

the NetWork LeadingIT

Chicagoland Cybersecurity Support

January 2025




Resolutions for a More Secure Business in 2025


Don't Take the Bait: How to Report Phishing Emails

Boost Your Business with AI: Top AI Tools for SMBs

Cyber Insurance For Small Business: Why You Need It And How to Get Covered In 2025

LeadingIT Core Values Victor

 GoLeadingIT.com

 815-788-6041

 @goleadingit

RESOLUTIONS FOR A MORE SECURE BUSINESS IN

2025

loading...

How confident are you in your business's ability to withstand a cyberattack? On January 1, 2025, many organizations will continue operating with the same outdated security measures, leaving them vulnerable to sophisticated cyberattacks.

Don't let your business become a statistic by this time next year. By committing to a multi-layered security strategy, you can not only protect your data but also ensure operational resilience. Here are the steps you can take to start the new year on a more secure footing.

1

Multi-Factor Authentication

MFA is one of the simplest yet most effective measures to secure access to your systems. By requiring users to verify their identity through two or more methods, such as a password and phone verification process, it significantly reduces the risk of unauthorized access.

2

Managed Firewalls

A firewall is your first line of defense against external threats. A managed firewall service not only blocks malicious traffic but also provides continuous monitoring and updates to adapt to evolving threats. Partnering with a cybersecurity company like LeadingIT ensures your firewall is always up-to-date, minimizing vulnerabilities.

3

Email Security

Phishing attacks remain one of the most common ways cybercriminals infiltrate businesses. Advanced email security tools, such as spam filters and anti-phishing software, are essential for detecting and blocking malicious emails before they reach your employees' inboxes. Additionally, training employees to identify phishing attempts adds another crucial layer of protection.

4

Dark Web Monitoring

Would you know if your business's credentials were exposed to the dark web? Dark web monitoring alerts you if sensitive information, like employee passwords or customer data, has been compromised, allowing you to act before it's exploited. Services like these can save businesses from catastrophic breaches and financial loss.

Pictured on the cover: Laura, Kelly, Mark

Don't Take the Bait:



How to Report Phishing Emails

Phishing emails are fraudulent messages designed to trick you into revealing sensitive information, such as passwords, credit card numbers, or bank account details. The Anti-Phishing Working Group (APWG) reports that an alarming 3.4 billion phishing emails are sent worldwide daily, and chances are one of these emails has landed in your inbox.

So what should you do when you get a phishing email? First, great job on identifying the phishing attempt. The next step is to report the phishing email.

Why Report Phishing Emails?

Your personal information, like your credit card number or social security number, could be stolen with a single click on a phishing email. It's a scary thought, but the reality is that 90% of data breaches are caused by these malicious attacks.

Reporting phishing emails is a simple yet powerful step that you can take to protect yourself and others from cyberattacks. By taking a few minutes to report these malicious messages, you're helping to make the internet a safer place. Your reports help law enforcement catch bad actors and help tech companies improve their security measures.

How to Report a Phishing Email

1. **Do Not Click on Links or Attachments:** Never click on any links or attachments in a suspicious email. This could lead to malware infection or unauthorized access to your accounts.

2. **Do Not Reply to the Email:** Avoid replying to the phishing email, as this could confirm your email address to the scammers.
3. **Forward the Email to Your Email Provider:** Most email providers have built-in reporting features. Look for a "Report Phishing" or "Report Spam" button within your email client.
4. **Report to the Anti-Phishing Working Group (APWG):** You can forward the phishing email to reportphishing@apwg.org. This organization collects and analyzes phishing reports to help identify and stop phishing attacks.
5. **Report to the Federal Trade Commission (FTC):** You can report phishing attempts to the FTC at ReportFraud.ftc.gov. This will help the FTC track phishing trends and take action against cyber criminals.
6. **Report to the Internet Crime Complaint Center (IC3):** If you believe you have been a victim of a phishing scam that resulted in financial loss, you can file a complaint with the IC3 at ic3.gov.

Additional Tips for Protecting Yourself from Phishing Attacks:

- **Be Skeptical:** Be wary of unsolicited emails, especially those that create a sense of urgency or offer incredible deals.

Continue reading on page 6

Boost Your Business with AI:



TOP AI TOOLS FOR SMBS

Artificial Intelligence (AI) is not just a buzzword—it's reshaping how businesses operate. In fact, 82% of companies are already adopting or exploring AI technology, and AI adoption is expected to contribute \$15.7 trillion to the global economy by 2030. From automating routine tasks to generating creative content, AI tools can greatly enhance your productivity and efficiency. Here are some top AI tools that SMBs can benefit from:

AI for Content Creation

- **InVideo AI:** This tool can help you create professional videos quickly and easily. With AI-powered features, you can generate personalized intros, outros, and even entire videos from text scripts.
- **Leonardo.ai:** Leonardo.ai can generate high-quality images and art based on text prompts. This tool is perfect for social media graphics, website banners, or product mockups.
- **Jasper AI:** Jasper is an AI-powered writing tool that helps you write blog posts, social media content, emails, and more. With templates and suggestions tailored to your brand voice, Jasper can help you write faster and more effectively, whether you're creating long-form content or short snippets.

AI for Communication and Customer Service

- **ChatGPT:** Enhance customer service with AI-powered chatbots. These chatbots can handle routine inquiries, provide product information, and even resolve simple issues, freeing up your team to focus on more complex tasks.

- **Grammarly Business:** Ensure professional communication with Grammarly's AI-powered writing assistant. It helps you write clear, concise, and error-free emails, reports, and other documents.

AI for Productivity

- **Microsoft Copilot:** Copilot integrates with Microsoft 365 apps like Word, Excel, and PowerPoint. It helps users draft documents, summarize meetings, and generate data-driven insights, making it easier to handle tasks like report generation and presentations.
- **Calendly:** Calendly automates the scheduling process, allowing clients and team members to select available meeting times without back-and-forth emails. It can integrate with calendars and time zones, making it easy to schedule with global clients and coworkers.
- **Todoist:** Use this tool to organize your to-do list, prioritize tasks based on deadlines, and track progress on multiple projects. This tool integrates with various platforms like Google Calendar and Slack and helps teams stay on top of important tasks without losing momentum.

Continue reading on page 7

CYBER INSURANCE FOR SMALL BUSINESS:

WHY YOU NEED IT AND HOW TO GET COVERED IN 2025

What Is Cyber Insurance?

Cyber insurance is a policy that helps cover the costs related to a cyber incident, such as a data breach or ransomware attack. For small businesses, this can be an essential safety net. If a breach happens, cyber insurance can help cover:

- **Notification Costs:** Informing your customers about a data breach.
- **Data Recovery:** Paying for IT support to recover lost or compromised data, such as restoring computer systems.
- **Legal Fees:** Handling potential lawsuits or compliance fines if you're sued because of an attack.
- **Business Interruption:** Replacing lost income if your business shuts down temporarily.
- **Reputation Management:** Assisting with PR and customer outreach after an attack.
- **Credit Monitoring Services:** Assisting customers impacted by the breach.
- **Ransom Payments:** Depending on your policy, cyber insurance will cover payouts in some cases of ransomware or cyber extortion.

These policies are typically divided into first-party and third-party coverage.

- First-party coverage addresses losses to your company directly, such as system repair, recovery and incident response costs.
- Third-party coverage covers claims made against your business by partners, customers or even vendors who are affected by the cyber incident.

Think of cyber insurance as your backup plan for when cyber risks turn into real-world problems.

Do You Really Need Cyber Insurance?

Is cyber insurance legally required? No. But, given the rising costs of cyber incidents, it's becoming an essential safeguard for businesses of all sizes. Let's look at a

couple of specific risks small businesses face:

- **Phishing Scams:** Phishing is a common attack targeting employees, tricking them into revealing passwords or other sensitive data. You would be shocked at how often we do phishing tests in organizations and multiple people fail. Your employees cannot keep your business safe if they don't know how.
- **Ransomware:** Hackers lock your files and demand a ransom to release them. For a small business, paying the ransom or dealing with the fallout can be financially devastating. Not to mention, in most cases, once the payment is received, the data is deleted anyway.
- **Regulatory Fines:** If you handle customer data and don't secure it properly, you could face fines or legal actions from regulators, especially in sectors like health care and finance.

While having strong cybersecurity practices is critical, cyber insurance acts as a financial safety net if those measures fall short.

Continue reading on page 6



■ *How to Report Phishing Emails* continued from pg 3...

- **Verify the Sender:** Hover your mouse over the sender's email address to check the actual domain name. Look for misspellings or unusual domains.
- **Check for Typos and Grammar Errors:** Phishing emails often contain grammatical errors or typos.
- **Be Cautious on Social Media:** Be mindful of what you share on social media, as scammers can use this information to personalize their phishing attacks.

The Bottom Line

The fight against phishing requires a collective effort. By reporting these scams and following the additional tips, you become a proactive defender of online security. So, the next time you encounter a suspicious email, remember: don't click anything, don't reply to anything, and report it!

■ *Cyber Insurance For Small Business* continued from pg 5...

The Requirements For Cyber Insurance

Now that you know why cyber insurance is a smart move, let's talk about what's required to qualify. Insurers want to make sure you're taking cybersecurity seriously before they issue a policy, so they'll likely ask about these key areas:

1. Security Baseline Requirements

- Insurers will check that you have basic security measures like firewalls, antivirus software and multifactor authentication (MFA) in place. These are foundational tools to reduce the likelihood of an attack and show that your business is actively working to protect its data. Without them, insurers may refuse coverage or deny claims.

2. Employee Cybersecurity Training

- Believe it or not, employee errors are a major cause of cyber incidents. Insurers know this and often require proof of cybersecurity training. Teaching employees how to recognize phishing e-mails, create strong passwords and follow best practices goes a long way toward minimizing risk.

3. Incident Response And Data Recovery Plan

- Insurers love to see that you have a plan for handling cyber incidents if they occur. An incident response plan includes steps for containing the breach, notifying customers and restoring operations quickly. This preparedness not only helps you recover faster but also signals to insurers that you're serious about managing risks.

4. Routine Security Audits

- Regularly auditing your cybersecurity defenses and conducting vulnerability assessments help

ensure your systems stay secure. Insurers may require that you perform these assessments at least annually to catch potential weaknesses before they become big problems.

5. Identity Access Management (IAM) Tools

- Insurers will want to know that you're monitoring who is accessing your data. IAM tools provide real-time monitoring and role-based access controls to make sure that only select people have access to the data they specifically need when they need it. They'll also check that you have strict authentication processes like MFA to enforce this.

6. Documented Cybersecurity Policies

- Insurers will want to see that you have formalized policies around data protection, password management and access control. These policies set clear guidelines for employees and create a culture of security within your business.

This is only the tip of the iceberg. They'll also consider if you have data backups, enforce data classification and more.

Conclusion: Protect Your Business With Confidence

As a responsible business owner, the question to ask yourself isn't if your business will face cyberthreats – it's when. Cyber insurance is a critical tool that can help you protect your business financially when those threats become real. Whether you're renewing an existing policy or applying for the first time, meeting these requirements will help you qualify for the right coverage.

AI for Data Analysis and Optimization

- **Power BI or Tableau:** Take advantage of the power of your data with these AI-powered business intelligence tools. Visualize data, identify trends, and make informed decisions to drive business growth.
- **SEMrush:** Improve your online visibility with this SEO tool. SEMrush can help you optimize your website for search engines, track your competitors, and analyze your backlink profile.

AI for Financial Management

- **QuickBooks with AI:** Automate accounting tasks such as expense tracking, invoicing, and tax calculations with QuickBooks' AI features. It helps you streamline your financial operations and gain better insights into cash flow.
- **Xero:** Xero uses AI to simplify accounting processes, allowing you to automate bill payments, reconcile bank transactions, and generate financial reports.
- **Expensify:** This AI-powered tool can automatically scan receipts, categorize expenses, and generate expense reports.



Backup and Disaster Recovery

5

Even the most secure systems can experience breaches or data loss. That's why reliable backups and a disaster recovery plan are crucial. Ensure backups are automated, encrypted, and stored off-site or in the cloud. With a comprehensive recovery plan, you can minimize downtime and avoid devastating data loss, ensuring business continuity. Even the most secure systems can experience breaches or data loss. That's why reliable backups and a disaster recovery plan are crucial. Ensure backups are automated, encrypted, and stored off-site or in the cloud. With a comprehensive recovery plan, you can minimize downtime and avoid devastating data loss, ensuring business continuity.

Employee Education

6

Human error remains a leading cause of security incidents. Empower your team by providing regular cybersecurity training, teaching them how to recognize threats, use strong passwords, and follow best practices. An educated workforce is a powerful shield against cyberattacks. In fact, 74% of cyber breaches are caused by human error. Prioritize employee education and build a culture of security awareness to minimize your overall threat risk.

Start the New Year on a Secure Note

If your business needs expert guidance to uplevel its security practices, LeadingIT offers all-inclusive IT services, from managed firewalls to employee training. As your trusted partner, we will help you stay secure and growth-focused.

LeadingIT Core Values Victor of the Month



Congratulations to Jeremiah Bird, our Bench Manager and Level 2 Technician, for clinching this month's Values Victor for Chasing Excellence!

Jeremiah has expanded his knowledge since he started as a bench tech, consistently pushing himself and growing into his current role. His journey and dedication to improvement are truly inspiring, making a significant impact on our team and lifting everyone's game.

Thanks, Jeremiah, for always setting the bar high and inspiring us all to level up. We're so lucky to have you!

LEADINGIT VALUES:

- We Are Driven
- We Chase Excellence
- We Are Humbly Confident
- We Are Accountable
- We Stay Positive

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



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



\$1000 REFERRAL PROGRAM

Do you know an organization that needs unlimited IT and cybersecurity support with an unbeatable guarantee?

You'll earn **\$50** for every referral.
If they sign up, you'll receive **\$1000!**

LEARN MORE



[GOLEADINGIT.COM/REFER](https://goleadingit.com/refer)

815-788-6041



WE ARE CELEBRATING!

Birthdays

Daniel Rabenold - January 6th
Lori Yarnall - January 21st
Simon Ramirez January 31st

Anniversaries

Stephen Taylor - 1/1/2010
James Clayton - 1/31/2022
John Funk - 1/23/2023
Bryce Frank - 1/29/2024