October 2026

GIO Tech Times

Putting the Power of IT Back in Your Business with Insider Tips for Speed, Simplicity, and Profit



Don't Get Hooked:

Understanding and Preventing Phishing Scams

An email from a trusted partner lands in your inbox. The branding looks familiar, the message sounds professional, and everything seems legitimate. You click the link, and just like that, you may be caught in a phishing trap.

The days of obvious phishing emails filled with poor grammar, strange formatting, and suspicious requests are fading. Cybercriminals are now using AI to create polished, convincing messages that are much harder to identify. AI can help attackers mimic a person's writing style, reference real business relationships, and use information found online to make a message feel authentic.

Phishing can take several forms, including email, text messages, QR codes, and highly targeted attacks against specific employees. Business email compromise is another common tactic, where an attacker impersonates an executive, employee, or vendor to request payments, banking information, or sensitive data.

Even careful, well-trained employees can be fooled, which is why technology and employee awareness need to work together.

How can your business stay protected?

Train employees regularly on current phishing tactics and encourage them to slow down when something feels unusual. Use strong email security tools to help detect malicious links and attachments, and enable multi-factor authentication to add another layer of protection.

Most importantly, verify unexpected or urgent requests through a separate communication method. If an email asks for a payment, password, wire transfer, or sensitive information, take a moment to confirm it before taking action.

Make sure employees also know how and where to report suspicious messages. Creating a culture where employees can ask questions without hesitation can prevent one convincing message from becoming a much bigger problem.

Phishing attacks are becoming more sophisticated, but slowing down, staying aware, and verifying unexpected requests can make all the difference.



POWERING IT *with Dan*

Employees are the Best Firewall

When most businesses think about cybersecurity, they think about firewalls, monitoring, and security software. While these tools are essential, your employees are just as important to your cybersecurity strategy.

Cybercriminals are constantly finding new ways to trick people through phishing emails, fake login pages, and convincing messages. Even the most cautious employee can be caught off guard when a threat looks legitimate.

That is why cybersecurity awareness training matters. It is not about making employees feel like the weakest link. It is about giving them the knowledge and confidence to recognize threats, make informed decisions, and know what to do when something does not look right.

At GIO Technologies, we believe education is one of the most powerful cybersecurity tools. Our training provides employees with practical skills to help protect themselves and your business.

Want to schedule training or a refresher for your team? Please reach out to us.

Dan Giordano
dan@giotechnologies.com

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.

TEAM GIO



Powered by Joe

Slow Down Before You Click

Cybersecurity does not always require complicated technology or an IT expert sitting beside you. Sometimes, one of the best ways to stay safe is simply to **slow down**.

We are all busy, and cybercriminals know it. They use urgency to get us to act before we have time to think. "Your account will be locked." "I need this right away." "Can you send this payment?" These messages are designed to make you react instead of question.

Before clicking a link, opening an attachment, or responding to an unexpected request, take a moment to look closely. Do you recognize the sender? Does the email address look right? Is the request unusual? Would you normally receive a message like this?

If something feels off, trust your gut and check before taking action. Reach out to the person directly using a phone number you already have, not one included in the suspicious message. Avoid replying to the email since their account could be compromised.

Remember, you do not have to figure it out alone. If you are ever unsure about an email, link, or request, call GIO. We are always happy to be an extra set of eyes and help you determine if something is safe.

Cybersecurity is a team effort, and every employee plays a role. When in doubt, pause, verify, and ask questions. A few extra seconds can make a big difference.

-Joe Costantino
support@giotechnologies.com

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.

GIO MONTHLY MOMENTS

Team GIO Customer Surveys

You may have noticed a new customer survey added to the bottom of our tickets. Your feedback means a lot to us because our top priority is, and always will be, having happy clients. We'd love to hear what we're doing well and if we can improve. Your feedback helps us continue to provide the level of service you expect from Team GIO.

As always, thank you for trusting us with your IT. We don't take that responsibility lightly, and we truly appreciate the opportunity to support your business.



We were proud to support the Harford County Deputy Sheriffs' Union at their annual golf tournament on 9/11. It was a great day to come together, support our local first responders, and honor others on this important day.

Our new office buildout is moving along quickly. The finish line is coming and we can't wait! October may be the month we close this project - We aren't trying to rush it but we are very excited to get into our new home at Rock Spring Road. Thank you to Petrie Construction for their hard work.





We are in the process of changing our mailing address. Please note our new mailing address is:

GIO Technologies, Inc.
2018 Rock Spring Road
Forest Hill, MD 21050