CYBERSECURITY AWARENESS SERIES

Phishing Awareness Training

Recognize. Resist. Report.

INTERNSHIP TASK
Mehdi Jaffari @CodeAlpha

THE THREAT LANDSCAPE

Phishing by the Numbers

36%

of all data breaches involve phishing

3.4B

phishing emails sent every single day

£50K

average financial loss per phishing incident

300%

increase in attacks since COVID-19

Sources: Verizon DBIR 2024 | IBM Cost of Data Breach | Statista 2024

WHAT IS PHISHING?

Understanding the Many Faces of Attack

Email Phishing

Mass emails impersonating trusted brands or institutions.

Smishing (SMS)

Fraudulent text messages tricking you into clicking links.

Vishing (Voice)

Phone calls from fake support agents or government officials.

Spear Phishing

Highly targeted attacks using personal details to deceive.

Whaling

Targeting C-suite executives with sophisticated lures.

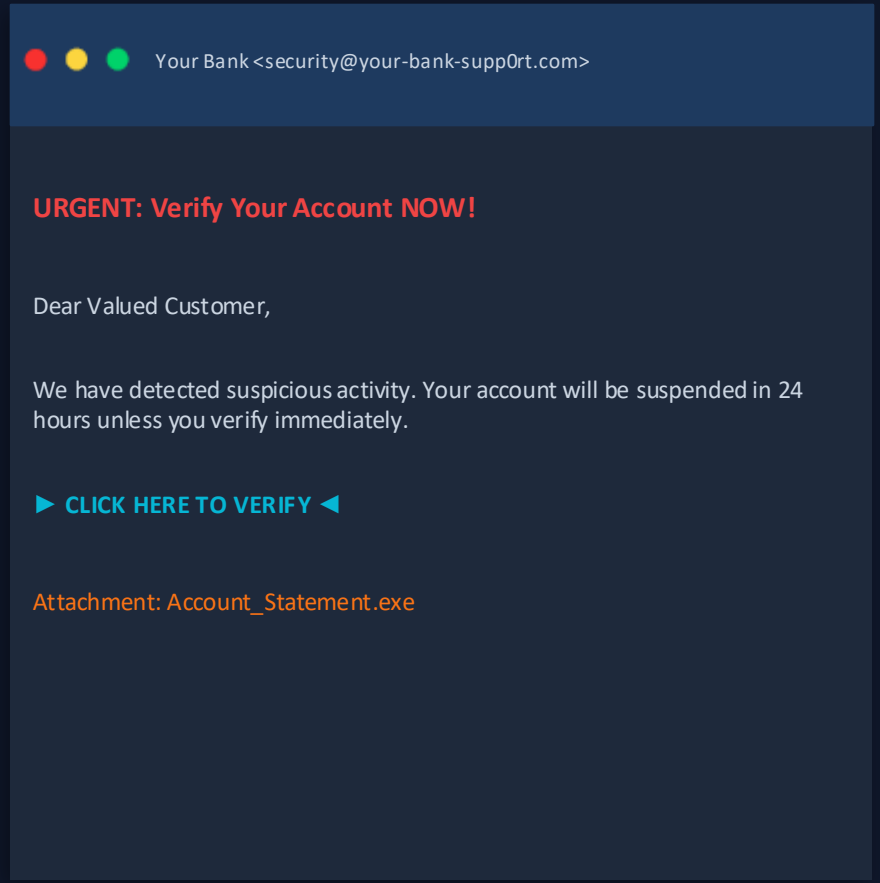
Clone Phishing

A legitimate email re-sent with malicious links or attachments.

RECOGNIZING PHISHING EMAILS

7 Red Flags to Watch For

1. Suspicious sender address (typos, strange domain)
2. Urgent or threatening language ('Act NOW!')
3. Generic greeting ('Dear Customer')
4. Unexpected attachments (.exe, .zip, .doc)
5. Suspicious or mismatched links (hover to check)
6. Poor grammar, spelling errors, odd formatting
7. Requests for personal info, passwords, or payment



FAKE WEBSITES & URL TRICKS

How Attackers Disguise Malicious Links

https://paypa1.com/login

⚠ Letter '1' replaces 'l'

https://amazon-security-alert.net

⚠ Legitimate brand, wrong domain

https://google.com.verify-id.ru

⚠ Subdomain trick — real domain is .ru

https://bit.ly/3xK9mP

⚠ Shortened URL hides true destination

SAFE BROWSING CHECKLIST

- Look for HTTPS and a padlock icon
- Manually type known URLs
- Hover over links before clicking
- Check for misspellings in domain
- Verify SSL certificate owner
- Use a password manager (won't autofill fakes)

SOCIAL ENGINEERING TACTICS

The Psychology of Manipulation

URGENCY

'Your account will be deleted in 2 hours' — fear prevents critical thinking.

AUTHORITY

Posing as IT support, a CEO, or a government agency to demand compliance.

SCARCITY

'Only one spot remaining' — artificial scarcity pressures quick decisions.

RECIPROCITY

Offering a 'free gift' first to create a sense of obligation to respond.

SOCIAL PROOF

'Your colleagues have already updated their info' — exploiting conformity.

FAMILIARITY

Using a name, photo or shared connection harvested from social media.

82% of security breaches involve a human element — social engineering is the #1 attack vector (Verizon DBIR 2024)

REAL-WORLD EXAMPLES

High-Profile Phishing Incidents

2016 — Democratic National Committee

A spear-phishing email tricked a campaign official into revealing Gmail credentials. The breach exposed tens of thousands of sensitive documents and influenced a US election.

💡 **Always verify password reset requests through a separate channel.**

2020 — Twitter / X

Attackers used phone-based social engineering to trick employees into granting system access. 130 high-profile accounts were hijacked to promote a Bitcoin scam netting $120,000.

💡 **Verify all unusual IT requests with your security team directly.**

2022 — Twilio

SMS phishing (smishing) messages impersonating IT convinced employees to hand over login credentials. Customer data of over 1,900 Signal users was exposed.

💡 **SMS messages — even from known numbers — can be spoofed.**

2023 — MGM Resorts

A 10-minute LinkedIn-based vishing call to the help desk compromised MGM's entire network, causing $100M+ in damages and days of service outages.

💡 **Help desks must use multi-factor identity verification protocols.**

BEST PRACTICES & TIPS

Your Phishing Defence Toolkit

Enable Multi-Factor Authentication

MFA blocks 99.9% of automated attacks even if credentials are stolen (Microsoft, 2023).

Think Before You Click

Hover over every link. If the URL looks suspicious or unexpected, don't click — report it.

Verify Requests Out-of-Band

Got an urgent request? Independently call the sender via a known number — never use a number in the email.

Keep Software Updated

Patched browsers and OS stop many phishing exploits. Enable automatic updates on all devices.

Use a Password Manager

Password managers won't autofill credentials on fake sites — your first automated defence.

Report Suspicious Emails

Don't delete — report! Your IT team can prevent the same attack from reaching your colleagues.

KEY TAKEAWAYS

Your 60-Second Security Checklist

01 STOP & THINK — Do not act under pressure. Attackers rely on urgency to cloud your judgment.

02 VERIFY — Independently confirm unusual requests via a known, trusted contact method.

03 HOVER — Always hover over links before clicking to preview the true destination URL.

04 PROTECT — Enable MFA on all accounts and use a password manager consistently.

05 REPORT — Report suspicious messages to your IT/security team immediately — don't delete.

When in doubt — DON'T click. Report to security@yourcompany.com