Insights Report

.HTM files &
Microsoft Entra Exploits

New surge identified in phishing threats – bypassing Microsoft 365 and other 3rd party vendors.

Executive Summary

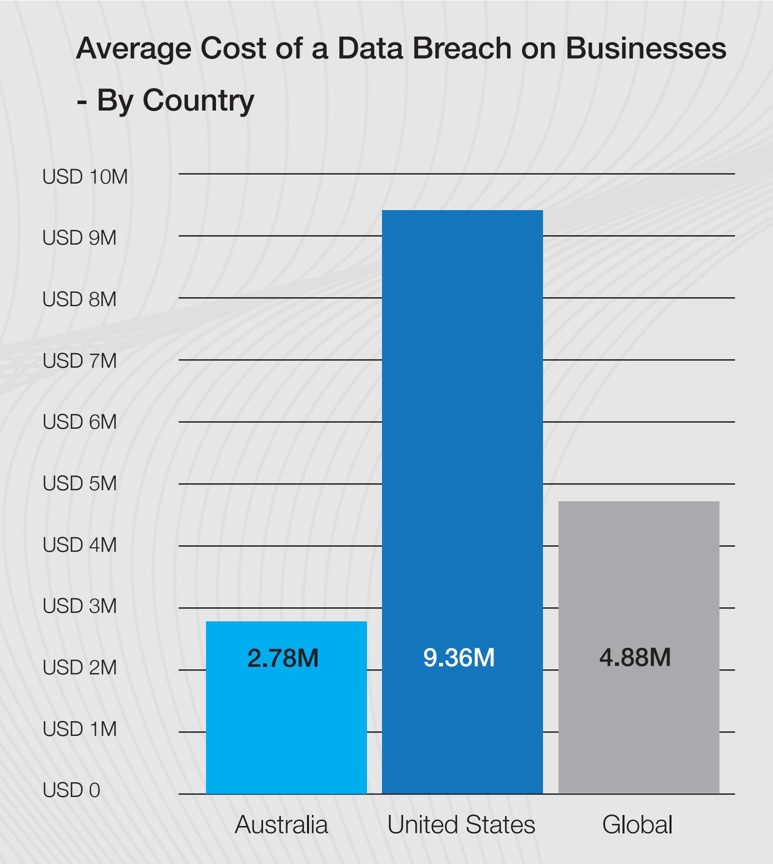
A sharp surge in evasive phishing attacks is actively targeting businesses — exploiting brand trust and urgency to deceive users and bypass standard email defences. These threats are no longer just a cybersecurity issue — **they represent a strategic risk to business continuity, leadership accountability, and reputation.**

MailGuard is intercepting these threats **faster than Microsoft 365 and third-party security vendors**, delivering proactive protection **before emails reach staff inboxes**.

This is a **defining moment for business leaders** to assess whether their current defences are fast and adaptive enough — because attackers are moving faster than ever, and consequences are escalating.

MailGuard doesn't replace Microsoft — it completes it. Acting inline with Defender, it provides a critical layer of protection before threats can reach the business's Microsoft environment.

Many boards assume email security is handled. But **today's threats bypass even advanced setups — and it only takes one click to trigger financial and reputational fallout.**



IBM Cost of a Data Breach Report 2024

Email is the starting point for 91% of cyberattacks.

Source: Microsoft.com

References:
https://www.microsoft.com/en-au/security/business/security-101/what-is-business-email-compromise-bec
https://www.ibm.com/reports/data-breach

Key Threat Insight - .HTM files

Attack Method

Emails appear to be **legitimate renewal notices, payment receipts, or invoice confirmations** — often impersonating Microsoft or other major brands.

They include a **.htm file attachment**, disguised as a trusted document.

Once clicked, users are taken to a **fake browser-based login** page designed to harvest credentials or initiate silent malware installation.

Why It's So Effective

- Tactics use familiar **branding and urgency triggers** to encourage users to act quickly.
- Attackers frequently alter **design, language, and sender tactics** to bypass filters and avoid detection.
- Even organisations with multi-layered security are vulnerable if their **detection speed** is too slow.

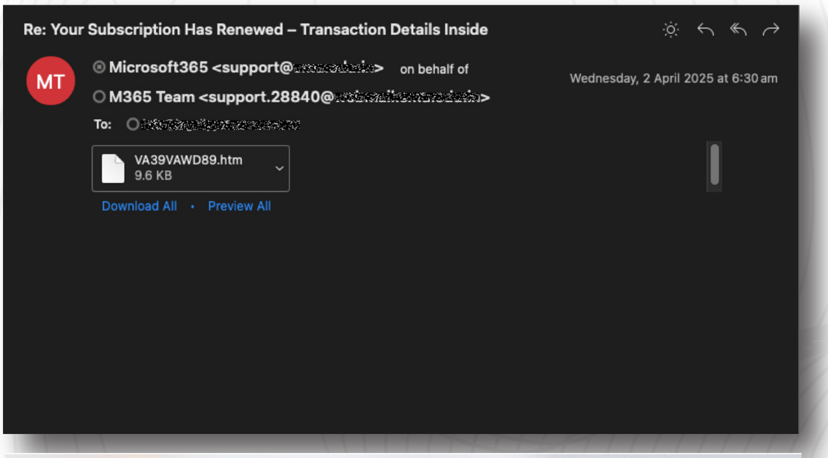
"Adversaries are leveraging advanced obfuscation techniques in client-side JavaScript to enable polymorphic and fileless payload deployment, including but not limited to ransomware and remote access trojans (RATs).

By dynamically reconstructing malicious code at runtime and embedding phishing assets within local file structures (e.g., MHTML or SVG containers), attackers bypass static and signature-based detection mechanisms.

These tactics reduce dependency on external C2 infrastructure, instead exploiting in-browser execution contexts (e.g., via DOM-based injection, sandbox evasion, or JavaScript-based content spoofing) to deliver malicious functionality while maintaining operational stealth."

— Anwar Ibrahim, CTO, MailGuard

.HTM Email Attacks Example 1



Re: Your Subscription Has Renewed – Transaction Details Inside

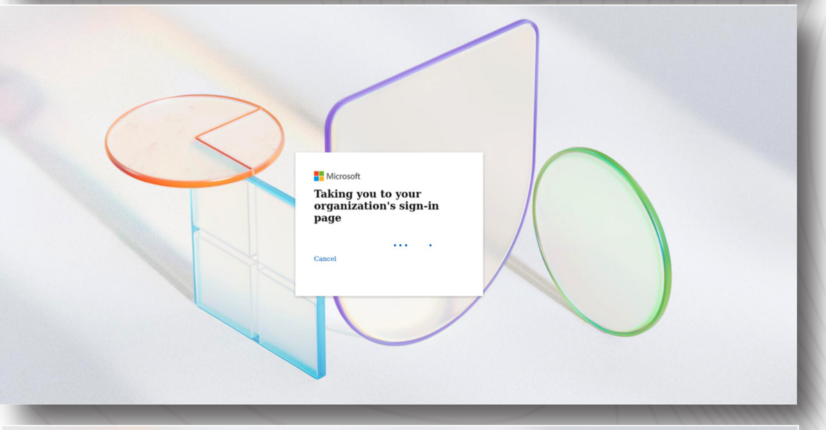
Microsoft365 <support@[redacted]> on behalf of

M365 Team <support.28840@[redacted]>

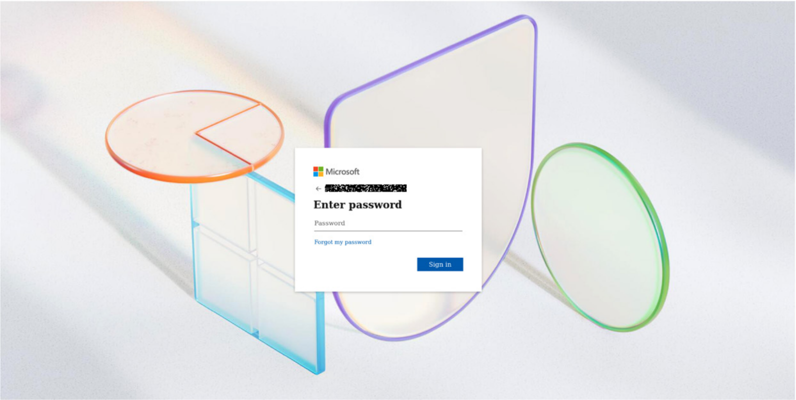
To: [redacted]

Wednesday, 2 April 2025 at 6:30 am

VA39VAWD89.htm
9.6 KB



Taking you to your organization's sign-in page



← [redacted]

Enter password

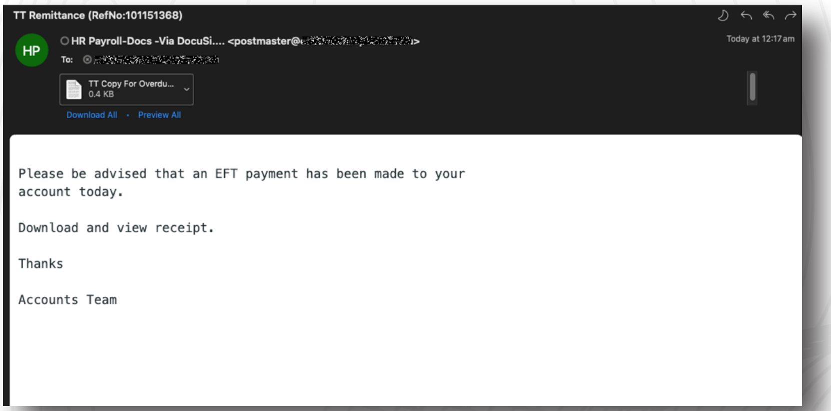
Password

In this first example, a seemingly innocuous email claims that **your subscription has expired**.

The **sender name is crafted to spoof Microsoft 365 Support**, inspiring confidence that it is a legitimate email from a trusted sender.

Clicking the attachment launches a phishing sequence which replicates the Microsoft sign-in process, in an attempt **to steal the user's Microsoft credentials**.

.HTM Email Attacks Example 2



TT Remittance (RefNo:101151368)

HR Payroll-Docs -Via DocuSi.... <postmaster@[redacted]>

To: [redacted]

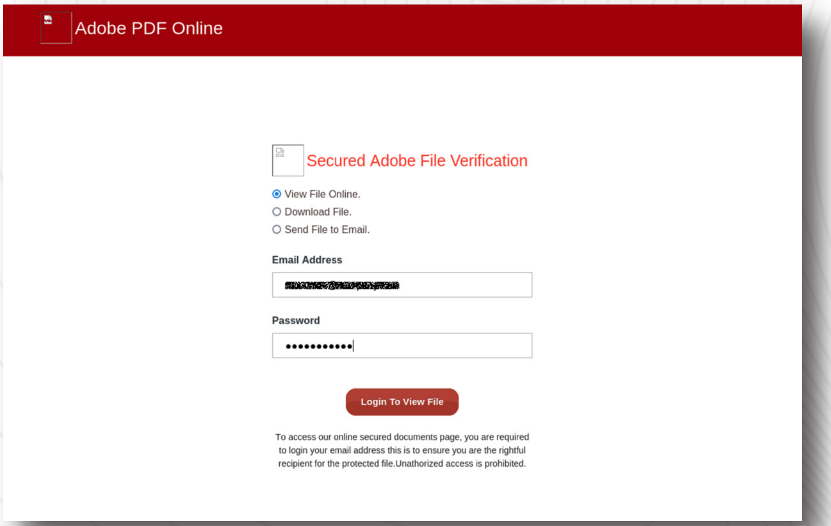
Today at 12:17 am

```
Please be advised that an EFT payment has been made to your
account today.

Download and view receipt.

Thanks

Accounts Team
```



Secured Adobe File Verification

● View File Online.
○ Download File.
○ Send File to Email.

Email Address: [redacted]

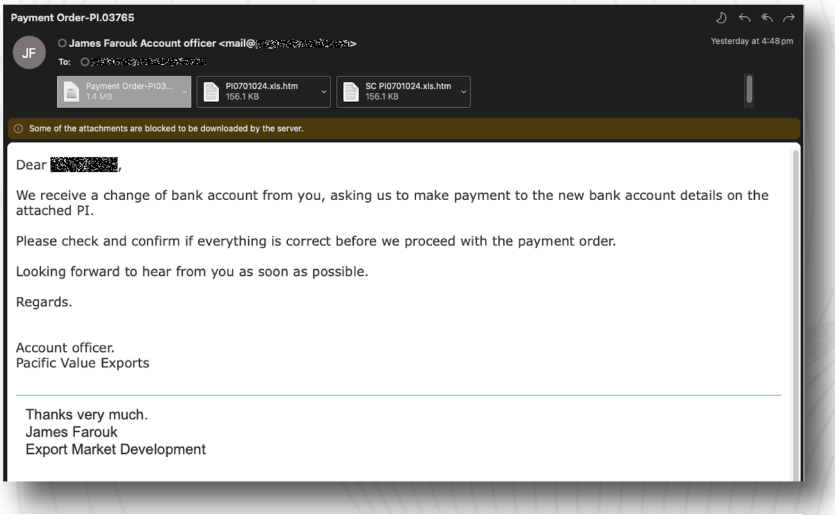
Password: ••••••••••••

To access our online secured documents page, you are required to login your email address this is to ensure you are the rightful recipient for the protected file.Unathorized access is prohibited.

This example from ‘**HR Payroll’ advises recipients that an EFT payment has been made to their account**, with a call to action to ‘**Download and view receipt**’.

The scam launches an Adobe PDF page which asks victims for their **email address (username) and password,** before they can view or download the file.

.HTM Email Attacks Example 3



Payment Order-PI.03765

JF James Farouk Account officer <mail@[redacted]>

To: [redacted]

Yesterday at 4:48 pm

Some of the attachments are blocked to be downloaded by the server.

Dear [redacted],

We receive a change of bank account from you, asking us to make payment to the new bank account details on the attached PI.

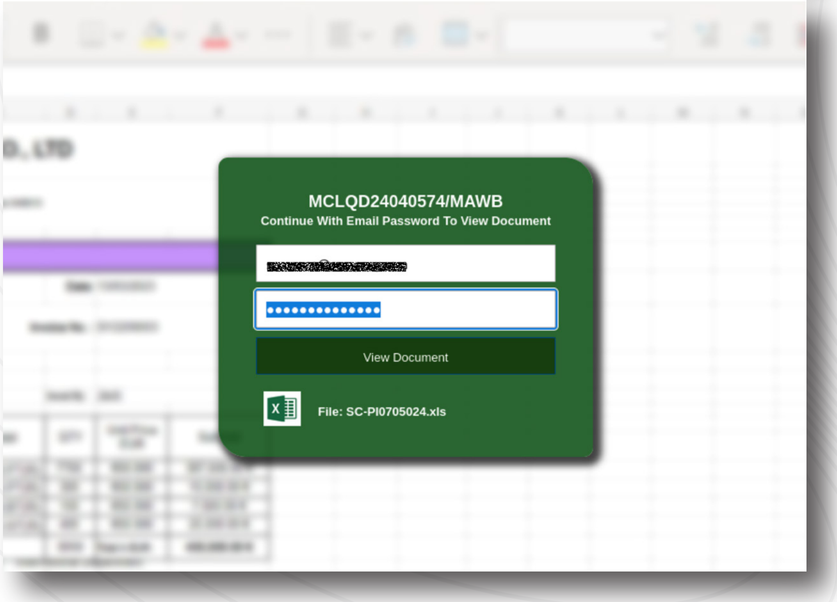
Please check and confirm if everything is correct before we proceed with the payment order.

Looking forward to hear from you as soon as possible.

Regards.

Account officer.
Pacific Value Exports

Thanks very much.
James Farouk
Export Market Development



MCLQD24040574/MAWB

Continue With Email Password To View Document

[redacted]

••••••••••••••

File: SC-PI0705024.xls

This third example **impersonates an Account Officer from an export business**, asking the recipient to **confirm their bank account details** before a payment can be processed.

In so doing, **the victim is required to provide their username and password** in order to view the document.

Key Threat Insight - Entra Exploit

Attack Method

Cybercriminals are spinning up **rogue Microsoft 365 tenants and abusing Microsoft's Entra B2B collaboration system to send guest invitations** that appear completely legitimate.

The emails carry the added urgency of a PayPal refund notice to prompt recipients into action.

While the emails are delivered from trusted Microsoft domains and IPs, the intent behind them is anything but.

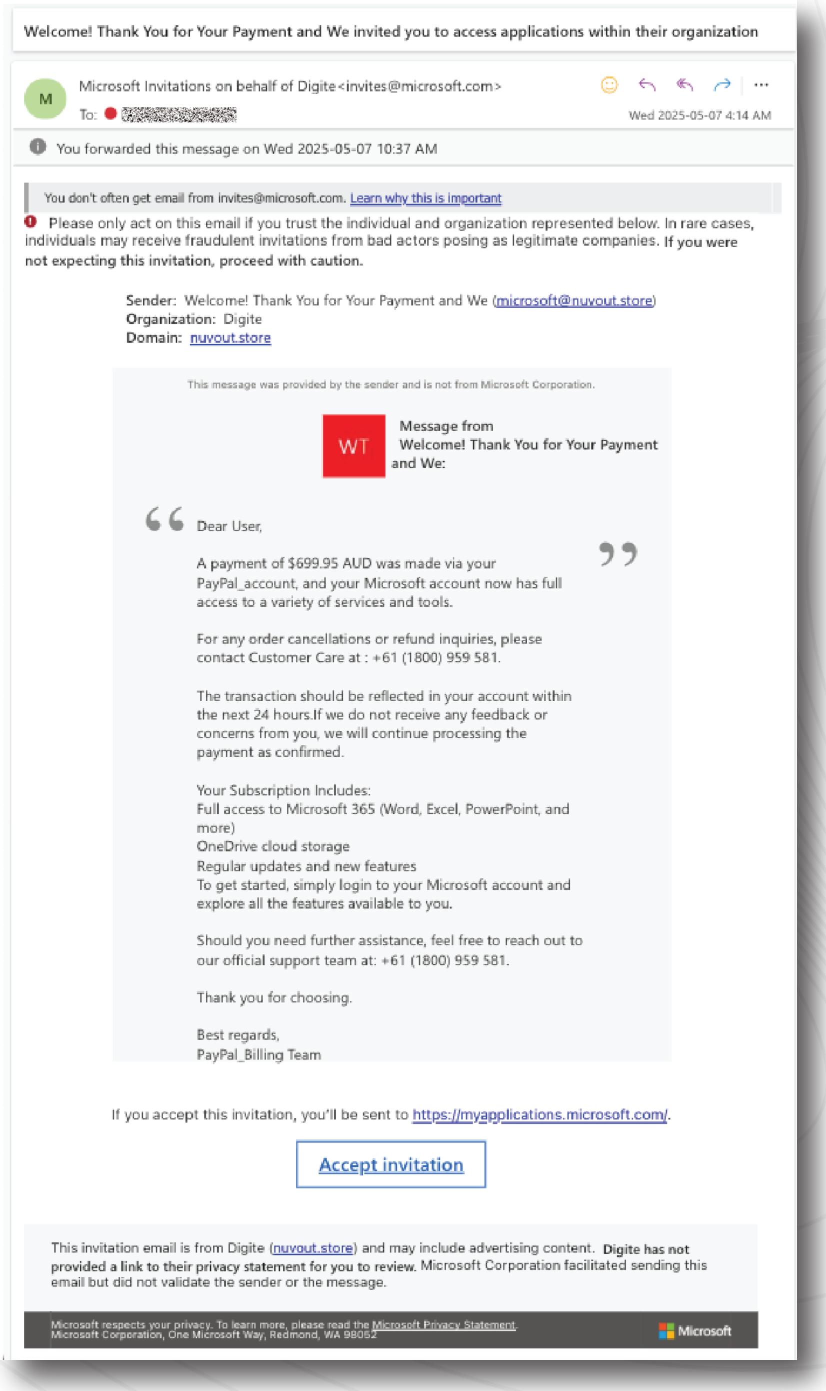
Why It's So Effective

- The emails are sent from Microsoft's own **invites@microsoft.com** address
- Allowing them to pass **SPF, DKIM and DMARC tests**
- They are **hosted on Microsoft infrastructure**, and
- Include links to **legitimate Microsoft services**, like **myapplications.microsoft.com**

Leadership questions worth asking:

- *How many **phishing attempts** were reported last quarter?*
- *What's our current **time-to-detect** on credential phishing?*
- *Who's responsible for what get's past **Microsoft Defender**?*

Microsoft Entra Exploitation Example 1



Welcome! Thank You for Your Payment and We invited you to access applications within their organization

Microsoft Invitations on behalf of Digite<invites@microsoft.com>

To: [redacted]

Wed 2025-05-07 4:14 AM

You forwarded this message on Wed 2025-05-07 10:37 AM

You don't often get email from invites@microsoft.com. Learn why this is important

Please only act on this email if you trust the individual and organization represented below. In rare cases, individuals may receive fraudulent invitations from bad actors posing as legitimate companies. **If you were not expecting this invitation, proceed with caution.**

Sender: Welcome! Thank You for Your Payment and We (microsoft@nuvout.store)
Organization: Digite
Domain: nuvout.store

This message was provided by the sender and is not from Microsoft Corporation.

Message from
Welcome! Thank You for Your Payment
and We:

Dear User,

A payment of $699.95 AUD was made via your PayPal_account, and your Microsoft account now has full access to a variety of services and tools.

For any order cancellations or refund inquiries, please contact Customer Care at : +61 (1800) 959 581.

The transaction should be reflected in your account within the next 24 hours.If we do not receive any feedback or concerns from you, we will continue processing the payment as confirmed.

Your Subscription Includes:
Full access to Microsoft 365 (Word, Excel, PowerPoint, and more)
OneDrive cloud storage
Regular updates and new features
To get started, simply login to your Microsoft account and explore all the features available to you.

Should you need further assistance, feel free to reach out to our official support team at: +61 (1800) 959 581.

Thank you for choosing.

Best regards,
PayPal_Billing Team

If you accept this invitation, you'll be sent to https://myapplications.microsoft.com/.

This invitation email is from Digite (nuvout.store) and may include advertising content. **Digite has not provided a link to their privacy statement for you to review.** Microsoft Corporation facilitated sending this email but did not validate the sender or the message.

Microsoft respects your privacy. To learn more, please read the Microsoft Privacy Statement.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

This example originates from **invites@microsoft.com** and includes templated text claiming to **confirm a Microsoft 365 subscription renewal**.

The real call to action however is a phone number offering a refund, where the cybercriminals conduct a vishing (voice phishing) attack.

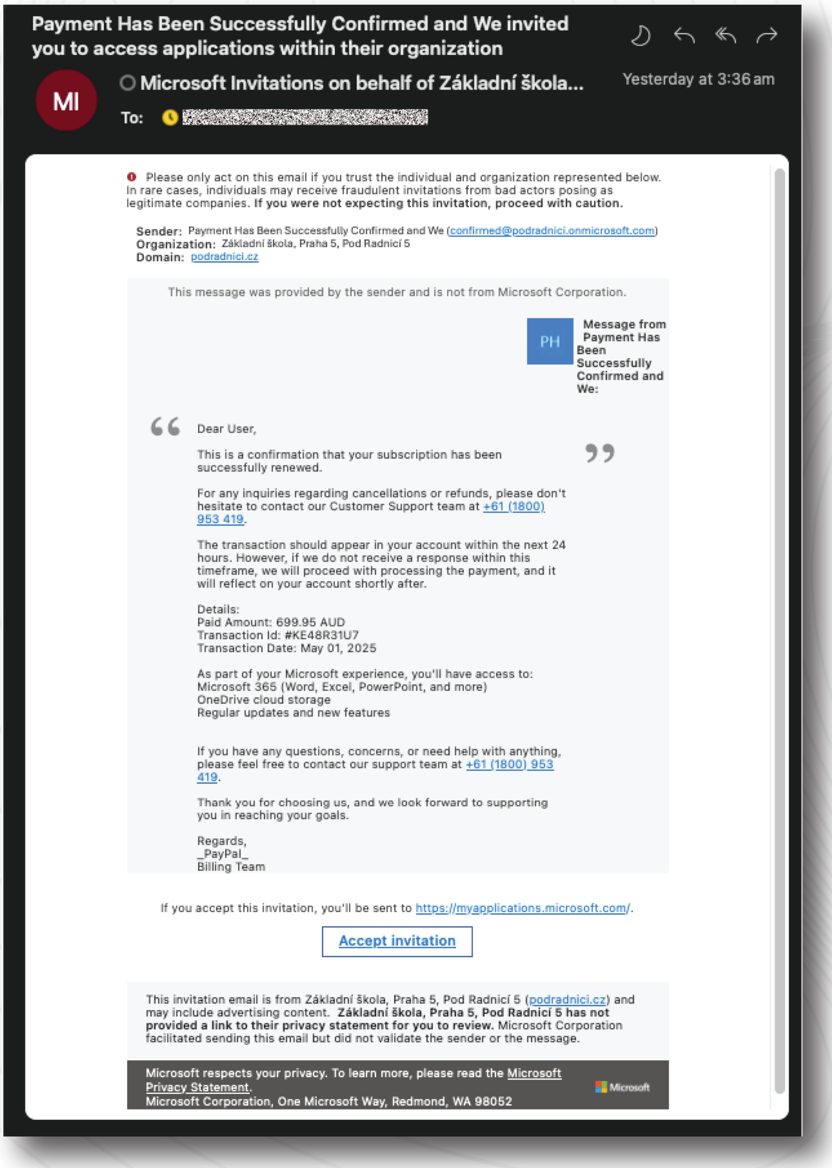
Victims are met with a fake PayPal support line where attackers harvest:

- **Login credentials,**
- **Multi-factor authentication codes, and**
- **Personal or financial information.**

If the recipient accepts the Microsoft guest invitation, they become part of the attacker's rogue tenant. From there, attackers can:

- **Auto-register malicious applications**
- **Harvest OAuth tokens, and**
- **Access or exfiltrate data via legitimate collaboration paths**

Microsoft Entra Exploitation Example 2



Payment Has Been Successfully Confirmed and We invited you to access applications within their organization

○ **Microsoft Invitations on behalf of Základní škola...** Yesterday at 3:36 am

MI

To: [redacted]

Please only act on this email if you trust the individual and organization represented below. In rare cases, individuals may receive fraudulent invitations from bad actors posing as legitimate companies. **If you were not expecting this invitation, proceed with caution.**

Sender: Payment Has Been Successfully Confirmed and We (confirmed@podradnici.onmicrosoft.com)
Organization: Základní škola, Praha 5, Pod Radnicí 5
Domain: podradnici.cz

This message was provided by the sender and is not from Microsoft Corporation.

PH **Message from Payment Has Been Successfully Confirmed and We:**

“ Dear User,

This is a confirmation that your subscription has been successfully renewed. ”

For any inquiries regarding cancellations or refunds, please don't hesitate to contact our Customer Support team at +61 (1800) 953 419.

The transaction should appear in your account within the next 24 hours. However, if we do not receive a response within this timeframe, we will proceed with processing the payment, and it will reflect on your account shortly after.

Details:
Paid Amount: 699.95 AUD
Transaction Id: #KE48R31U7
Transaction Date: May 01, 2025

As part of your Microsoft experience, you'll have access to:
Microsoft 365 (Word, Excel, PowerPoint, and more)
OneDrive cloud storage
Regular updates and new features

If you have any questions, concerns, or need help with anything, please feel free to contact our support team at +61 (1800) 953 419.

Thank you for choosing us, and we look forward to supporting you in reaching your goals.

Regards,
PayPal
Billing Team

If you accept this invitation, you'll be sent to https://myapplications.microsoft.com/.

This invitation email is from Základní škola, Praha 5, Pod Radnicí 5 (podradnici.cz) and may include advertising content. **Základní škola, Praha 5, Pod Radnicí 5 has not provided a link to their privacy statement for you to review.** Microsoft Corporation facilitated sending this email but did not validate the sender or the message.

Microsoft respects your privacy. To learn more, please read the Microsoft Privacy Statement.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

This second email example is a variation on the same Microsoft Entra scam exploiting Microsoft infrastructure to avoid detection.

In this example the scam is using the **same tactic**, but uses a **different tenant** and **callback number**.

Consequences of Inaction

If even one of these attacks slips through, organisations face:

- **Account Takeover** – Unauthorised access to Office 365 and sensitive internal systems.
- **Malware & Ransomware Infiltration** – Disruption of operations and costly recovery.
- **Financial Loss & Reputational Harm** – Breach exposure, client distrust, and legal implications.

The average cost of an email-based breach exceeds $4.88 million, not including the long-tail impact on customer confidence.

"The successful execution of advanced phishing campaigns poses significant threats to an organization's information security management system (ISMS), impacting the confidentiality, integrity, and availability of information assets.

Such attacks often result in unauthorized credential harvesting, enabling lateral movement across Microsoft 365 tenants, and exfiltration of sensitive corporate data via compromised services like SharePoint, OneDrive, and Exchange. A pertinent example is the phishing scam intercepted by MailGuard, where attackers impersonated the CEO of FlySafair and utilized a fake Microsoft OneDrive login page to harvest corporate email credentials. This occurrence underscores the necessity for robust access control measures (ISO 27001), effective asset management, and stringent operations security protocols.

Furthermore, the deployment of such sophisticated phishing techniques can lead to reputational damage, emphasizing the importance of compliance and comprehensive information security incident management."

— Prathik Chandrashekar, Head of Engineering, MailGuard

Why MailGuard Is Critical

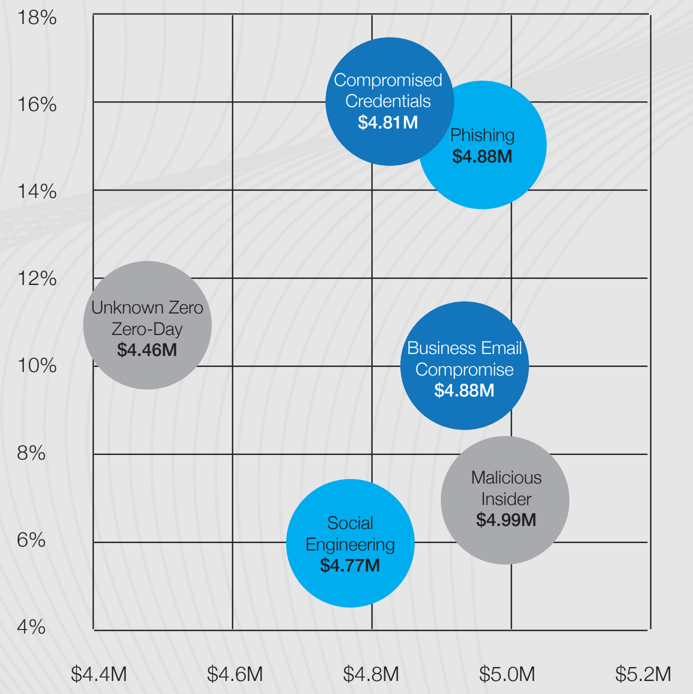
All examples of .HTM attack types and Microsoft Entra exploitation were **100% intercepted by MailGuard before reaching users**. Threats that in some instances had bypassed Microsoft Defender, Proofpoint, and other well-known security stacks based on Microsoft metadata analysis.

MailGuard delivers:

- **Inline detection before mailbox delivery.** This is where breaches are stopped — not after damage is done, but before users ever see the threat.
- **7-month lead time on emerging phishing patterns** such as QR code attacks
- **Seamless integration** and deployment inline with Microsoft 365 and Google, blocking threats before they reach users.

This is **precision cyber defence at speed**, engineered to intercept threats before human error comes into play.

Cost and Frequency of Initial Attack Vectors that are Email-Related



IBM Cost of a Data Breach Report 2024

292 Days

to identify and contain breaches involving stolen credentials.

References:
https://www.ibm.com/reports/data-breach

Email Persists as the Number One Vector for Cyberattacks

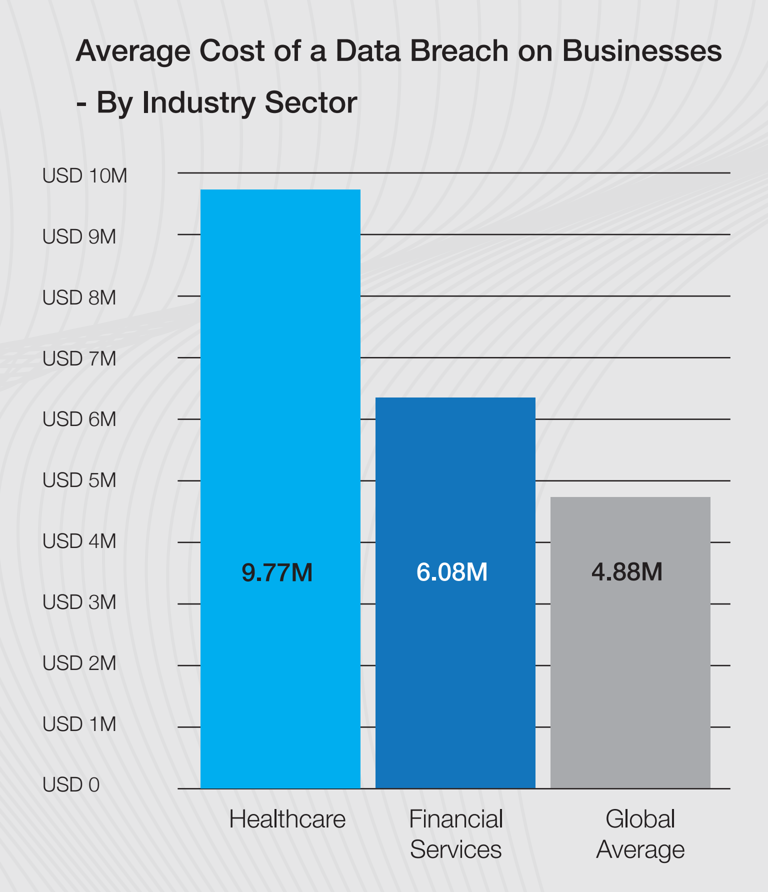
According to Cyber.gov.au, **91% of cyberattacks start with phishing emails.**

The **top 3 self-reported cybercrime types for business** are:

- **Email compromise (20%)**
- Online banking fraud (13%)
- **Business email compromise (13%)**

Ransomware incidents account for ~11% of all reported incidents, and more recently, malicious cyber actors have adjusted their tactics to include stealing sensitive data. In addition, **12% of ransomware victims were also extorted for payment to prevent their data being leaked or sold online.**

66% of security leaders identified AI as a key contributor to cybersecurity threats, and **48% cited advanced phishing and social engineering scams.**



IBM Cost of a Data Breach Report 2024

References:
https://www.aic.gov.au/publications/sr/sr43
ttps://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024
https://www.microsoft.com/en-au/security/business/security-101/what-is-business-email-compromise-bec
https://datacom.com/au/en/solutions/security/security-insights/cybersecurity-index-2025
https://www.ibm.com/reports/data-breach

A Strategic Call To Action

These are not isolated campaigns — they reveal **consistent gaps that even strong defences like Microsoft 365 can't always catch alone**.

Cybercriminals are winning on **speed and innovation**, requiring board-level leaders to respond with equal urgency.

Modern leadership demands action from us before damage is done, meaning **protection is no longer optional — it's a strategic imperative.**

You don't need a rip-and-replace. You just need to close the final gap — before the next inbox breach makes the news.

Let's **schedule a time** to review your organisation's security posture — and assess how **MailGuard can complement your defences**, strengthening control, boosting resilience and tackling new strategic challenges**, to stay ahead of evolving threats**.

"I couldn't speak more highly of MailGuard as a reliable service provider."

— IT Manager, Porsche

"The entire implementation process was very simple and easy to manage"

— Help Desk Specialist, Lincraft

"We've seen email-based attacks surge. MailGuard and Defender 365 together have helped us stay protected."

— CISO, Silk Logistics

Built in Australia. Trusted Globally.

MailGuard is a global leader in email threat detection. A pioneer in cloud email security since 2001, MailGuard invented the concept of pre-filtering email threats before inbox delivery, laying the foundation for the Secure Email Gateway (SEG) category.

Today, MailGuard protects organisations globally with AI-powered threat detection, seamlessly deployed inline with Microsoft's ecosystem and Google, among other email providers.

At the heart of our platform is **MyGuard** — our proprietary AI threat engine developed with over **A$35 million in R&D**. MyGuard combines:

- Gen-AI powered LLMs
- Bayesian and fingerprint-based classifiers
- Real-time behavioural heuristics

…to stop advanced threats on first encounter before they reach staff inboxes — including those that bypass Microsoft and other cloud email security vendors

MailGuard is **ISO/IEC 27001:2022 certified**, trusted by **over 5,500 organisations**, including governments, law firms, banks, hospitals, and ASX-listed companies. Recognised for our unmatched speed in detecting zero-day email threats, we have consistently stopped sophisticated exploits, like **QR code phishing, Dropbox-based malware**, and **Azure AD Guest Invite fraud**, months ahead of Microsoft, and other leading platforms.

In an era of rising cyber regulation and board-level accountability, MailGuard enhances your Microsoft 365 or Google security stack with minmal disruption, easy activation, and elite-speed protection, fulfilling your fiduciary and operational responsibilities.

Trusted by Global Leaders. Since 2001.

- A **leader in advanced 'zero zero-day' email threats** missed by Microsoft 365 and other 3rd party vendors.
- Achieve peace of mind with MailGuard, a solution **trusted by global leaders** that ensures your email is secure.
- Benefit from **A$35M+ in R&D, including proprietary AI & ML-powered threat detection**, to boost your cybersecurity confidence.
- AI-powered email threat detection and inline architecture intercepts and blocks threats hours faster, on first encounter.

"It's the type of innovation that we want to see."

— Satya Nadella, CEO & Chairman, Microsoft

"MailGuard has developed world-leading cloud and email security IP. This is IP that is unique to Australia; it's among the leading cloud and email security solutions anywhere in the world."

— Hon. Malcolm Turnbull, Former Australian Prime Minister

"You are being led by what I see as one of the world's best, at preventing and protecting your secure infrastructure, securing your people, and securing your business"

— Steve Miller, COO, Microsoft Asia

www.mailguard.com.au

Let's Connect

Make time today to talk to our local team of experts about fortifying your inboxes.
expert@mailguard.com.au