CARISMA SOLUTIONS

An Xcelerate Venture

Partner of choice for Financial Solutions
Across Australia since 2006

Phishing Attack Incident – Lessons for a Safer Workplace

This presentation explores a recent phishing attack within an organization and extracts vital lessons to enhance workplace cybersecurity awareness.

We will uncover the incident's timeline, identify key vulnerabilities, and outline actionable prevention strategies to strengthen our defenses against similar threats.



Carisma Solutions confidential



Background & Company Overview

Company Profile

Over 250 staff provide accounting, superannuation, and administrative services primarily for Australian clients, relying heavily on digital communication.

Communication Reliance

Email is a primary channel, including group IDs like all-staff for disseminating important alerts and notices.

Security Incident

A recent phishing email triggered a cyberattack after being mishandled internally, exposing gaps in awareness and protocols.

Incident Summary

1

Phishing Email Received

A director received a disguised phishing email designed to appear legitimate.

2

Email Forwarded

The director forwarded it to all staff with a cautionary note about its illegitimacy.

3

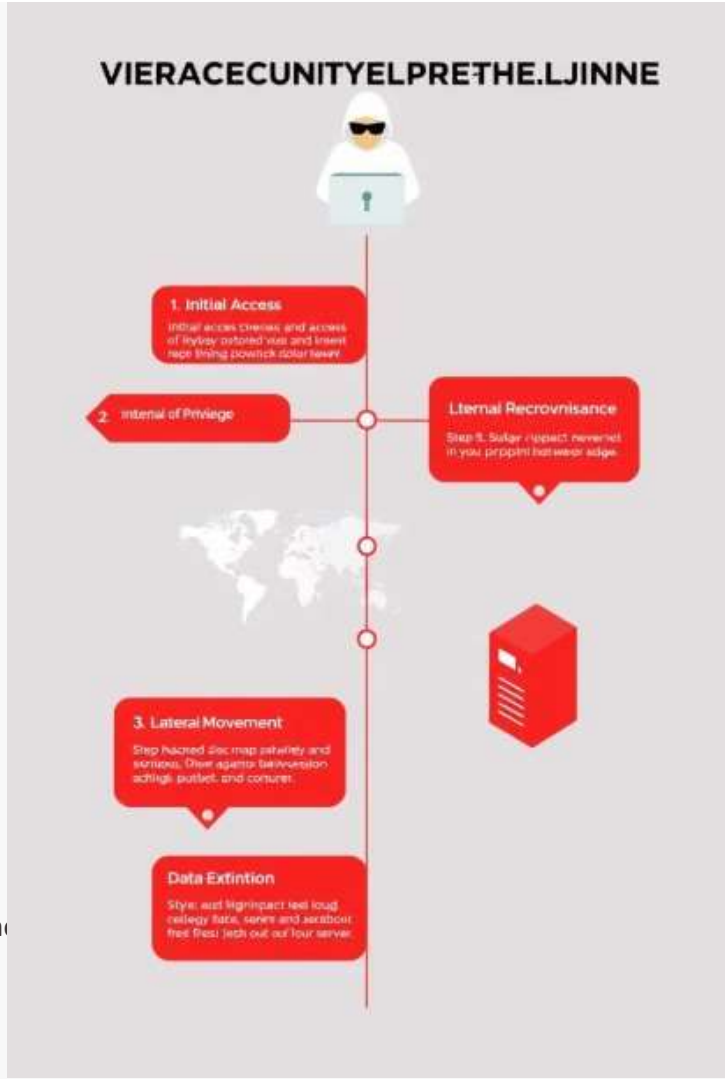
Misinterpretation Occurred

A staff member misunderstood the warning and clicked the malicious link.

4

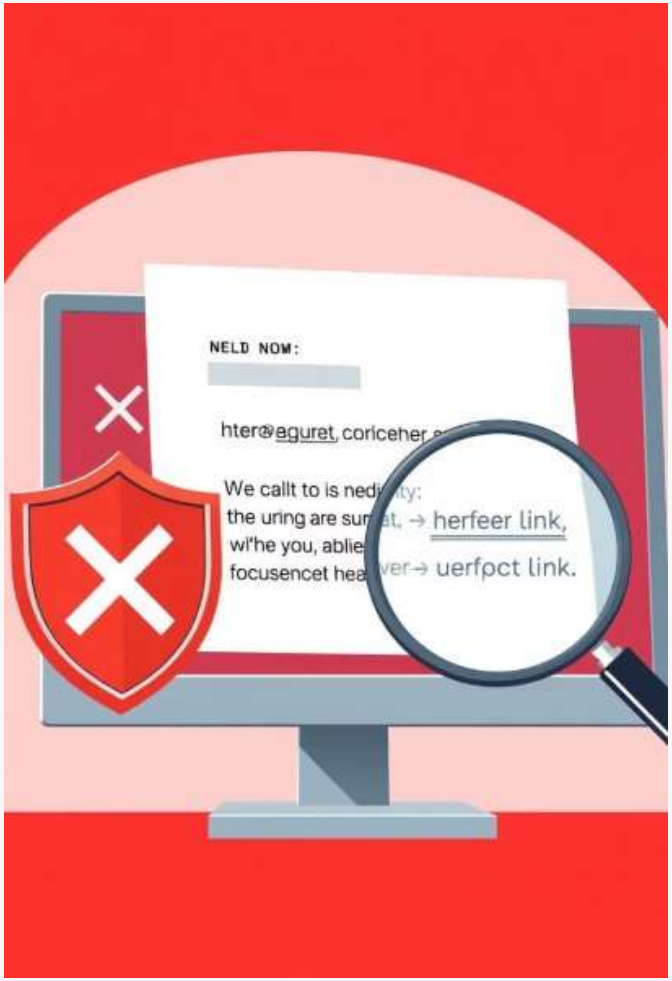
Cyberattack Triggered

The click enabled a cyberattack causing operational risks and potential data breach



Chain of Events – What Went Wrong?

1. Phishing email mimicked routine internal communication with formal language but had subtle anomalies in sender details.
2. The director's cautionary message contained jargon that confused some staff, diluting the warning's impact.
3. A key staff member did not immediately report clicking the link, delaying response efforts.



Anatomy of a Phishing Email

Subject Line

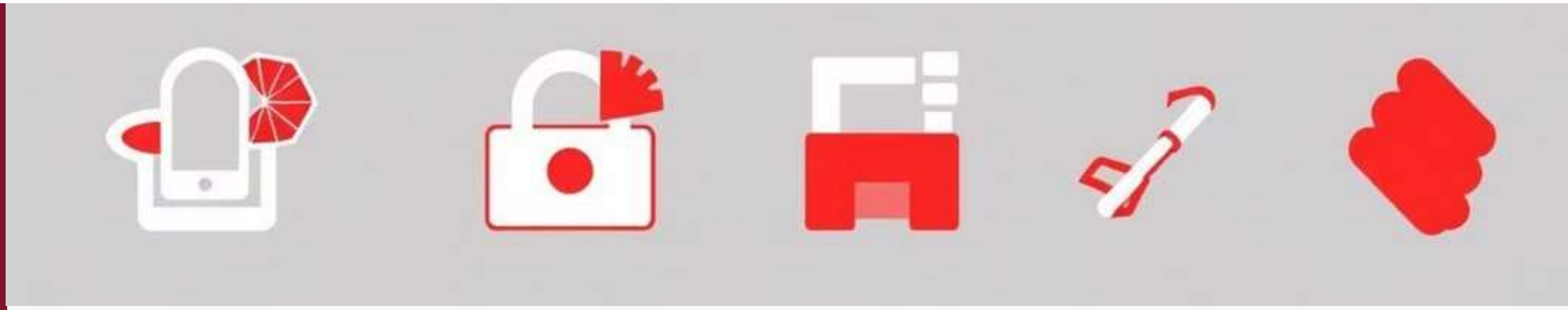
“Urgent: Action Required on Financial Document” designed to elicit quick response.

Sender's Email Address

A subtle character change like “john.doe@company-supp0rt.com” with zero replacing “o” signals a fraudulent origin.

Call to Action

The “Download Document” link is the malicious payload meant to infect systems upon clicking.



Recognizing Phishing Triggers

Urgency & Pressure

Phrases demanding immediate action like “urgent” aim to bypass rational thinking.

Slight Domain Mistakes

Look out for misspelled or extra characters in email domains signaling spoofing attempts.

Unexpected Attachments/Links

Verify suspicious links or attachments by confirming with the sender before clicking.

Unfamiliar Sender or Context

Always question emails that appear out of context or from unknown sources even if they seem work-related.

What Could Have Been Done Differently?

Clear Communication

Use straightforward, jargon-free language when warning employees about suspicious emails.

Verification Protocol

Encourage staff to always confirm with IT before opening unsolicited links or attachments.

Prompt Reporting

Instill a culture where suspicious activities are immediately reported without assumptions of safety.

Automated Email Filtering

Enhance IT systems to detect and quarantine phishing attempts proactively before reaching end users.



Preventative Measures – Our Action Plan

Email Awareness Training

Regularly schedule sessions focused on identifying phishing and suspicious patterns with real examples.

Enhanced Email Filters

Upgrade antiphishing technologies to automatically detect and block fraudulent emails before delivery.

Multi-Factor Authentication

Implement MFA comprehensively to reduce risks from compromised credentials.

Incident Reporting Protocol

Establish clear, accessible steps for staff to follow immediately upon receiving suspicious emails.



Common Cyber Threat Scenarios

Credential Theft via Fake Login Pages

What Happens: Staff receives an email pretending to be from software like Xero, MYOB, or QuickBooks with a "login issue" link.

Threat: The link leads to a fake login page. When staff enter credentials, attackers steal them.

Risk: Unauthorized access to client accounting data.

Fake Client Onboarding Requests

What Happens: A cybercriminal pretends to be a new client and sends a fake onboarding request, including supposed "financials" in an attachment.

Threat: The attached zip or PDF file installs malware.

Risk: Malware may log keystrokes, access internal files, or spread across the network.

Infected Excel or PDF Files from "Clients"

What Happens: Staff receives a "revised payroll sheet" or "updated super form" from a spoofed client email.

Threat: These contain macros that install ransomware.

Risk: Systems are locked until ransom is paid; client data may be leaked.

Vendor Spoofing in Approval Workflows

What Happens: Fake invoices or payment approval requests are sent using emails that closely mimic known vendors.

Threat: Approvals may go through quickly in busy finance teams.

Risk: Fraudulent payments or disclosure of sensitive client details.

Shared Folder Exploits

What Happens: A fake "ShareFile" or "OneDrive" email asks staff to open a document urgently.

Threat: The link installs spyware that watches internal traffic and captures logins.

Risk: Ongoing undetected access to payroll, tax files, or ATO correspondence.

Advanced Threat Scenarios

Social Engineering via LinkedIn

What Happens: Attackers research staff on LinkedIn, then use that info to craft convincing spear phishing emails (e.g., "Can you update this on behalf of Karen from Payroll?").

Threat: Email appears legitimate due to insider-like language.

Risk: Staff might unknowingly share or upload sensitive files.

Unauthorized Remote Access Tools

What Happens: Staff may download a screen-sharing app to "help a client" without approval.

Threat: The app is a remote access Trojan (RAT).

Risk: Attackers now have full access to the machine.

Deepfake Voicemail or Video Messages

What Happens: A fake voicemail (or AI-generated video) appears to come from a director or client asking to "urgently share last quarter's payroll reports."

Threat: Targets emotions (urgency, fear of escalation).

Risk: Staff complies and leaks critical data without questioning.

Public Wi-Fi Exploits During Remote Work

What Happens: Staff working from cafes or airports connect to fake Wi-Fi hotspots.

Threat: Man-in-the-middle attackers intercept login sessions.

Risk: Sensitive data, passwords, and session cookies are stolen.

Supply Chain Attack on Shared Portals

What Happens: A third-party app used for file sharing (like Dropbox, FYI Docs, or Practice Protect) gets compromised.

Threat: Malicious files are uploaded and auto-shared with your team.

Risk: Mass infection, data corruption, or credential theft across all clients.



Essential Cybersecurity Prevention Tips

- **Verify requests:** Use a second channel like phone or Teams chat to confirm.
- **Check links carefully:** Hover over URLs and verify email domains before clicking.
- **Limit software installs:** Only install software approved by IT for security.
- **Use strong protections:** Enable MFA and use password managers for account safety.
- **Report concerns:** Immediately alert IT about suspicious activity, even if unsure.

Contact Us

Ind: 044 2826 0205
Aus: +61 409 164 237

Carisma Solutions Pvt Ltd

biz@carisma-solutions.com.au

carisma-solutions.com.au

Presence across all states of Australia

Queensland Government
VICTORIA State Government
ACT Government
Tasmanian Government
Government of South Australia
GOVERNMENT OF WESTERN AUSTRALIA
NORTHERN TERRITORY GOVERNMENT

CARISMA SOLUTIONS

An Xcelerate Venture

THANK YOU!

Carisma Solutions confidential.

Proprietary Information Disclaimer

"All information" contained herein, including but not limited to intellectual property, trade secrets and proprietary methodologies, process, solutions, models are confidential and proprietary to Carisma Solutions Pvt Ltd., www.carisma-solutions.com.au

It is intended solely for the use of the individual or entity to whom it is addressed or presented, for the purpose of review, consideration and evaluation only.

Recipients are strictly prohibited from disclosing, reproducing, or distributing this or any part of this document to any third party without prior express written consent from Carisma Solutions Pvt Ltd.,

If you have received this proposal/ Presentation / Document / File in error, please notify us immediately and delete the same.

For Carisma Solutions Pvt Ltd.,
Director - director@carisma-solutions.com.au