Insights Report

QR Code Phishing

The next frontier of evasion: QR code phishing threats, bypassing Microsoft 365 and other 3rd party vendors.

mailguard
A GlobalGuard Company

Executive Summary

QR code phishing, or "quishing", is rapidly emerging as a preferred tactic for sophisticated attackers seeking to bypass text- and link-based email defences.

By **embedding malicious URLs inside seemingly innocuous QR images**, adversaries are redirecting users to credential-harvesting portals or malware delivery sites without triggering traditional filters.

MailGuard's proprietary defence IP and OCR-driven image analysis are blocking these threats months ahead of Microsoft Defender and other third-party vendors, ensuring organisations remain one step ahead of this fast-evolving vector.

In Australia, one cyber attack is reported **every six minutes.**

Source: Cyber.gov.au

References:
https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024#:~:text=Year%20in%20review%20*%20email%20compromise%20(20%),(13%)%20*%20business%20email%20compromise%20fraud%20(13%)

Key Threat Insight - QR Codes

Attack Method

- Emails masquerade as MFA notifications, invoice confirmations or account alerts, featuring an **inline QR code or a QR image in a PDF/Microsoft Office document** attachment.
- When scanned, typically via a mobile device, the **QR resolves to a fake login page or malware-drop server**.
- Advanced campaigns embed CAPTCHA-style checks and JavaScript routines to **capture multi-factor tokens or session cookies**, enabling full account takeover.

> *"By concealing phishing URLs within QR images and leveraging mobile device behaviours, adversaries can harvest credentials and session tokens, straight from mobile endpoints, completely under the radar of static, signature-based defences."*
>
> **— Anwar Ibrahim, CTO, MailGuard**

Why It's So Effective

- Filter Evasion: **QR payloads hidden in images sidestep URL-scanning** engines and link-parsing rules.
- Mobile-First Targeting: On smaller screens, **users rarely preview URLs before scanning**, and device settings often **auto-open QR links**.
- Dynamic Obfuscation: Attackers **rotate landing-page templates and domain infrastructure**, reducing the lifespan of blacklists and reputation rules.

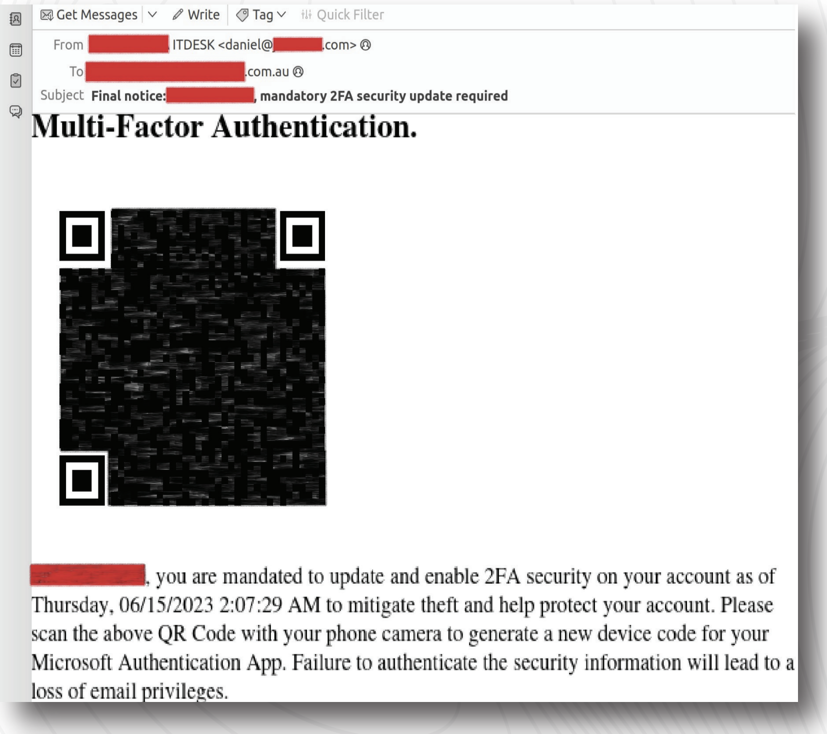
Technical Deep Dive

- **Data Encoding Layers:** Attackers embed a short redirect URL (e.g. bit.ly or custom domains) which then chains to the final phishing or malware URL, minimizing the visible payload size and evading simple signature checks.
- **Dynamic Code Generation:** Payload URLs are often generated on the fly, with unique tokens per recipient to foil blacklist-based defences and enable per-target tracking.
- **Steganographic Obfuscation:** Some campaigns overlay benign logos or incorporate the QR within benign imagery, requiring advanced image-processing (beyond basic OCR) to isolate and decode the actual code.

Evolution of Tactics

Phase	Characteristics	Notable Shifts
2020-2021: Emergence	Simple, static QR codes embedded in email signatures or PDFs	Low-volume tests: easily blacklisted domains
2022: Professionalization	Branded codes with corporate logos: multi-step re-direct chains	Use of URL shorteners; greater scan conversion
2023 - Present: Stealth & Polymorphism	CAPTCHA gates, dynamic pre-recipient URLs, steganographic overlays	On-the-fly code rendering; JavaScript token grabs

QR Code Phishing Example



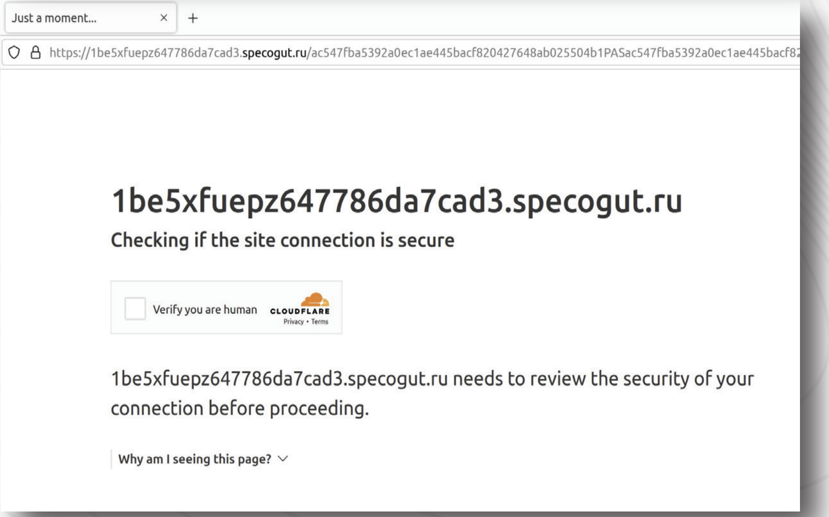
From [redacted] ITDESK <daniel@[redacted].com>

To [redacted].com.au

Subject **Final notice:[redacted], mandatory 2FA security update required**

Multi-Factor Authentication.

[redacted], you are mandated to update and enable 2FA security on your account as of Thursday, 06/15/2023 2:07:29 AM to mitigate theft and help protect your account. Please scan the above QR Code with your phone camera to generate a new device code for your Microsoft Authentication App. Failure to authenticate the security information will lead to a loss of email privileges.


Just a moment...
https://1be5xfuepz647786da7cad3.specogut.ru/ac547fba5392a0ec1ae445bacf820427648ab025504b1PASac547fba5392a0ec1ae445bacf82
Verify you are human
CLOUDFLARE
Privacy • Terms
Why am I seeing this page?

1be5xfuepz647786da7cad3.specogut.ru

Checking if the site connection is secure

1be5xfuepz647786da7cad3.specogut.ru needs to review the security of your connection before proceeding.

Attackers attempt to bypass email filters by **embedding an image of a custom QR code in an email, rather than a link** to a phishing page.

When scanned by a mobile phone camera, the **QR code image will open the phishing page** instead.

This example is masquerading as a security notification that a ‘mandatory 2FA security update’ is requred.

Upon arrival **at the phshing page, users are presented with a number of CAPTCHA prompts** which mandate that the web client is an actual browser (or can simulate a browser) and is actively executing JavaScript.

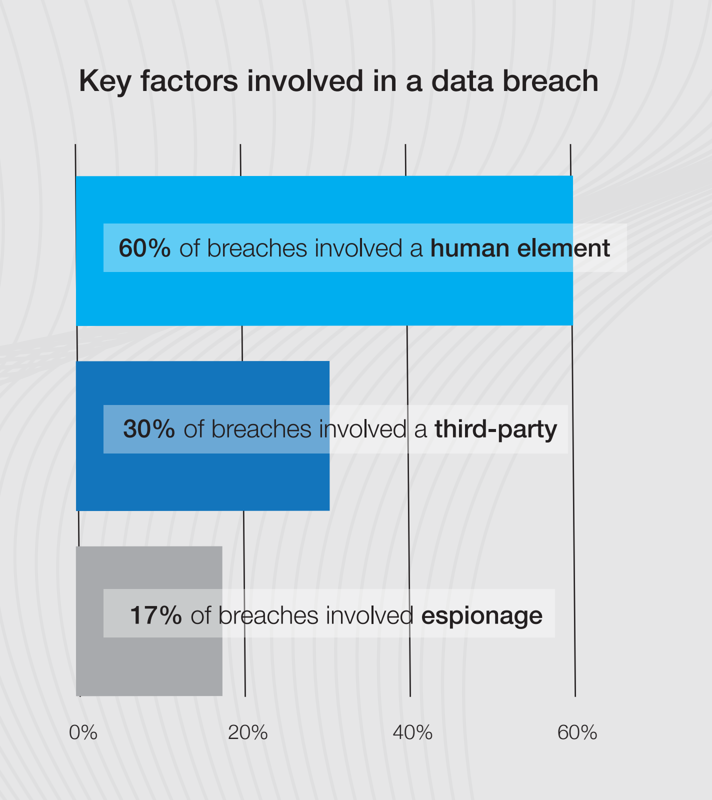
This example is attempting to harvest the user’s Microsoft credentials.

Consequences of Inaction

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

- **Account Takeover** – Unauthorised access to Microsoft 365 VPN portals and other critical systems.
- **Malware & Ransomware Deployment** – Silent installations that can propogate laterally and encrypt data.
- **Financial Loss & Reputational Harm** – Breach response costs, regulatory fines and erosion of customer trust.

The average **cost of an email-based breach exceeds USD 4.88 million**, not including the long-tail impact on brand and customer loyalty.



2025 Verizon Data Breach Investigations Report

References:
https://www.verizon.com/business/resources/Tdc6/reports/2025-dbir-data-breach-investigations-report.pdf
https://www.ibm.com/reports/data-breach

Why MailGuard Is Critical

MailGuard delivers:

- MailGuard's proprietary defence IP and OCR-driven image analysis **detects and decodes QR payloads in email bodies and attachments**.
- 7-Month Lead Time: **Early identification of emerging quishing patterns**, including new encoding and delivery methods.
- **Seamless integration** and deployment inline with Microsoft 365 and Google, blocking threats before they reach users.

All quishing attempts were **intercepted by MailGuard, months before** they appeared to be stopped on Microsoft Defender or other leading platforms.

> *"Quishing represents a paradigm shift in phishing, blurring the line between physical and digital attack surfaces.*
>
> *Without robust image-analysis and real-time detonation, organisations leave their most critical assets exposed."*
>
> **— Prathik Chandrashekar, Head of Engineering, MailGuard**

Email Persists as the Number One Vector for Cyberattacks

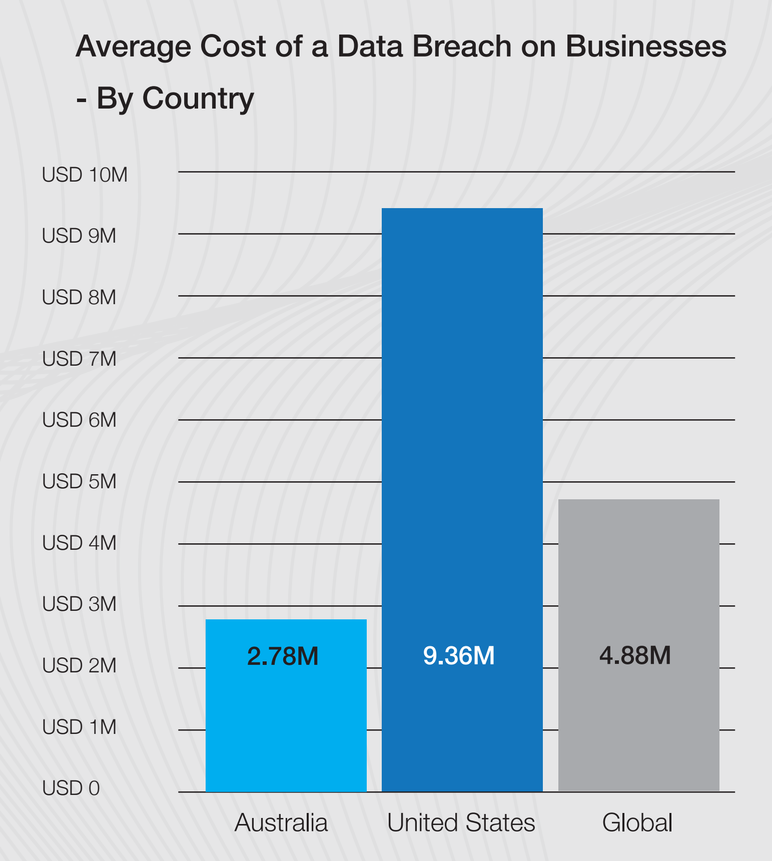
According to Cyber.gov.au, **91% of cyberattacks start with phishing emails.**

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

Quishing is not an isolated anomaly, it’s evidence that **static defences are being outpaced**.

Cybercriminals are innovating at machine speed; **board-level leaders must respond** with equal agility.

Modern security demands proactive, image-aware protection before human error can be exploited.

Let’s **schedule a time** to review your organisation’s security posture — and assess how **MailGuard can deliver precision defence against the rising tide of QR code phishing**.

"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

mailguard
A GlobalGuard Company