Phishing Attacks: Protecting Your Digital World

Presented by Tahir Nisar, Cyber Security Intern (Remote) at Code Alpha

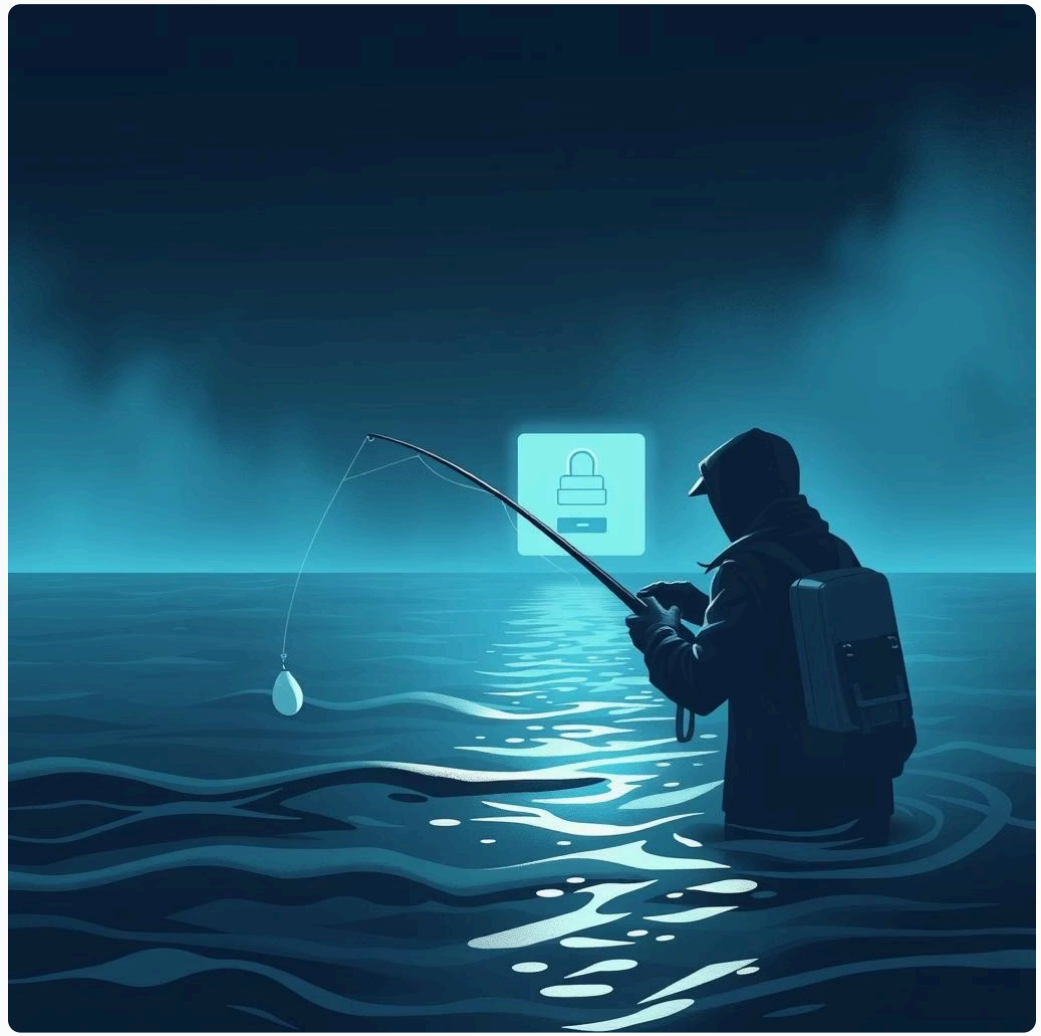
Phishing is a leading cyber threat, causing 90% of security incidents. UK businesses face a 75% phishing attack rate (CybSafe 2023). Our goal is to equip you to recognise and combat these deceptive attacks effectively.

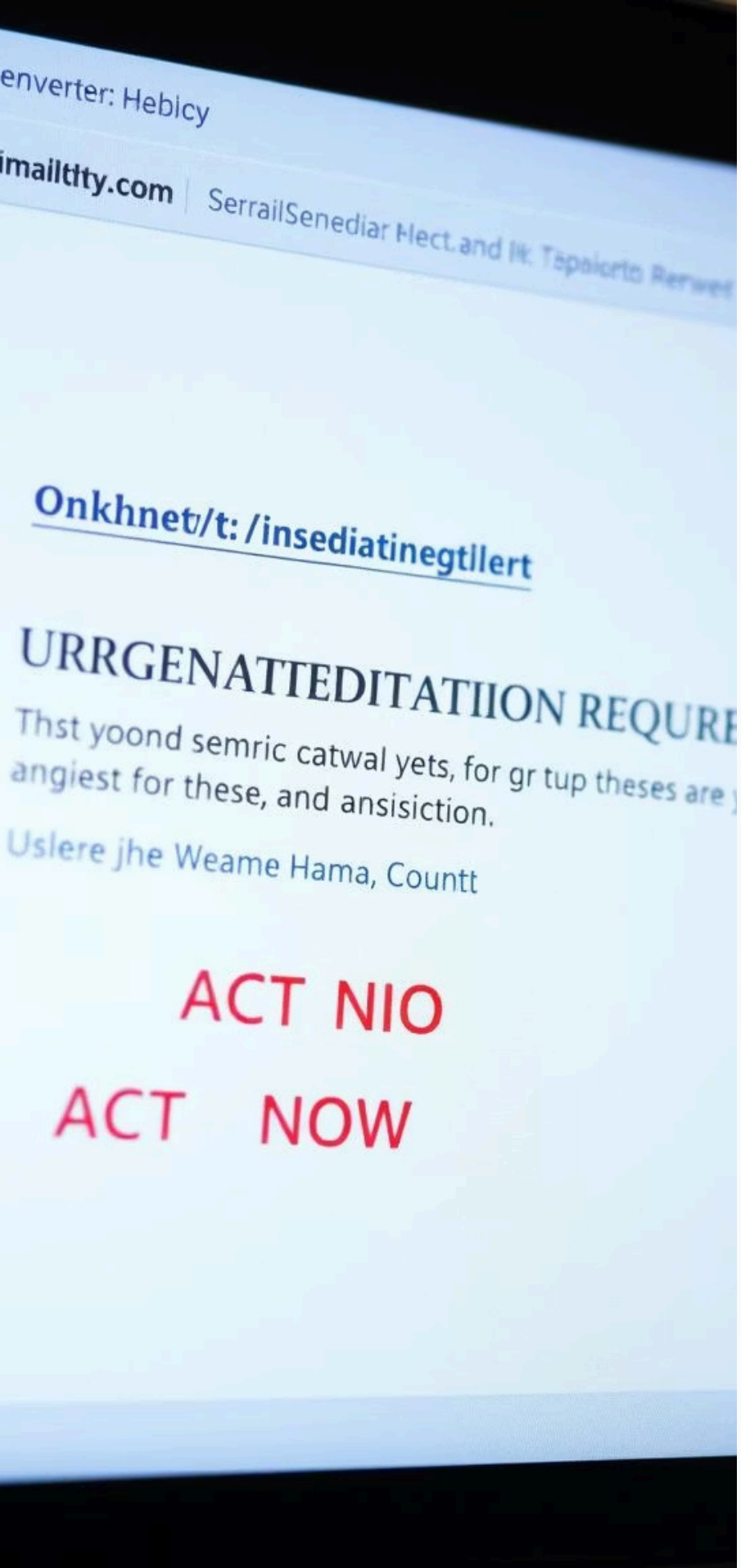
by Tahir Nisar

Understanding Phishing: The Deception Game

Phishing is a social engineering attack designed to trick individuals into revealing sensitive data, such as login credentials or financial information. Attackers often mimic trusted entities like banks, tech support, or government agencies to gain credibility.

The average cost of a data breach stemming from a phishing attack is estimated at £3.8 million (IBM, 2023), highlighting the significant financial impact. Common tactics include deceptive emails, SMS messages (Smishing), voice calls (Vishing), and sophisticated cloned websites.





Spotting Phishing Emails: Key Red Flags

Suspicious Sender

Look for generic or misspelled email addresses, such as **paypal@securesvc.net**, that attempt to impersonate legitimate organisations.

Urgent/Threatening Language

Be wary of messages that create a sense of panic, like "Your account will be suspended" or "Immediate action required" to pressure you into acting quickly.

Grammar & Spelling Errors

Professional organisations maintain high standards for communication. Numerous errors are a strong indicator of a fraudulent email.

Unusual Links/Attachments

Always hover your mouse over links to check the URL before clicking. Be extremely cautious with unexpected attachments, which may contain malware.

Identifying Fake Websites: Don't Get Caught

URL Discrepancies

Check for mismatched domains, for instance, **amazon-login.com** instead of **amazon.co.uk**. Slight variations are common.

Lack of HTTPS

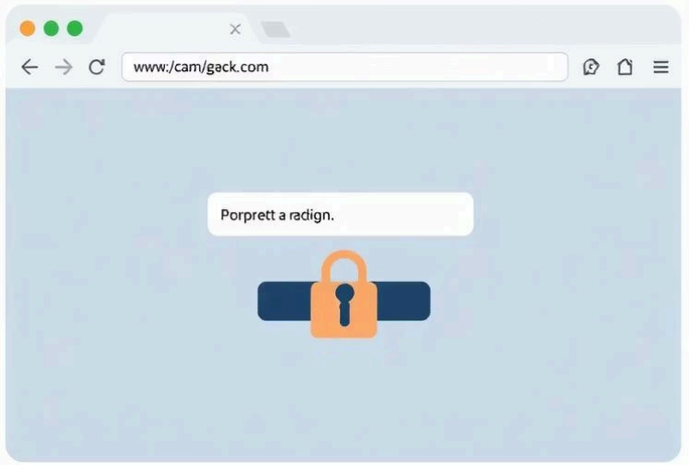
Always verify the padlock icon and "https://" in the address bar, indicating a secure connection. Missing this is a major red flag.

Poor Design Quality

Fraudulent sites often have low-resolution logos, inconsistent branding, and an unprofessional layout, betraying their true nature.

Too Good to Be True Offers

Be suspicious of unrealistic discounts or prize notifications. If an offer seems implausibly generous, it’s likely a scam.



Social Engineering: Manipulating Human Behaviour

Social engineering exploits psychological vulnerabilities to trick individuals into performing actions or divulging confidential information.

Pretexting

Inventing a false scenario, like posing as "IT support needing your password," to gain your trust.

Baiting

Offering something desirable, such as free downloads or gift cards, to lure users into a trap.

Quid Pro Quo

Promising a service, like "help with password reset," in exchange for your sensitive data.

Impersonation

Posing as a senior executive (CEO Fraud/BEC) or a trusted contact to deceive you.

Urgency/Fear

Creating panic with messages like "Act now or lose access!" to bypass critical thinking and force immediate action.

Best Practices: Your Shield Against Phishing

Verify Everything

Always call the sender using official contact information, never details provided in a suspicious email.

Multi-Factor Authentication (MFA)

Activate MFA on all accounts; it adds a critical second layer of security, blocking 99.9% of automated attacks.

Strong, Unique Passwords

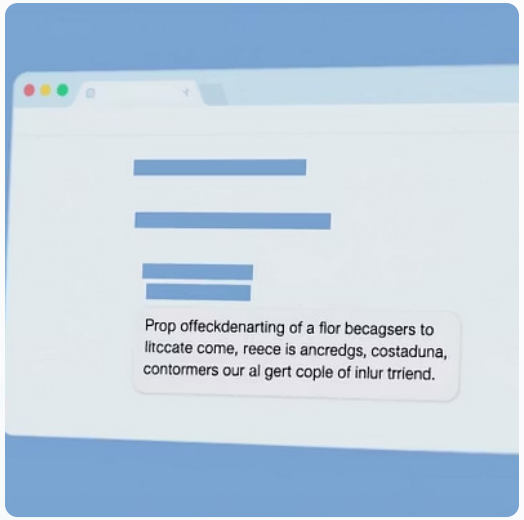
Use complex and distinct passwords for each of your online accounts to prevent credential stuffing.

Keep Software Updated

Regularly patch and update all your software to fix security vulnerabilities and prevent exploitation by attackers.

Additionally, always utilise robust security software, including antivirus, anti-malware, and firewalls, to provide comprehensive protection against various cyber threats.

Real-World Phishing Examples



- **Twitter Hack (2020):** Social engineering led to the compromise of employee accounts, facilitating a high-profile cryptocurrency scam.
- **NHS Phishing Campaigns (2020-2022):** Numerous attacks exploited COVID-19 themes, targeting both staff and the public with deceptive messages.
- **Business Email Compromise (BEC):** The average cost of a BEC attack in the UK exceeds £50,000 (NCSC), involving impersonation to trick employees into transferring funds.
- **Royal Mail Scam (2023):** Fake delivery texts redirected victims to fraudulent payment sites, often demanding small fees for package redelivery.

Interactive Quiz & Conclusion

Quiz: Which of these is a phishing red flag?

A) A generic greeting like "Dear Customer"

B) A valid URL (e.g., https://www.google.com)

C) A professional and error-free email

D) A request to update your password on a known, secure site

Answer: A) A generic greeting like "Dear Customer"

Key Takeaways:

- Stay vigilant and always question unsolicited requests.
- Verify all suspicious communications through official channels.
- Enable Multi-Factor Authentication (MFA) wherever possible.

Your awareness and proactive steps are the strongest defence against phishing attacks.

Thank you for your attention. Questions?