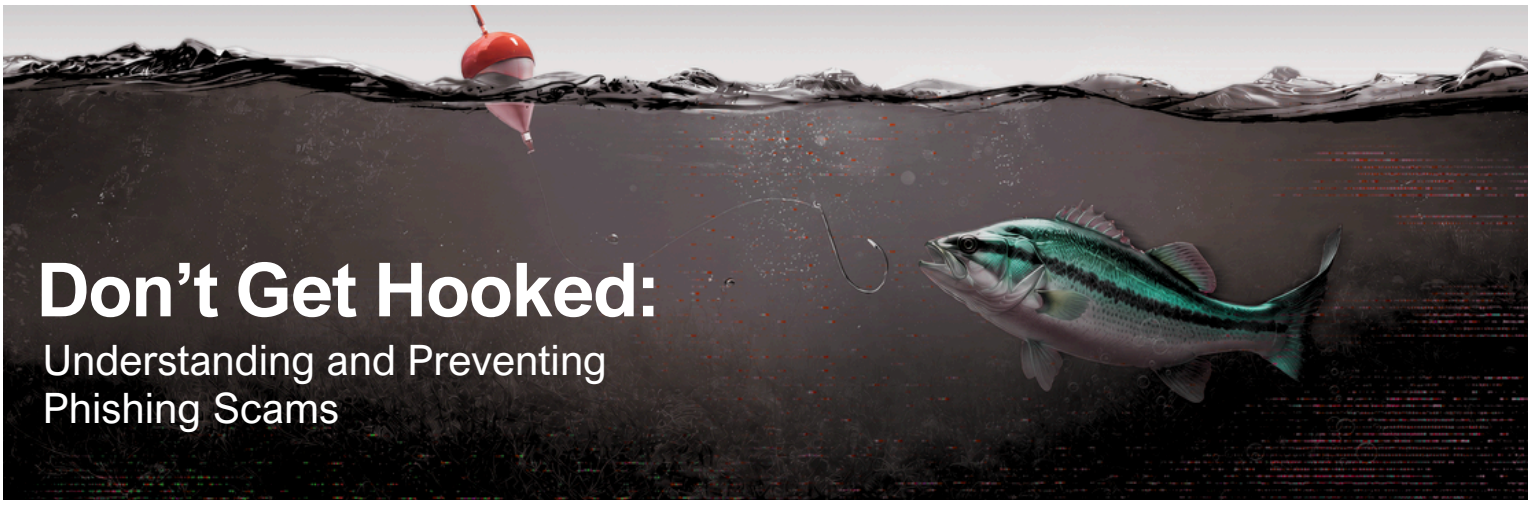
October 2026

Tech Times

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



Don't Get Hooked:

Understanding and Preventing Phishing Scams

An email from a trusted partner lands in your inbox. Everything seems legitimate. The branding is familiar. The message sounds professional. You click the link, and just like that, you're caught in a phishing trap. AI is helping cybercriminals create polished messages, making scams harder than ever to spot. It's crucial for decision-makers to understand these evolving threats and take steps to protect their data.

Easy-to-spot phishing scams with obvious requests for sensitive information, poor grammar and suspicious links are a thing of the past. Cybercriminals now use AI to create convincing messages that sound like they come from trusted sources.

Even careful, well-trained employees can be tricked by these messages.

COMMON TYPES OF PHISHING SCAMS

Email phishing: Attackers send emails that appear to come from a trusted source. The messages may contain malicious links or attachments designed to steal information, gain access to accounts or install malware.

AI-powered phishing: Cybercriminals create messages based on online information. They copy someone's writing style, mention real business relationships or use details about an employee to appear legitimate.

Spear phishing: To attack a specific person or business, bad actors research their victim and use relevant details to create a highly personalized message to gain the recipient's trust.

Business email compromise: An attacker impersonates an executive, employee or vendor to request payment, banking details or sensitive information.

Smishing: Hackers use text messages to get recipients to click on a malicious link, share information or call a fraudulent number.

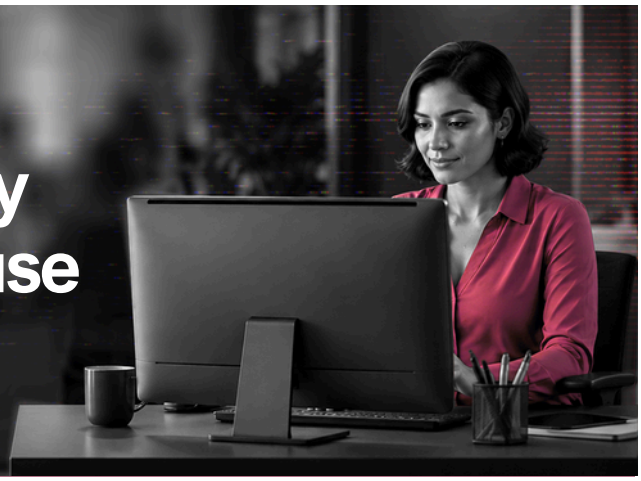
QR-code phishing: Also known as quishing, this uses a QR code to direct someone to a fake website. They often appear in emails, documents, posters or packages.

HOW TO PROTECT YOUR BUSINESS FROM PHISHING ATTACKS

- Train employees to recognize AI-generated emails and other phishing tactics.
- Use advanced email security tools to detect malicious links and attachments.
- Enable multi-factor authentication.
- Verify urgent requests for payments, passwords or sensitive data in a separate channel.
- Limit publicly available employee and business information.
- Keep software, systems and security tools up to date.
- Make it easy for employees to report suspicious messages.

Key Takeaway:
One convincing message can expose sensitive data, so knowing what to watch for is key to staying secure.

Your Biggest Cybersecurity Risk May Be Inside the House



When most businesses think about cybersecurity, they picture a hacker across the world. But damaging threats can already be inside your business. Employees, vendors, partners and executives pose a significant risk to business, whether through intent or simple mistakes. Understanding these threats, recognizing warning signs and knowing how to respond could be the difference between a close call and a costly breach.

Insider threats aren't one-size-fits-all. They come in several forms, each with its own potential to cause serious harm.

Data theft
Data theft is when someone downloads, copies or leaks sensitive information. It includes stealing company devices.

Sabotage
Sabotage is when an employee, activist or competitor damages, disrupts or destroys your organization by deleting important files, infecting devices or locking critical systems.

Unauthorized access
Unauthorized access is when someone gains access to business-critical information they shouldn't be viewing, either intentionally or unintentionally.

Negligence and error
Mishandled data, ignored security protocols and avoidable mistakes can unintentionally expose your business as effectively as a malicious actor.

Credential sharing
Sharing passwords with colleagues or friends creates opportunities for unauthorized access and cyberattacks.

Unauthorized AI use
Employees use AI tools that aren't approved by your business and expose sensitive company or customer information.

SPOTTING RED FLAGS

Train your team to keep an eye out for these tell-tale signs of insider threats.

Unusual access patterns: An employee begins accessing confidential company information unrelated to their role.

Excessive data transfers: An employee downloads a large volume of data or moves it to external storage devices.

Authorization requests: Someone repeatedly requests access to business-critical information.

Use of unapproved devices: Employees access confidential business data on personal laptops or other devices.

Disabling security tools: Someone disables antivirus software, firewall protections or other security controls.

Behavioral changes: One of your employees begins missing deadlines, acting unusually secretive or displaying signs of extreme stress.

BUILDING YOUR DEFENSES FROM THE INSIDE OUT

Here are five steps you can take to build a comprehensive cybersecurity framework and help keep your business protected.

1. Implement a strong password policy and use multi-factor authentication.

2. Ensure your employees access only the data and systems required for their roles. Regularly review and update privileges.

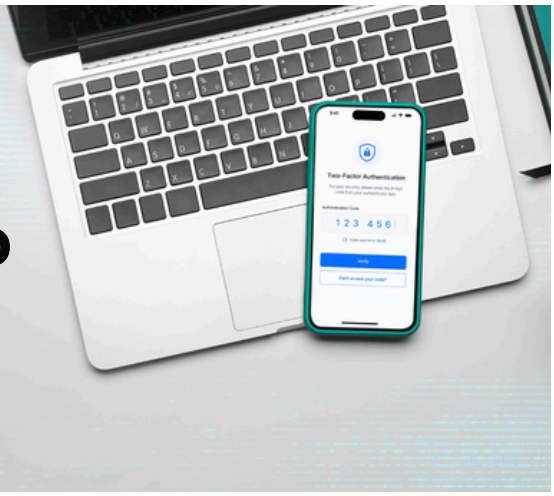
3. Educate and train your employees on insider threats, security best practices and the safe use of AI tools.

4. Back up your important data regularly to be sure you can recover from an incident.

5. Develop a comprehensive incident response plan outlining how your business will address insider threat incidents.

Key Takeaway:
Keep an eye out for cybersecurity risks both inside and outside your business.

6 Free Ways to Improve Your Cybersecurity



Cybersecurity is often treated as another expensive technology problem. However, the biggest risks for many businesses come from missed, delayed or inconsistent security practices.

Here are the six free improvements you can make this week to reduce cyber risk.

1. TURN ON MULTI-FACTOR AUTHENTICATION

Multi-factor authentication, or MFA, should be your first priority. It adds another step to the sign-in process, so even if someone uses a stolen password, they can't easily access the account.

Most platforms offer MFA for free. Turning it on closes one of the easiest gaps that attackers exploit.

Enable it first for:

- Microsoft 365 or Google Workspace
- Banking and payroll
- Cloud storage
- VPN access
- Business-critical applications

2. REMOVE ACCOUNTS NO ONE USES

Accounts belonging to former employees, temporary contractors and old vendors can remain active long after they're gone. Because these accounts are often overlooked, they may provide attackers with an easier entry point to your systems.

Review your user accounts and ask:

- Does this person still work with us?
- Does this account still serve a business purpose?
- Does the account still need the access it has?

If the answer is no, disable or remove the account.

3. STOP GIVING EVERYONE ADMINISTRATOR ACCESS

Administrator accounts have broad control over your systems. They can install software, change settings and disable security protections. That makes them especially valuable to attackers.

Take stock of access across your business and ask:

- Does this person need it to do their job?
- Could they use a standard account?
- Is administrative access still appropriate for the accounts that currently have it?

Remove administrator privileges where they're not required. Giving people only the access they need helps limit the impact of a compromised account.

Cartoon of the Month

"You must be the new remote employee."

10 Steps to Build a Cyber-Smart Team

Cybersecurity isn't just an IT responsibility. It's a team sport. Follow these 10 steps to make every employee a defender of your business.

1. Train your team
2. Encourage communication
3. Lead by example
4. Establish clear guidelines
5. Recognize good practices
6. Make it personal
7. Test your team's readiness
8. Encourage employees to speak up
9. Tailor training by role
10. Unite your team

4. TURN ON AUTOMATIC UPDATES

Attackers often target software with known vulnerabilities. Updates help close those gaps.

Check that automatic updates are enabled for:

- Windows and macOS
- Phones and tablets
- Web browsers
- Microsoft Office
- Antivirus software
- Key business applications

Keeping systems up to date closes known gaps before attackers can use them.

5. START USING A PASSWORD MANAGER

Strong passwords matter, but expecting employees to remember a complex, unique password for every account isn't realistic.

A password manager can help users:

- Create strong passwords
- Store them securely
- Avoid password reuse
- Share credentials safely when needed

The fewer passwords employees have to remember, the less likely they are to reuse weak ones.

6. MAKE SURE YOUR BACKUPS WORK

Having backups isn't enough. You need to know you can restore your data when something goes wrong.

Check your backups and ask:

- When did our last successful backup run?
- Has anyone tested a restore recently?
- How long would recovery take?

A backup protects your business only if it works when you need it.

.....

Key Takeaway:
Cybersecurity doesn't have to start with a major investment. It starts with closing the gaps that create unnecessary risk.

The six steps discussed in this article can reduce common risks without adding cost.

COMING NEXT MONTH

IT BUDGET FORECASTING

Next month, we're helping you take the guesswork out of IT budgeting. From aging hardware and software renewals to new hires and unexpected expenses, knowing what's ahead can help you plan with confidence. We'll show you what to put on your radar, where surprise costs can hide and how to build a clearer technology forecast so you can make smarter decisions about your business in the year ahead.

Find What's Lurking in Your Network This October?

Cyber threats don't wear costumes.

Hidden vulnerabilities, exposed passwords, and phishing risks could be putting your business at risk right now.

Our FREE Cybersecurity Risk Analysis uncovers security gaps, tests your defenses, and helps ensure your backups can protect your business when it matters most.

Don't let cybercriminals scare you this season.

INSTANTLY CLAIM YOUR FREE CYBERSECURITY RISK ANALYSIS: WWW.WINDSTARTECH.COM/CYBERRISK OR CALL OUR OFFICE AT (877) 310-0123