

Cybersecurity Awareness Month

Protect Your Business with Point Alliance

Solutions for **Success**



POINT ALLIANCE

Presentation Overview

- About Point Alliance
- Recent Cyber Attacks
- Why Microsoft Cloud?
- The Three Pillars of Cybersecurity 
- Staying Secure at Work and Home:
Best Practices for All
- Assessment Offerings
- Next Steps



Point Alliance

Jonathan Hamilton

- **President** \Point Alliance
- jonathan.hamilton@pointalliance.com
- [linkedin.com/in/jonathandavidhamilton](https://www.linkedin.com/in/jonathandavidhamilton)



John Zarei

- **CEO** \Point Alliance
- john.zarei@pointalliance.com
- linkedin.com/in/**johnzarei**



Point Alliance

- Microsoft Solutions Partner
 - Modern Work
 - Security
 - Digital & App Innovation Azure
 - Data & AI Azure
- Microsoft Gold Partner with 11 Competencies (legacy)
- 100% Microsoft Certified Team
- pointalliance.com/companyprofile



Recent Cyber Attacks

Every year the number of attacks increases, and adversaries develop new methods of evading detection.



Increase in Cyberattacks: Cyberattacks surged nearly 50% in early 2025, with ransomware incidents up 126% year-over-year.



Evolving Threats: Adversaries are leveraging AI-driven phishing, deepfakes, and stolen credentials to evade detection.



Email Exposure: Around 90% of cyber incidents still begin with a phishing or email-based attack vector.



Cost of Data Breaches: The average global data breach cost reached \$4.88 million in 2024, the highest on record.

Why Microsoft Cloud?

Why Companies with Security Concerns Should Choose Microsoft Cloud?



Comprehensive Security Features

Antiphishing, Antispam, and Antimalware: Built-in protection against common threats

Advanced Threat Protection**: Real-time threat detection and response capabilities



Data Protection and Compliance:

Encryption: Protects data both in transit and at rest

Data Loss Prevention (DLP): Prevents accidental sharing of sensitive information

Compliance Manager: Helps manage and meet regulatory requirements



Seamless Integration:

Unified Management: Centralized management of security policies and configurations

Integration with Microsoft 365 Apps: Enhances productivity while maintaining security



Scalability and Flexibility:

Supports Both SMBs and Enterprises: Tailored solutions for businesses of all sizes

BYOD Support: Securely manage both corporate and personal devices



Proactive Security Measures:

Regular Security Updates: Continuous improvements and updates to security features

AI and Machine Learning: Utilizes advanced technologies to detect and mitigate threats

Microsoft Our unique vantage point

100 trillion	4.5 million	38 million
100 trillion security signals processed daily	4.5 million net new malware file blocks every day	38 million identity risk detections analyzed in an average day
15,000+	34,000	5 billion
15,000 partners in our security ecosystem, making it one of the largest in the world	34,000 full-time equivalent security engineers employed worldwide	5 billion emails screened daily on average to protect users from malware and phishing

Microsoft Bragging Right...



Recognized as a Leader in the Gartner, Inc. Magic Quadrant™ for Access Management for the 8th consecutive year (2024).



Named a Leader in the Gartner Magic Quadrant™ for Endpoint Protection Platforms in 2025 (6th consecutive appearance).



Named a Leader in the Forrester Research Wave™: Zero Trust Platform Providers in Q3 2025.



Ranked #1 globally for modern endpoint security market share for three years in a row (25.8 % share in 2023, growing to 28.6 % in 2024) per IDC.

The Three Pillars of Cybersecurity

The Three Pillars of Cybersecurity: Technology, Processes and People

An effective cybersecurity program includes **technology** solutions, **processes**, and **people** that together reduce the risk of business disruption, financial loss, and reputational damage from an attack.

Technology



Intune and Endpoint Management: Point Alliance helps you leverage Microsoft Intune to manage and secure all your endpoints (laptops, mobile devices, etc.). This ensures that devices accessing your network are compliant with security policies and reduces the risk of data breaches.



Cost-Effective Security Solutions: We implement essential security tools like firewalls, antivirus software, and spam filters designed for SMBs to protect your business without excessive cost.



Multi-Factor Authentication (MFA) Setup: We simplify the deployment of MFA across your key systems, adding an extra layer of security without disrupting daily operations.



Data Backup and Recovery: Our team sets up automated, secure backup solutions that protect your critical data both on-premises and in the cloud.



Continuous Monitoring and Alerts: Point Alliance offers affordable endpoint monitoring tools that provide real-time alerts for suspicious activity, enabling quick, proactive action.

Processes

Incident Response Planning: Point Alliance will collaborate with you to create a streamlined incident response plan, ensuring rapid action and minimal disruption in case of an attack.

01

Policy Audits and Updates: We regularly audit and update your security policies, making sure they align with industry standards and regulatory compliance.

02

Affordable Risk Assessments: We provide risk assessments that fit your budget, helping you identify and mitigate vulnerabilities in your business.

03

Patch Management Services: Our managed patching services keep your software and systems up to date, reducing exposure to known vulnerabilities.

People



Tailored Employee Training: Point Alliance offers customized cybersecurity training programs for SMBs, ensuring employees understand threats and adopt best practices without complexity.



Access Control Solutions: We help set up role-based access controls, ensuring employees only have access to the systems and data relevant to their roles.



Promoting a Security-First Culture: Our team helps foster a security-conscious environment, with clear protocols and easy reporting mechanisms for suspicious activity.

Staying Secure at Work and Home: Best Practices for All

Staying Secure at Work and Home: Best Practices for All

The Threat Landscape



DIGITAL



IN-PERSON



PHONE

Common Traits of Phishing

Asking for
Personal Info.

Inconsistencies
in Links

Unrealistic
Threats

Generic
Greetings

A Sense of
Urgency

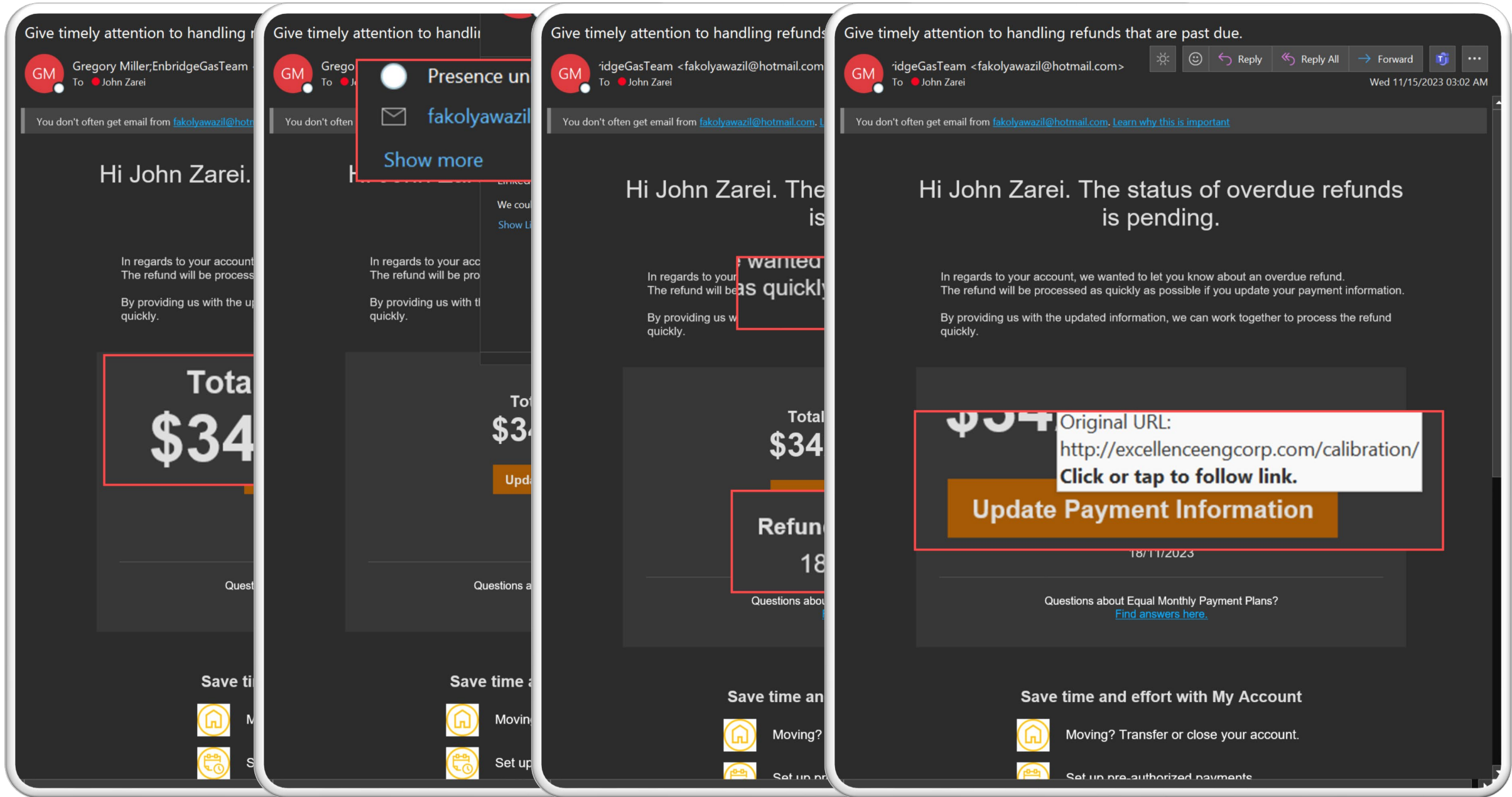
You're Asked to
Send Money

Too Good to be
True

Poor Spelling &
Grammar

Suspicious
Attachments

From
Government
Agency

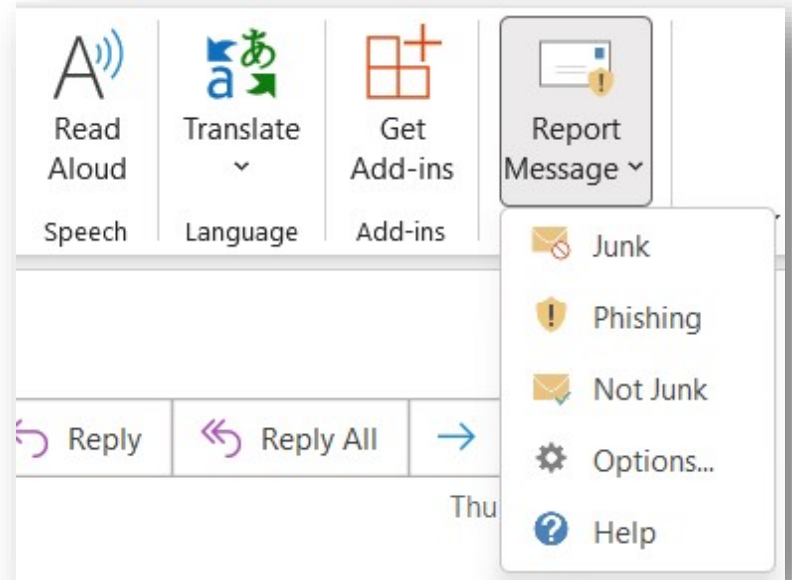


Use the Outlook Report Message

Report suspicious messages to Microsoft as well as manage how your Microsoft 365 email account treats these messages.

Messages that your Microsoft 365 email account marks as junk are automatically moved to your Junk Email folder.

If you choose Junk, Phishing, or Not Junk, you'll have the option to send a copy of the message to Microsoft, along with your classification of the message.



Securing the sign-in process

One of the most important ways to ensure the safety of your online accounts is to keep your sign-in process secure.



Create strong
passwords



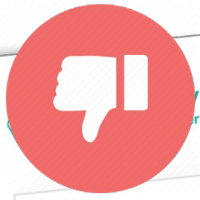
Keep passwords
secure

Create strong passwords

Hackers don't break in; they sign-in. If you use passwords as part of your sign-in process, you'll need to make sure they are as strong as possible.

Strong passwords are:

- At least 12 characters long (but 14 or more is better)
- A combination of uppercase letters, lowercase letters, numbers, and symbols
- Not a word that can be found in a dictionary or the name of a person, character, product, or organization
- Significantly different from your previous passwords
- Easy for you to remember but difficult for others to guess



🇬🇧 EN ▾ FAQ

Mydogisbobby



Time for a password change!

- Your password is easily crackable.
- ⚠️ Frequently used words
- Your password does not appear in any databases of leaked passwords



This password can be cracked faster than the time it takes to get back from a short walk



🇬🇧 EN ▾ FAQ

Mydogisbobbyfromtoronto



Nice password!

- Your password is hack-resistant.
- Your password does not appear in any databases of leaked passwords

Your password will be bruteforced with an average home computer in approximately...

3225 centuries



🇬🇧 EN ▾ FAQ

Mydogisbobbyfromtoronto2023!!



Nice password!

- Your password is hack-resistant.
- Your password does not appear in any databases of leaked passwords

Your password will be bruteforced with an average home computer in approximately...

10000+ centuries



Keep passwords secure

Once you've created strong passwords that hackers can't crack, you must keep them secure. If they can't break your passwords, criminals will try to trick you into revealing them.

To keep your passwords as safe as possible, follow these guidelines:

- ✓ Don't share a password with anyone—not even a friend or family member
- ✓ Never send a password by email, instant message, or any other means of communication that is not reliably secure
- ✓ Never re-use the same password—all your passwords should be unique
- ✓ Always access websites using trusted links
- ✓ Don't hesitate to change passwords immediately on accounts you suspect may have been compromised

Tell-tale signs of a Tech support scam



You get an unexpected call from someone claiming to be tech support (Be aware! Some scammers have tools to generate fake Caller IDs).



You get an error message asking you to call a number urgently.



Your tech support contact asks you to pay them to fix your “problems” with cryptocurrency or gift cards.



Your support technician asks you to download software from an email or third-party website.



Tech support asks you for your password or other private, sensitive data.

Working more securely while travelling

There's a lot of good advice out there about picking a space that's ergonomically comfortable, and where you can minimize distraction, **but there are some security considerations as well.**



Working more securely while travelling



Pick a space that's private. Select a place where people can't "shoulder surf"; look over your shoulder at what's on your screen.



If you're having conference calls or video meetings, be aware of whether other people might be able to eavesdrop, even inadvertently. Even if (sometimes especially if) you're wearing headphones. Other people may still be able to hear your voice when you speak.



Don't allow others to use your work devices. If you have to walk away from your device, lock your device to prevent others from seeing what you're working on. Press Windows logo key + L on a Windows device, to quickly lock your screen.



Only use encrypted Wi-Fi for business. Wi-Fi encrypted with WPA-2 is more secure than Wi-Fi that is open for all to access.



Avoid using free charging stations in airports, hotels or shopping centers. Bad actors have figured out ways to use public USB ports to introduce malware and monitoring software onto devices. Carry your own charger and USB cord and use an electrical outlet instead.

Assessment Offerings

Assessment Offerings



Microsoft 365 Security
Assessment



Microsoft 365 Copilot
Readiness Assessment



Microsoft 365 Tenant
Assessment

Next Steps

Next Steps

 Microsoft 365 Tenant Security Review & Risk Assessment

 User Access Security & Privileged Access Management

 Data Security Audit & Insights

 Multi-platform Device Management Strategy

 Licensing Utilization Optimization

 Cloud Backup Strategy for Data Protection & Recovery

 Staff Cybersecurity Training & Awareness Planning

Resources



[1ty.me - One Time Self Destructing Links For Sharing Sensitive Information](https://1ty.me)



[Norton Password Generator](#)



[CYBER.ORG - Test the Strength of Your Passwords](https://www.cyber.org)



[Have I Been Pwned: Check if your email has been compromised in a data breach](#)

Questions?



Upcoming S4S Webinars

- Third Tuesday of Each Month
- AI @ Work - Every 2nd Friday
- pointalliance.com/events

2025 23 SEP	SOLUTIONS FOR SUCCESS EDUCATION SERIES Seamless Device Management with Microsoft Intune 🕒 11:30 AM - 30 MINUTES Register	2025 26 SEP	AI AT WORK: THE COPILOT SERIES The Future of Work: Powered by Copilot 🕒 11:30 AM - 45 MINUTES Register
2025 10 OCT	AI AT WORK: THE COPILOT SERIES The Future of Work: Powered by Copilot 🕒 11:30 AM - 45 MINUTES Register	2025 21 OCT	SOLUTIONS FOR SUCCESS EDUCATION SERIES Cybersecurity Essentials: Protect Your Business 🕒 11:30 AM - 30 MINUTES Register
2025 24 OCT	AI AT WORK: THE COPILOT SERIES The Future of Work: Powered by Copilot 🕒 11:30 AM - 45 MINUTES Register	2025 07 NOV	AI AT WORK: THE COPILOT SERIES The Future of Work: Powered by Copilot 🕒 11:30 AM - 45 MINUTES Register
2025 18 NOV	SOLUTIONS FOR SUCCESS EDUCATION SERIES Building Modern Apps with Azure, React, NextJS, and Angular 🕒 11:30 AM - 30 MINUTES Register	2025 21 NOV	AI AT WORK: THE COPILOT SERIES The Future of Work: Powered by Copilot 🕒 11:30 AM - 45 MINUTES Register
2025 05 DEC	AI AT WORK: THE COPILOT SERIES The Future of Work: Powered by Copilot 🕒 11:30 AM - 45 MINUTES Register	2025 16 DEC	SOLUTIONS FOR SUCCESS EDUCATION SERIES Building the Future: Migrating Your Infrastructure to Azure 🕒 11:30 AM - 30 MINUTES Register

Leave us a review

