



Phishing, Fakes & Browser-Based Attacks

October 21, 2026 | 11:00–11:30 AM Eastern

Presented by

Davin Singh
VP of Managed Services



Welcome to the Cyber Smart Series

Practical cybersecurity awareness for the decisions employees make every day

Today's Presenter:



Davin Singh
VP Managed Services
BitbyBit

30 MINUTES

Focused, plain-language
training

REAL EXAMPLES

Familiar experiences attackers
imitate

PRACTICAL ACTIONS

Simple steps employees can
use immediately

Today: recognize the trap, pause before acting and know when to report.

Why Cyber Awareness Still Matters

62%

**of breaches
involved the human
element.**

41%

**of social-
engineering
breaches involved
vectors beyond
email alone.**

31%

**31% of breaches
involved
vulnerability
exploitation, now
the leading initial
access vector.**

48%

**48% of breaches
involved a third
party, including
vendors, SaaS
providers and
cloud platforms.**

Source: Verizon 2026 Data Breach Investigations Report

This Month in Cyber: Real Headlines

What attackers have been doing over the past five weeks, and what each attack needed from a person

OCT 16, 2026

FBI & CISA joint alert

AI is making phishing emails and texts harder to tell from the real thing

The ask: Click a link in a real-looking message

OCT 12, 2026

Huntress research

Fake ChatGPT assistants lure users into ClickFix malware

The ask: Copy and paste a “fix” into your computer

SEPT 17, 2026

FBI public service announcement

Fake police and officials: \$1.6B+ stolen since January 2025

The ask: Pay or share personal details, fast

SEPT 7, 2026

CloudSEK research

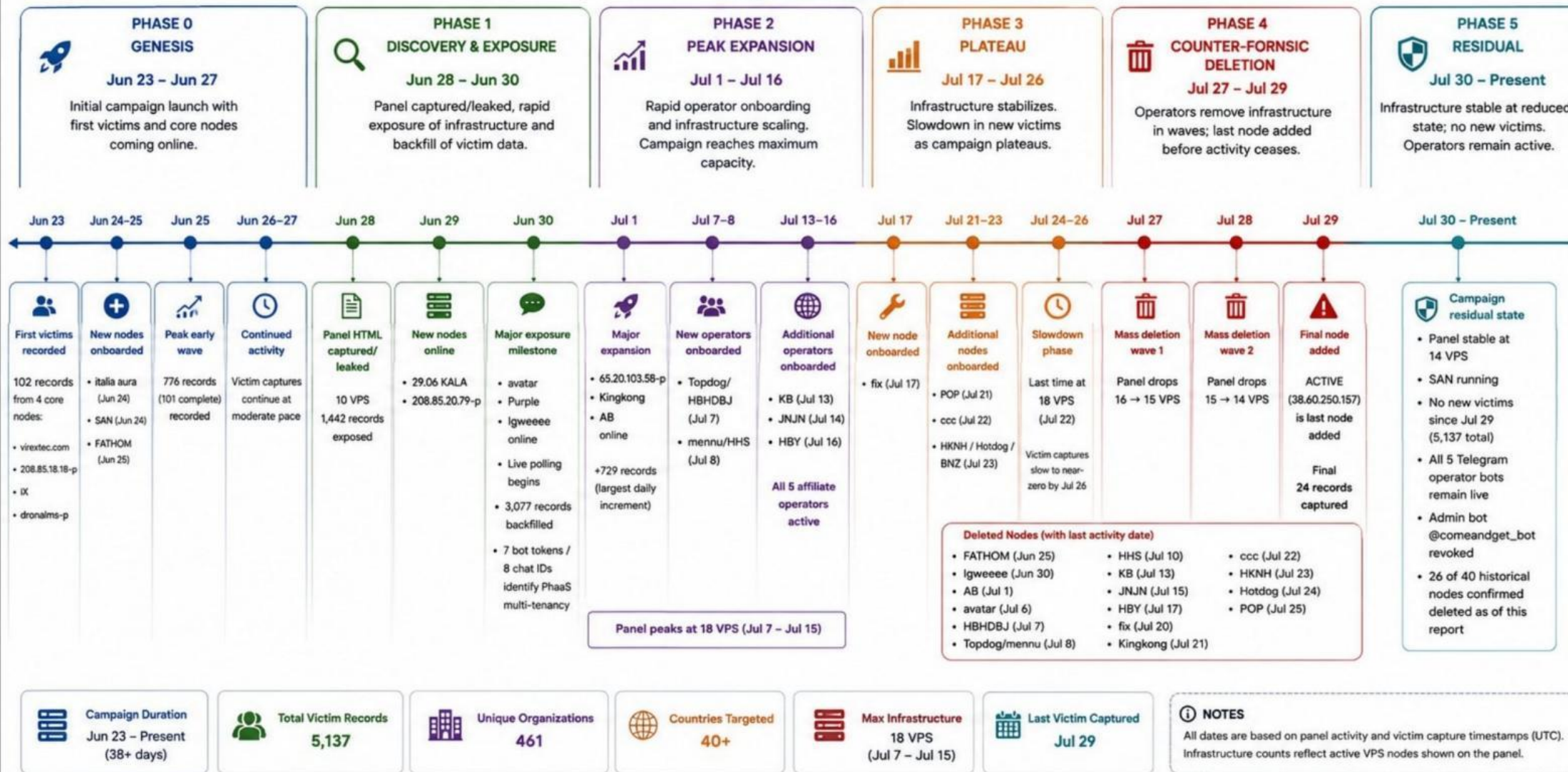
Fake Microsoft 365 sign-in pages got past MFA at 258 organizations

The ask: Sign in on a page that only looks real

No one broke through a firewall. Each attack needed a person to act.

BIGBEAR 2.0 PHISHING-AS-A-SERVICE CAMPAIGN TIMELINE

June 23 – Present



The Good News: You Are a Strong Defense

TRAINING WORKS

33% → 4%

of employees clicked a simulated phishing email before training, versus after one year of ongoing practice

KnowBe4 2026 Phishing by Industry Benchmarking Report

Don't Make It Easy for Them

Cybersecurity Awareness Month 2026 • CISA & the National Cybersecurity Alliance

What You Will Learn

- 01 Recognize deceptive sign-in experiences
- 02 Avoid malicious browser and CAPTCHA prompts
- 03 Check QR-code destinations before opening
- 04 **Use Stop. Check. Report. when something feels wrong**

QUICK AUDIENCE QUESTION

Which is hardest to judge?

LOGIN PAGE

BROWSER UPDATE

CAPTCHA

QR CODE

Keep your answer in mind as we walk through each trap.



SOCIAL ENGINEERING

When familiar-looking experiences become traps.

Browser-in-the-Browser Attacks

A fake sign-in window drawn inside the page you're on.

REAL-WORLD EXAMPLE • JUNE 2026

Unit 42 found fake Microsoft 365 popups with a fake address bar, padlock and real-looking URL.

WHY IT WORKS

It drags like a real window, then sends you to the real Microsoft page so you think you mistyped.

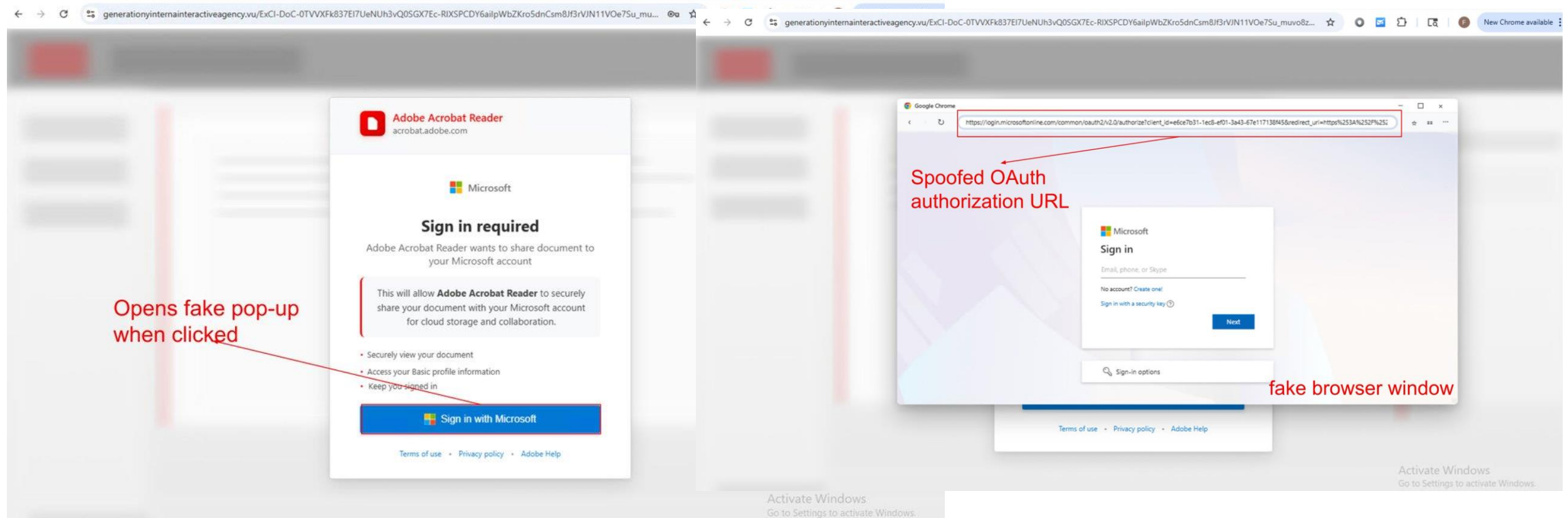
SAFER RESPONSE

Try dragging it outside the browser: a fake can't leave the page. If your password manager won't fill it in, stop and call IT.

Do not trust appearance alone.

Browser-in-the-Browser Attacks

A fake sign-in window drawn inside the page you're on.



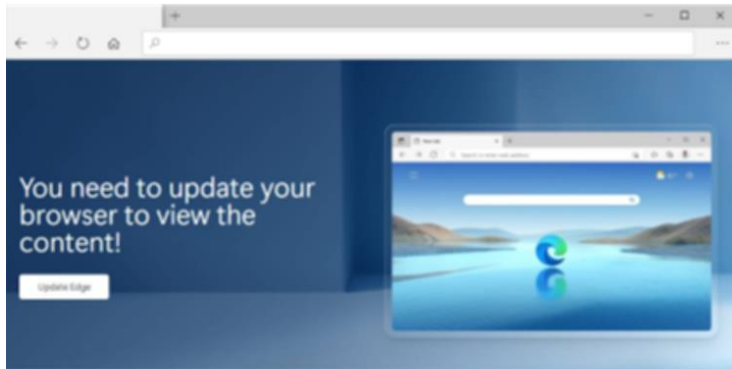
Do not trust appearance alone.

ClearFake Attacks

Fake browser updates turn a familiar maintenance task into a malware trap.

THE SETUP

A compromised website displays an update overlay that resembles your browser.

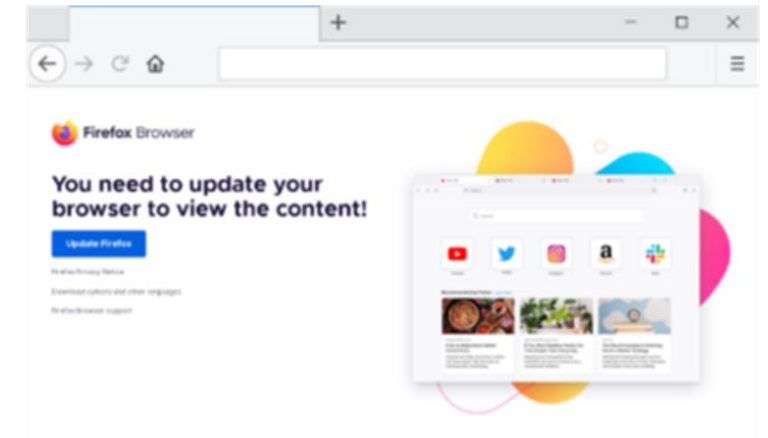
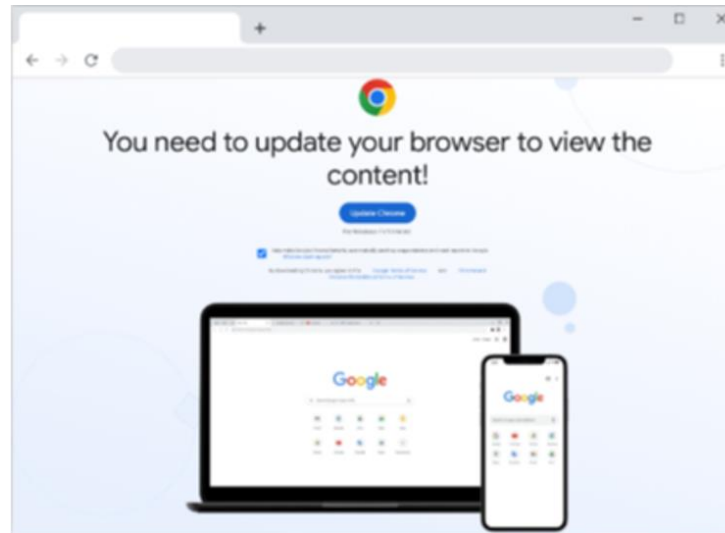


SAFER RESPONSE

Close the prompt.
Update from the browser settings or an approved IT process.

RED FLAGS

An update prompt appears on an unrelated site, pressures you to act or downloads an unexpected file.



Never install a browser update from a website prompt.

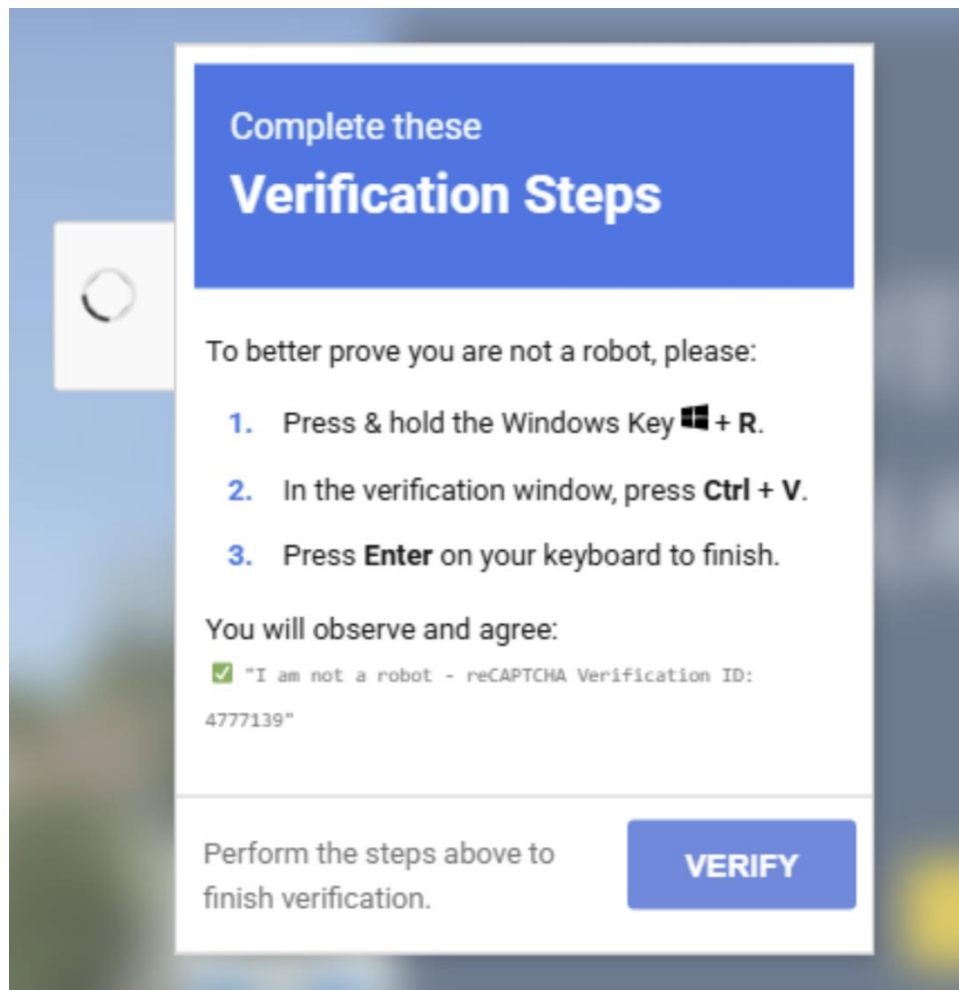
ClickFix Attacks

The “fix” is the attack.

THE WARNING SIGN

A CAPTCHA or error prompt tells you to press Windows+R, paste a command or run instructions.

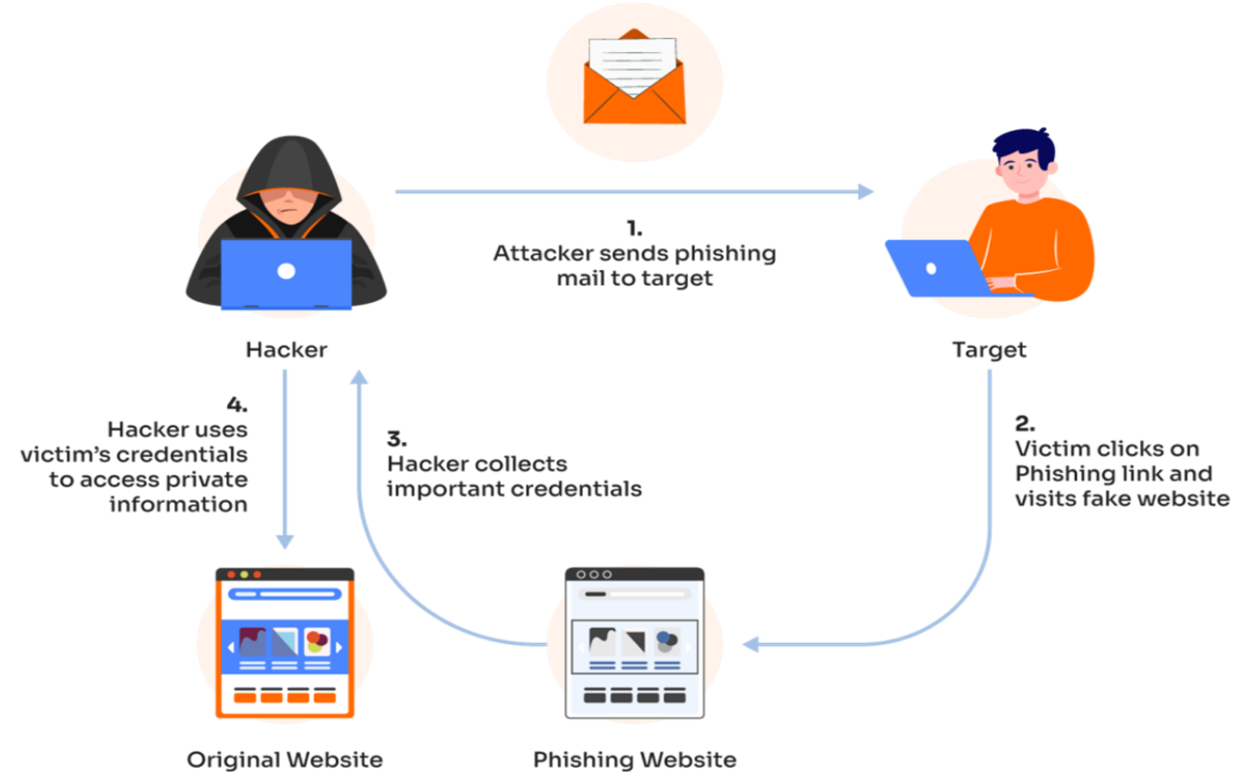
Never run commands provided by a website to prove you are human.



Close the page and report it to IT or security immediately. If the page was opened from an email, also report the original message as phishing in Outlook.

Phishing and Pharming: What to Inspect

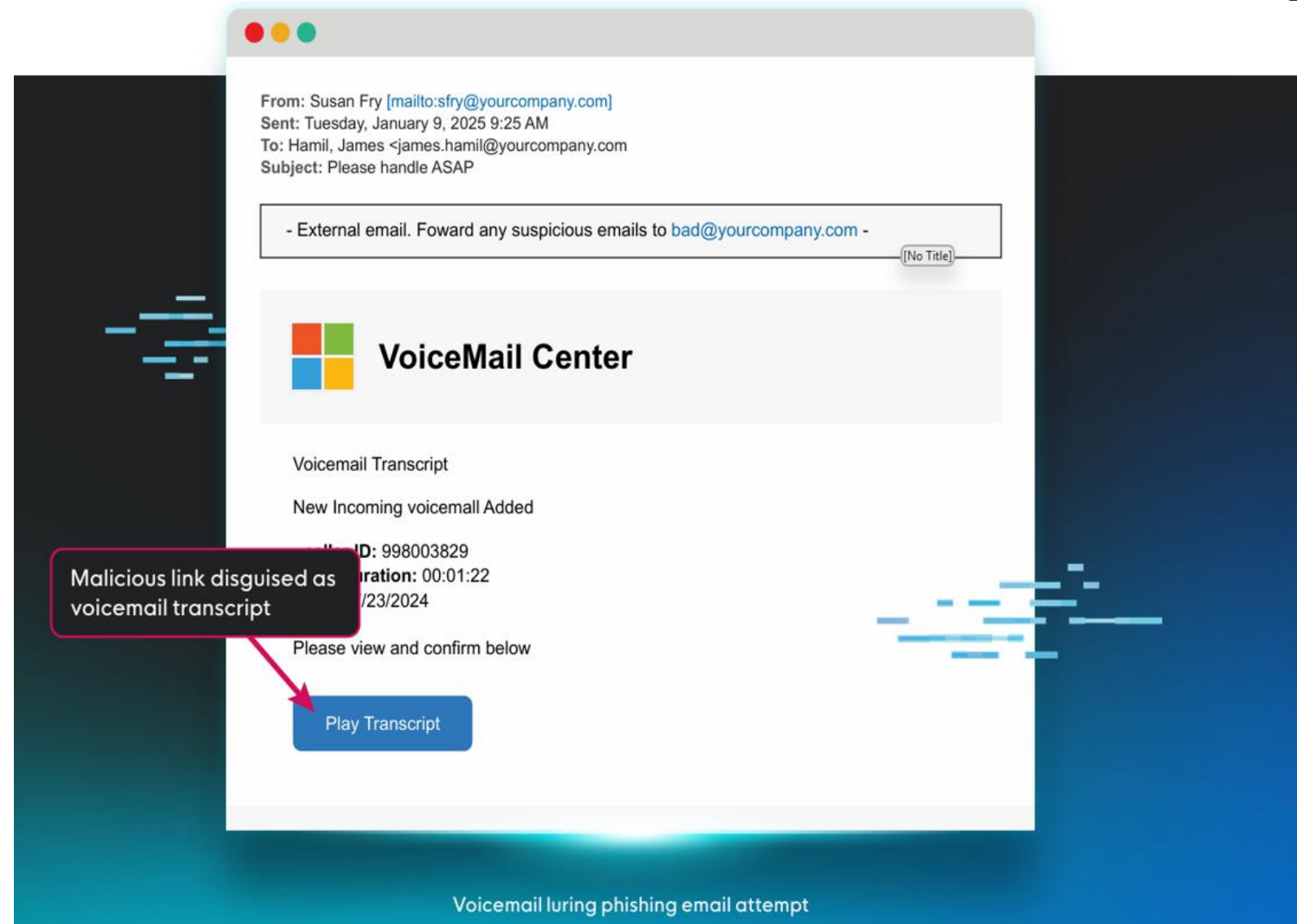
- ✓ Was the message or sign-in expected?
- ✓ Does the request create pressure or bypass normal process?
- ✓ Can you reach the service through a trusted bookmark or app?
- ✓ Can you verify the request with the sender another way?



If the destination or request cannot be verified, do not proceed.

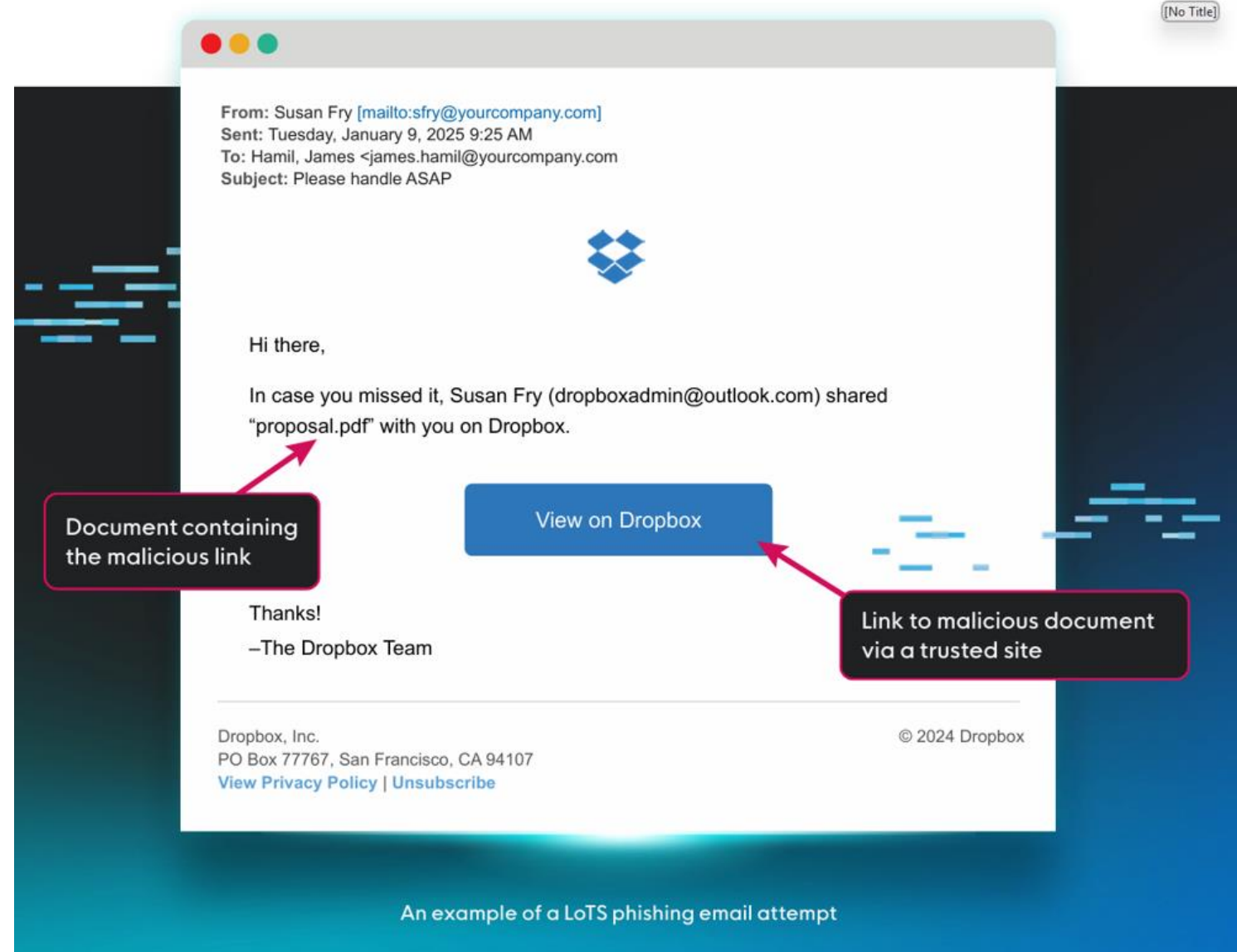
Phishing and Pharming: Fake Voicemail

Suspicious
Voicemail
Notification



Phishing and Pharming: Malicious Shared Document

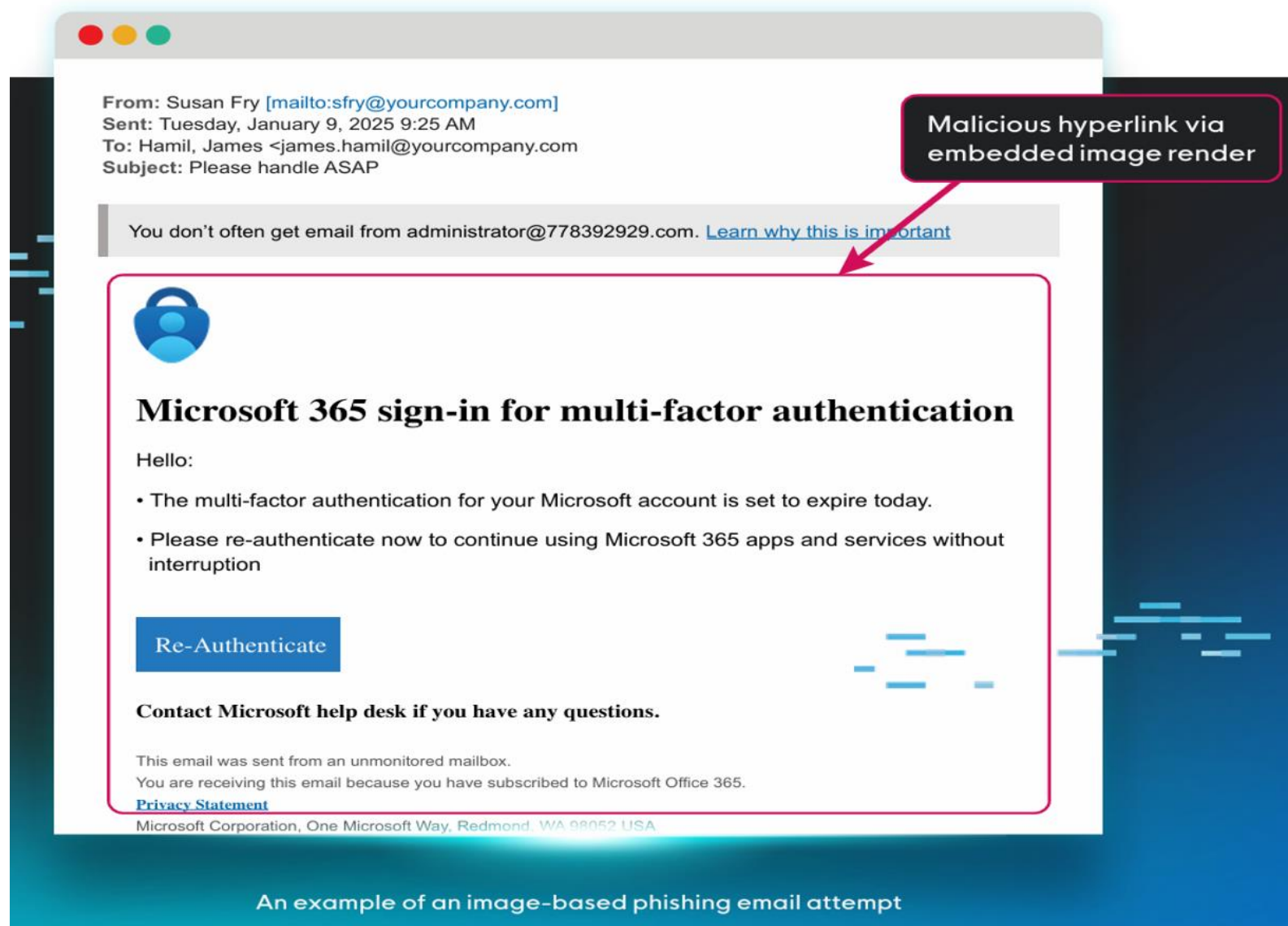
Unexpected
Shared
Document Link



An example of a LoTS phishing email attempt

Phishing and Pharming: Fake Microsoft 365 Sign-In

Fake M365
Authentication
Request

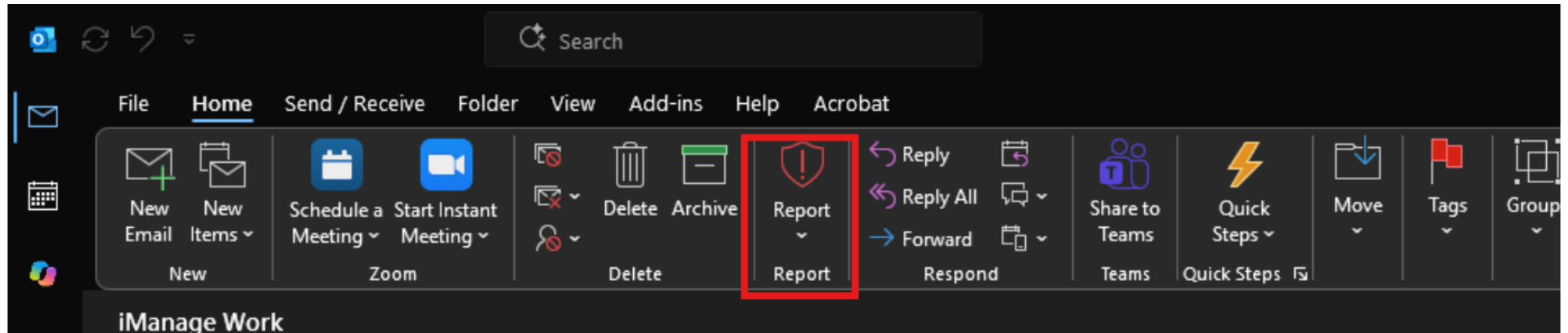



An example of an image-based phishing email attempt

Reporting Junk or Phishing Email

If you receive a suspicious or unwanted email in your Inbox, please report it directly through Outlook:

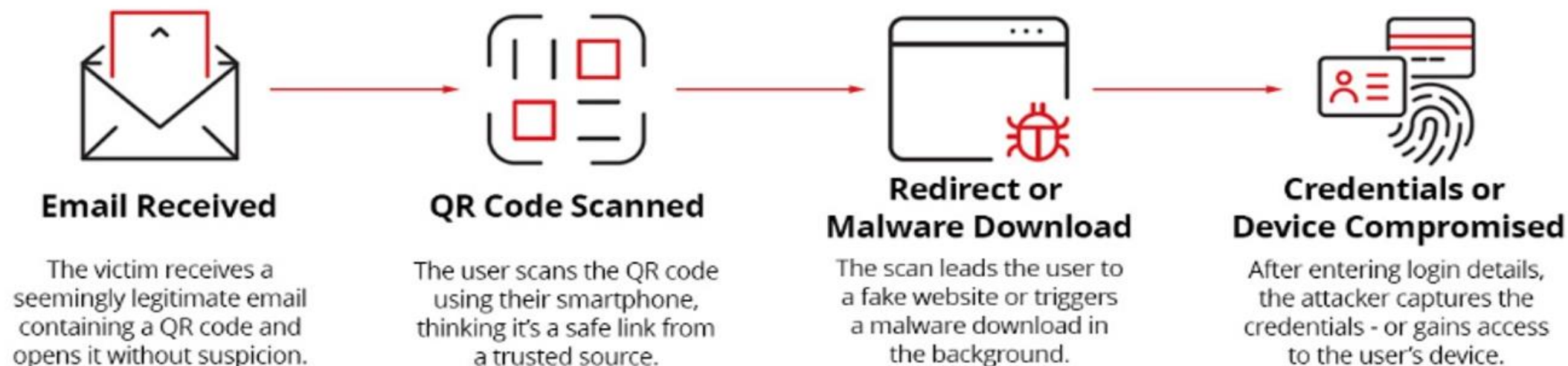
1. Select the suspicious email.
2. Select **Report** from the Outlook toolbar.
3. Choose the appropriate option:
 - **Report Junk** for unwanted or spam email.
 - **Report Phishing** if you believe the message is attempting to impersonate someone, steal information, or trick you into clicking a malicious link or opening an attachment.



Quishing: Think Before You Scan

QR codes hide the destination until a device reads them.

Preview first. Open second.



PAUSE

Was this QR code expected and is the source trustworthy?

PREVIEW

Read the destination before opening it.

CHECK

Look carefully at the domain and use a trusted site or app when possible.

REPORT

Tell IT or security about suspicious codes or destinations.

STOP. CHECK. REPORT.

STOP

Pause before entering credentials, installing an update, scanning a code or following instructions.

CHECK

Use a trusted website, app, phone number or colleague to verify the request.

REPORT

Notify IT or security quickly, even if you already clicked or entered information.

Fast reporting gives the organization more options to respond.

Five Things to Remember

1

Do not trust a sign-in prompt because it looks familiar.

2

Update browsers through settings or an approved IT process.

3

Never run commands provided by a CAPTCHA or website error.

4

Preview QR-code destinations and inspect the domain.

5

If something feels wrong: Stop. Check. Report.



QUESTIONS?

If you see something suspicious

Stop. Check. Report.
Follow your organization's reporting process.

Next Cyber Smart Session

Vishing, Account Takeover & Shadow Tech
January 20, 2027



866.391.1566 | info@bitxbit.com | bitxbit.com