an organization that needs fast + friendly IT and cybersecurity support?

**If they sign up, you'll receive $1000!**

LEARN MORE

GOLEADINGIT.COM/REFER
815-788-6041

## WE ARE CELEBRATING!

### Birthdays

**Garrett McCleary** - October 5th

**Dustin Looper** - October 10th

**Andrew Foote** - October 16th

**Mark Peasley** - October 25th

**John Funk -** October 26th