CodeAlpha

PHISHING AWARENESS

Stay Safe Online

By Renad Alajlan

Introduction

Phishing is a type of cyberattack where hackers pretend to be someone you trust.They may send emails or messages that look real, but are actually fake.Their goal is to trick you into giving away personal information like passwords or bank details.These attacks are dangerous because they look normal and can fool anyone if they’re not careful.

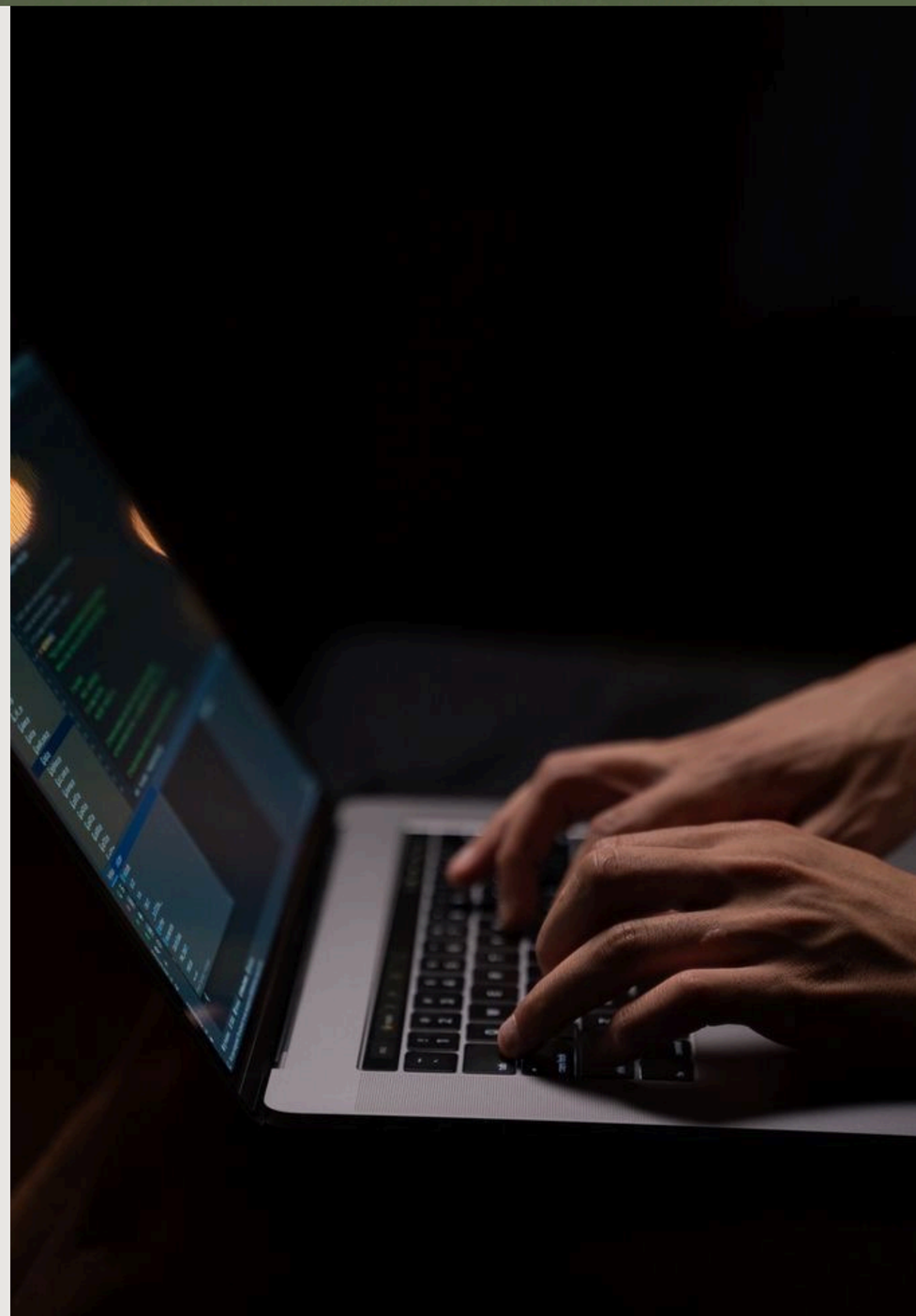
Understanding Fishing Threats

Emails Phishing

is a cyberattack where scammers send fake emails to trick people into revealing sensitive information like passwords or bank details.

Website Phishing

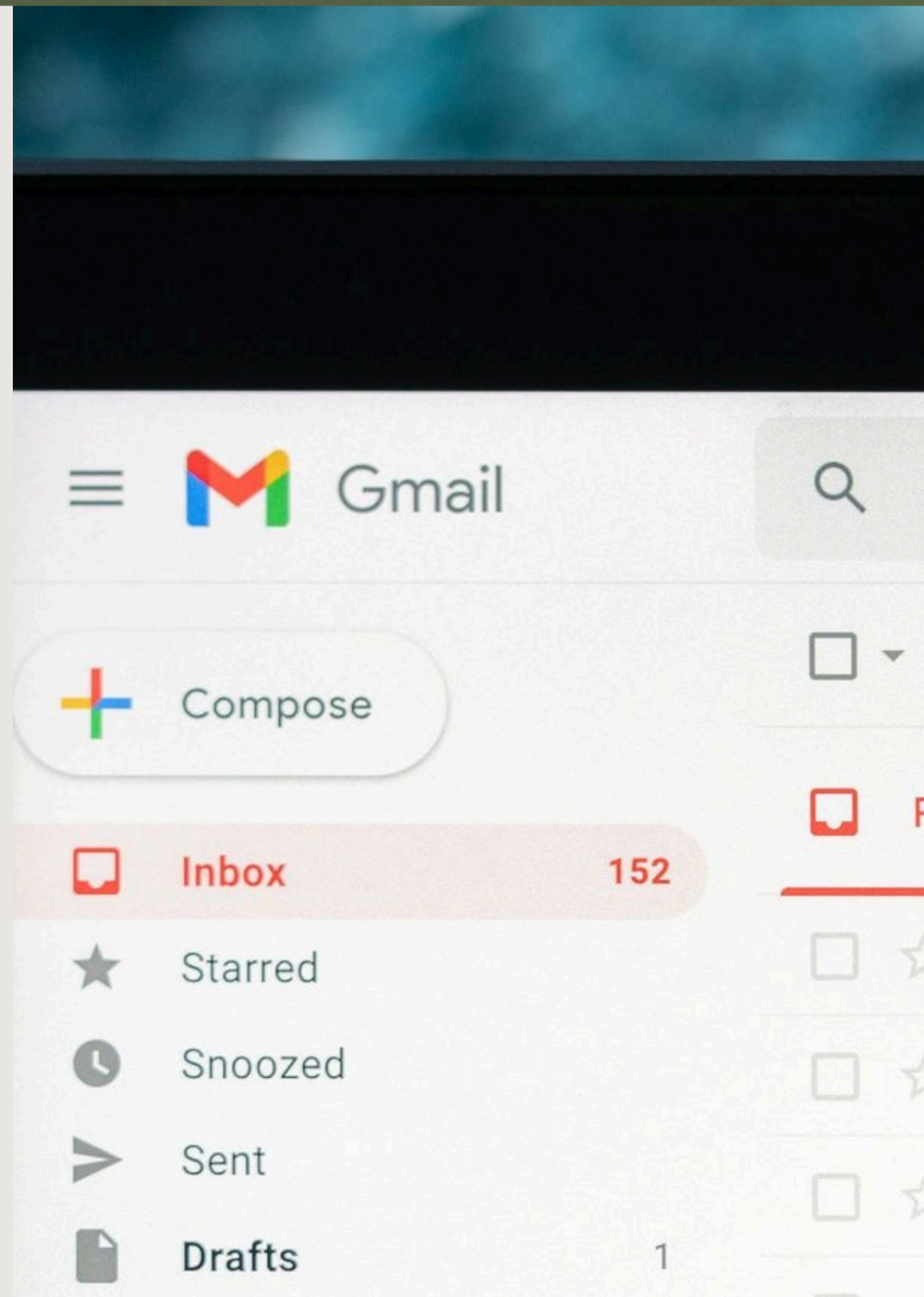
is when attackers create fake websites that look real to trick users into entering sensitive information like usernames, passwords, or credit card numbers.



Recognising a Phishing Email

Warning Signs !

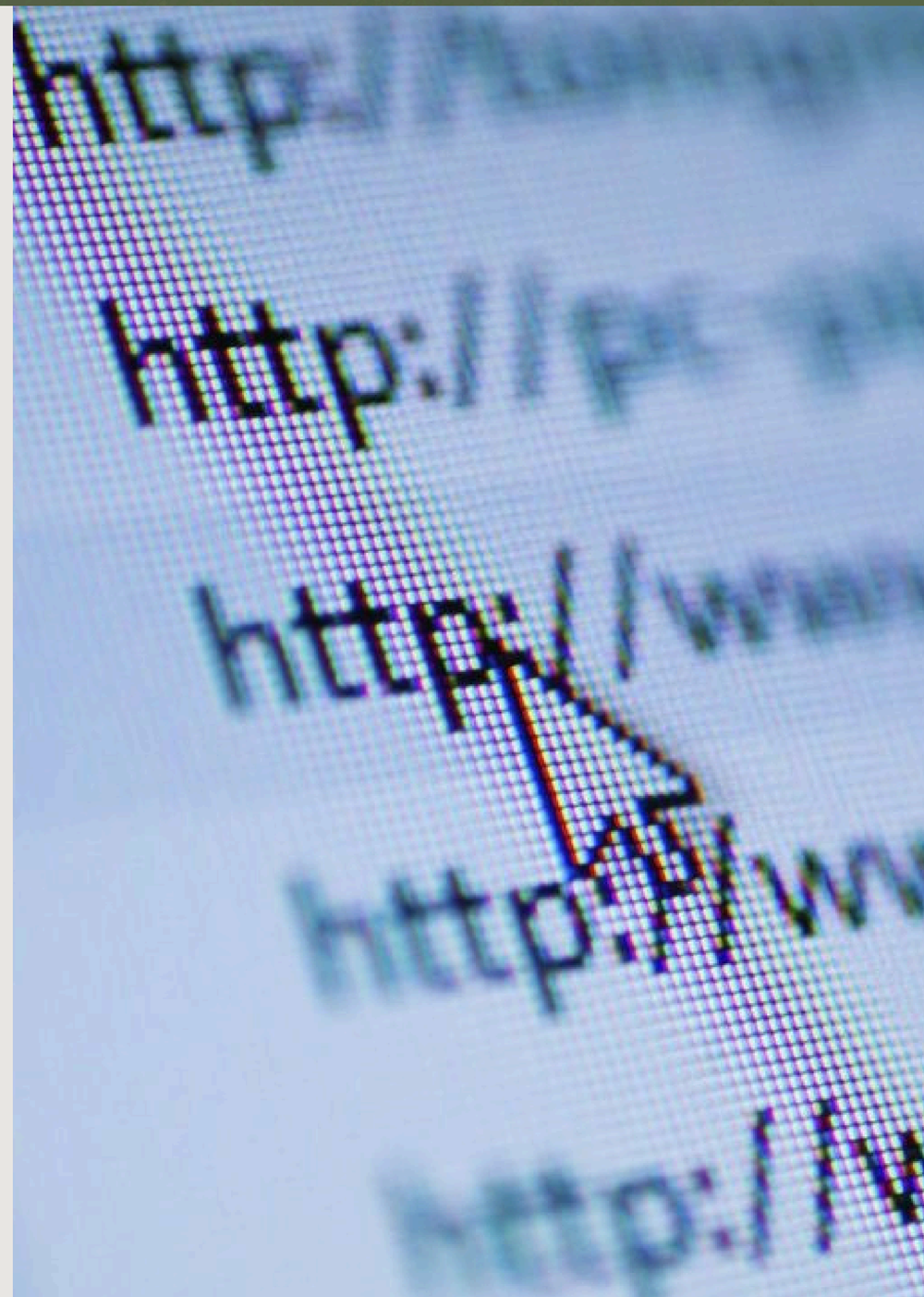
- Spelling and grammar mistakes
- a strange or misspelled address like (e. g. support@paypal.com)
- It may ask you to "act fast" or "verify your account now" using scary or urgent language.
- Generic greetings (e.g. "Dear customer")
- Suspicious links or attachments



Recognising a Fake Websites

Warning Signs !

- Misspelled URLs (e.g. www.faceboook.com)
- No security lock @ in the address bar
- Poor design or unusual formatting
- Requests for personal or banking information
- The website feels "off" or looks different than usual



What is social Engineering?

Social engineering is when hackers use psychology instead of code to trick people. They act like someone you trust – for example, your company's IT staff or your bank.
They use fear, urgency, or friendliness to convince you to give up your personal information.
Phishing is a common example of social engineering because it plays with your emotions to make you act fast without thinking.

Best Practices to Stay Safe

1

Think Before You Click

Phishing emails try to scare or rush you. Check the sender and hover over links before clicking. If unsure, visit the website directly.

2

Use Strong Passwords & 2FA

Use a strong, different password for each account. Turn on two-factor authentication to stay protected even if your password is stolen.

3

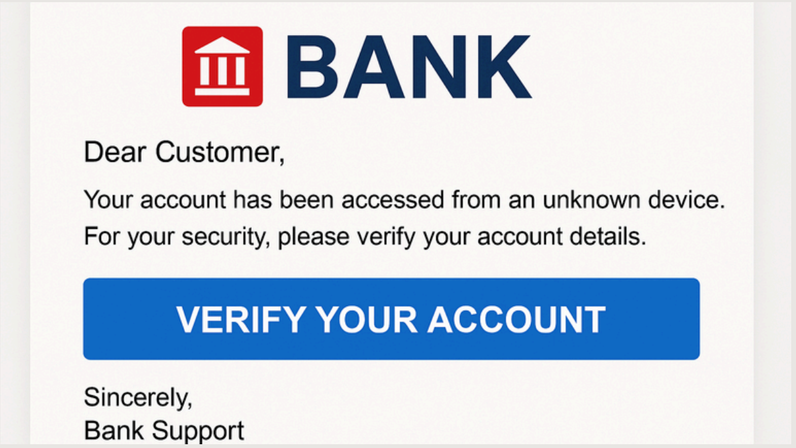
Stay Informed and Aware of New Tricks

Learn about common scams and how phishing works. The more you know, the safer you'll be.

Real-World Phishing Examples

You might get an email pretending to be from Netflix asking you to update your payment info.

Or a text from a fake bank telling you to click a link and confirm your account.



Test Your Awareness

Scenario 1

Email Gift Scam

You get an email saying you won a $500 gift card.
What should you do?
Correct Answer: Report or delete the email.

Scenario 2

Fake Bank Login

A text asks you to log in through a strange link.
What's the best step?
Correct Answer: Call the bank using their official number.

Scenario 3

Password Reset Request

You get an unexpected email saying:
"Your account password was changed. If this wasn't you, click here to secure your account."
What should you do?
Correct Answer: Don't click the link.

Conclusion

Phishing attacks are everywhere, and they can happen to anyone.
The most important thing is to stay alert and think before you act.
If you don’t trust an email or message, don’t click it.
Always verify who’s contacting you. And most importantly – share this knowledge to help your friends and family stay safe too.

CodeAlpha

THANK YOU

Stay alert, stay safe

This presentation was submitted as part of the Cyber Security Internship Program at CodeAlpha.

by: Renad Alajlan