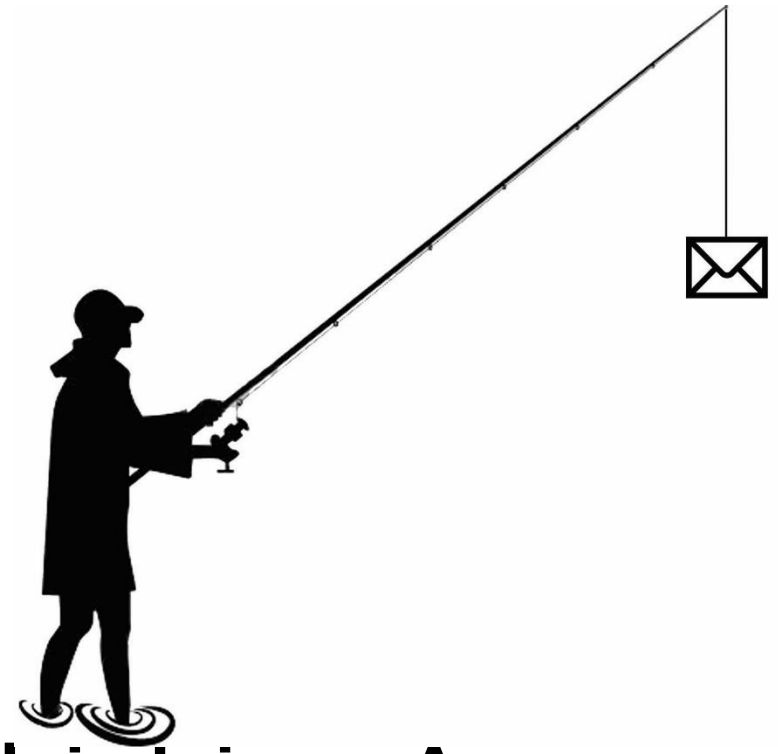
المختبر المرجعي الوطني
National Reference Laboratory
Managed by LabCorp
A Mubadala Company

Information Technology Department



Phishing Awareness

DON'T GET HOOKED

How to Recognize and Avoid

PHISHING ATTACKS

What is Phishing?

Phishing is when a hacker impersonates a legitimate institution or a co-worker to lure you over email or a call into providing sensitive data such as passwords or banking information.

Phishing is on the rise!

What is Phishing?

The Go-To Social Engineering Strategy

Phishing attacks are **techniques** used by cybercriminals to con users/employees into **revealing sensitive information** or **installing malware** by way of electronic communication.

Phishing Attack Methods

MOST COMMON TYPE OF PHISHING ATTACK

MASS-SCALE **PHISHING**

Attack where fraudsters **cast a wide net of attacks** that aren't highly targeted

HIGHLY TARGETED TYPE OF PHISHING ATTACK

SPEAR **PHISHING**

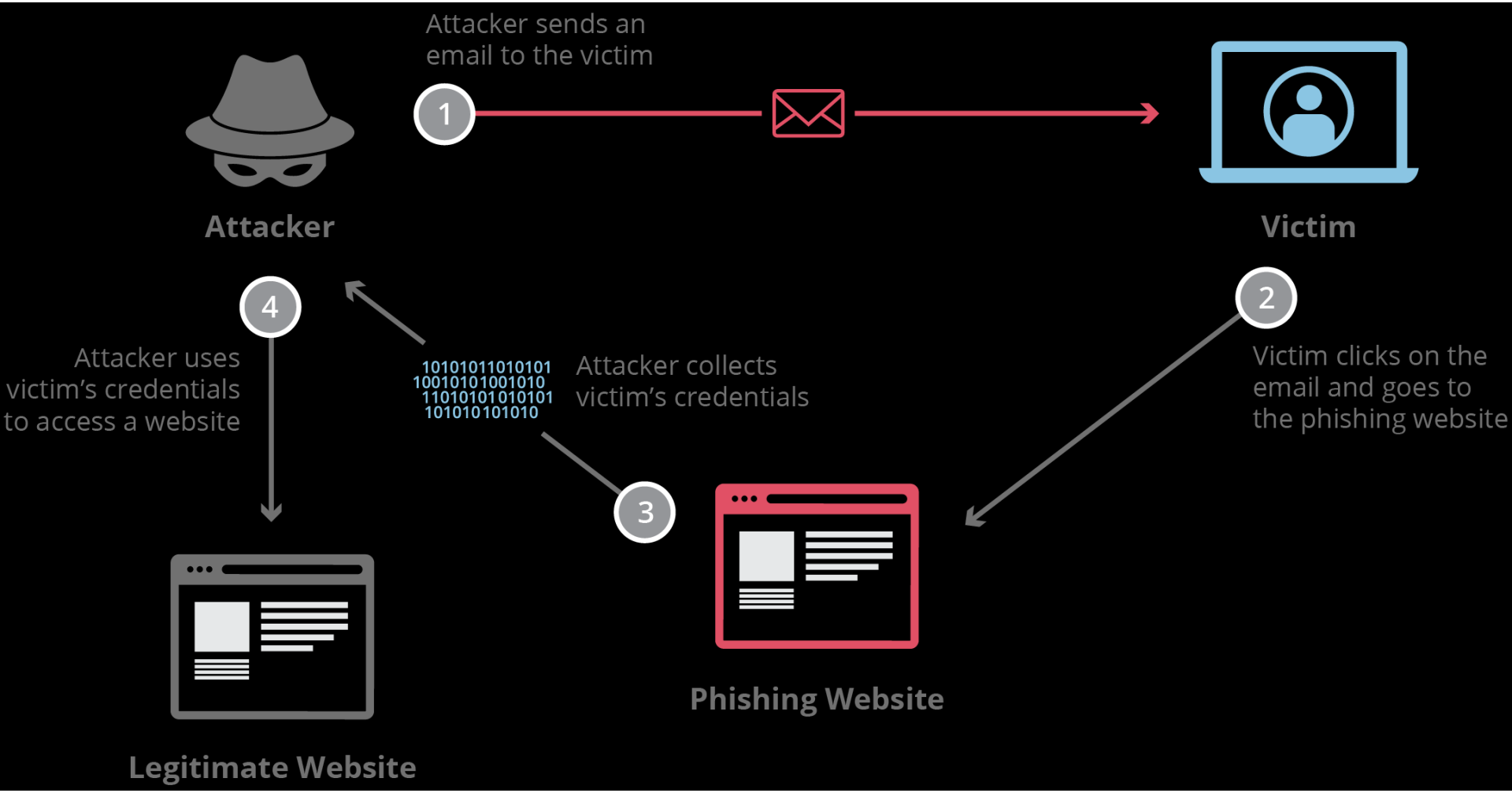
Tailored **to a specific victim or group of victims** using personal details

THE **MOBY DICK** OF PHISHING ATTACKS

WHALING

Specialized type of spear phishing that **targets a "big" victim** within a company

e.g., CEO, CFO, or other executive

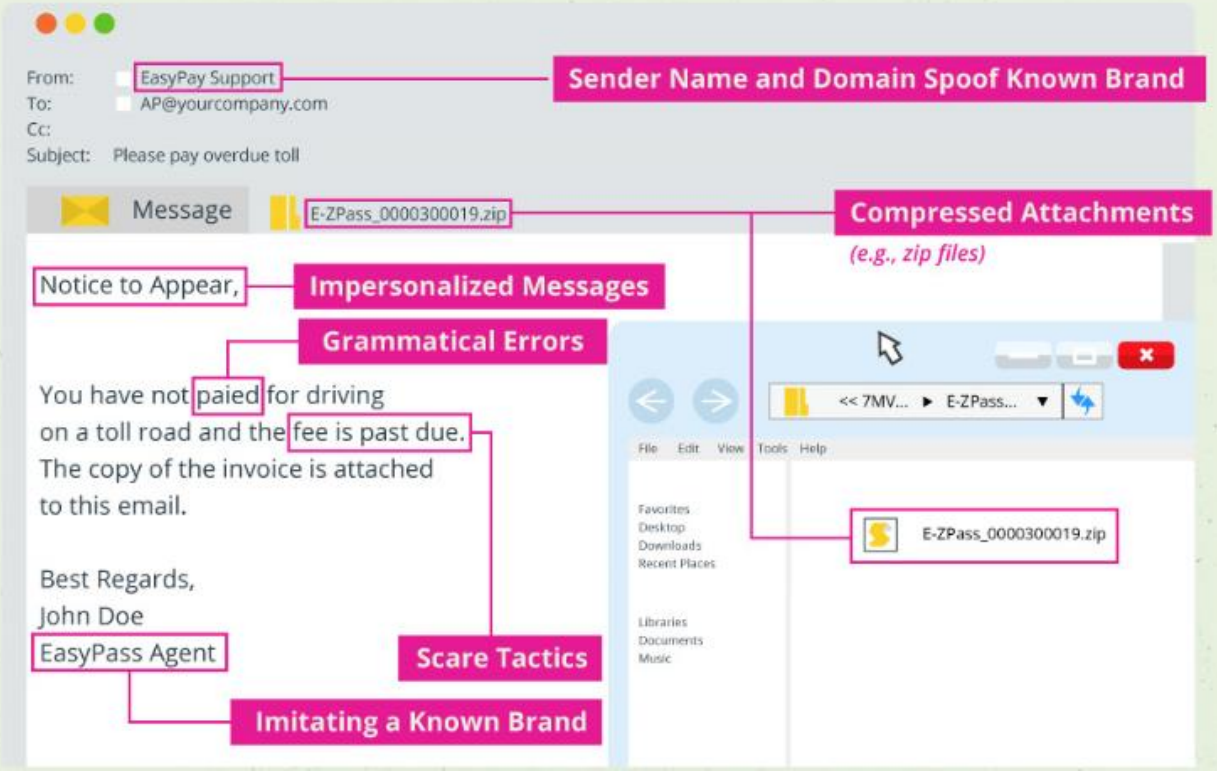

Attacker sends an email to the victim
1
Attacker
Victim
4
Attacker uses victim's credentials to access a website
10101011010101
10010101001010
11010101010101
10101010101
Attacker collects victim's credentials
2
Victim clicks on the email and goes to the phishing website
3
Phishing Website
Legitimate Website

Keep Your Eyes Peeled for **All Forms** of Phishing Attacks

EMAIL PHISHING

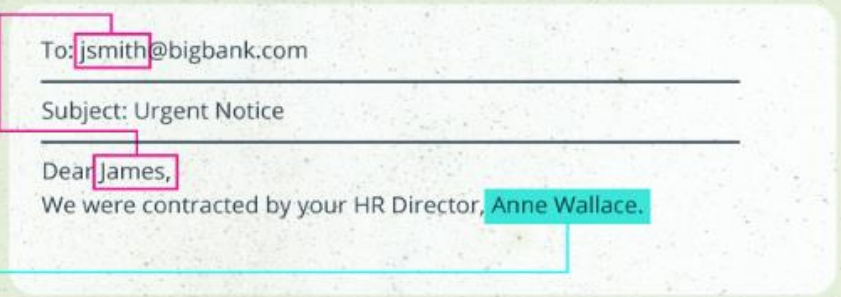
Fraudsters send **phony emails** that appear to come from valid sources in an **attempt to trick users** into revealing personal and financial information

What to look for?



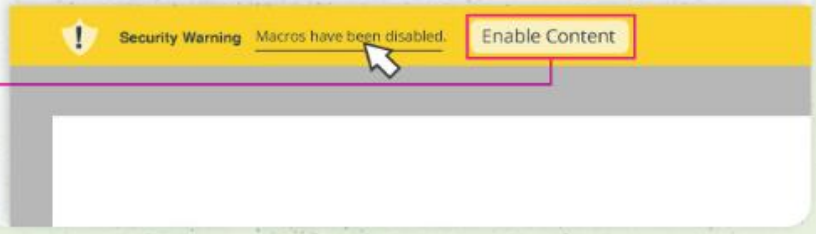
Highly Personalized Messages

Unlike mass phishing emails, spear phishing messages are highly personalized and will often reference coworkers' or friends' names



Embedded Malicious Files

Common file attachments *(.doc, .xls, .ppt, etc.)* can contain malicious macros



Spoofed Links

Spoofed link text can hide a hyperlink's actual destination

Spoofed Websites

Links to spoofed versions of well-known websites can look legitimate and are used to steal info submitted via forms or distribute malware to visitors

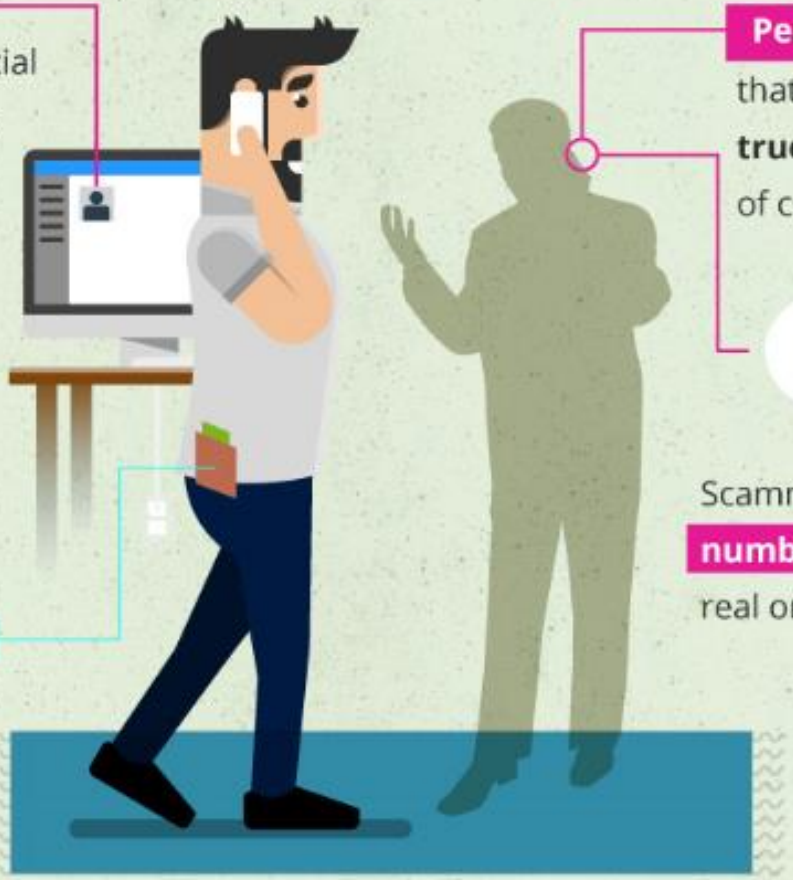
VISHING

Short for **"voice phishing,"** vishers use the telephone to solicit unsuspecting victims for **financial or personal details**

What to look for?

Personal data can be gathered from social media profiles, providing criminals with sensitive details to make attacks seem more legitimate

Persuasive phone tactics that are **too good to be true** are a dead giveaway of criminal activity



Vishers utilize **fear tactics** to con you into thinking your money is in danger and you must act quickly

Scammers often **alter phone number/IDs** to disguise the real origin of the call

First Things First—Be Vigilant Online and Use Your Common Sense!

Always be suspicious of any unsolicited communication from businesses or individuals, regardless of the message medium

Don't click on links or attachments in suspect emails, texts, or social media messages

Directly contact the purported sender via their official website, phone number, or email address if you are not sure about the legitimacy of a message you have received

Report suspected phishing scams to your IT and security teams

6 COMMON PHISHING ATTACKS AND HOW TO PROTECT AGAINST THEM

HOW TO IDENTIFY PHISHING SCAMS AND PROTECT YOURSELF

1 Deceptive Phishing

Email messages claiming to come from recognized sources ask you to verify your account, re-enter information, or make a payment.

SCAM'S OBJECTIVE:
Trick you into providing the details they need to access your bank account.

HOW TO AVOID IT:
Look out for generic greetings or requests for information that the sender should already have.

2 Spear Phishing

A more sophisticated version in which the sender uses available information to direct their request at you.

SCAM'S OBJECTIVE:
Directly target you to acquire your banking details or other data.

HOW TO AVOID IT:
Look out for typos, and 'alarming' threats or ultimatums.

3 CEO Fraud

Phishers use an email address similar to that of an authority figure to request payments or data from others within in the company.

SCAM'S OBJECTIVE:
For the victim to transfer money directly to the cybercriminals.

HOW TO AVOID IT:
Double-check suspicious requests with the boss before putting the business in jeopardy.

4 Pharming

Fraudsters hijack a website's domain name and use it to redirect visitors to an imposter site.

SCAM'S OBJECTIVE:
To intercept and steal online payments.

HOW TO AVOID IT:
Check that the URL of any site asking for data is authentic – look for the secure certificate.

5 Dropbox Phishing

Realistic-looking emails claiming to come from Dropbox request the user to click through to "secure" their account or download a shared document.

SCAM'S OBJECTIVE:
To install malware on the victim's computer.

HOW TO AVOID IT:
Set up two-step verification, for example with a USB key.

Google Docs Phishing 6

A message invites victims to view documents on Google Docs. The landing page is indeed on Google Drive so it seems convincing, but entering your credentials will send them straight to the scammers.

SCAM'S OBJECTIVE:
Access to your Google account, including Gmail, Google Play and Android applications.

HOW TO AVOID IT:
Examine the page carefully for errors, such as corrupt characters in the language selection box. Check which service you are entering – it is listed below "One account. All of Google."

Additional Resources

- https://gulfnews.com/business/sectors/technology/cybercrime-cost-uae-dh5-14b-this-year-1.1933736

- https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/

  https://blog.capterra.com/do-you-know-how-to-prevent-phishing-test-your-it-knowledge-with-these-5-phishing-quizzes/

- https://www.valuewalk.com/2016/09/phishing-attacks-protect

For more Information
Please contact IT Service

its@nrl.ae