PHISHING AWARENESS TRAINING

Internship at CodeAlpha

PRESENTED BY:

SADARI KARTHIK KUMAR YADAV

STUDENT ID: CA/CS3/11125

BATCH: APRIL BATCH - M3

DOMAIN : CYBER SECURITY

CONTENTS

- Introduction
- What is Phishing
- Types of Phishing Attacks
- Signs of a Phishing Attempt
- Why it’s important for you to follow phishing guidance actively
- Preventing and Responding to Phishing Attacks
- Example of Phishing Mail
- Original Mail
- Phishing Simulation Exercises
- Conclusion

Introduction

- Welcome to Phishing Awareness Training.
- Phishing attacks are among the most common cyber threats today.
- This training module aims to educate you about recognizing and avoiding phishing emails, websites, and social engineering tactics.

What is Phishing?

- Phishing is a form of cybercrime that uses social engineering techniques to trick individuals into revealing sensitive information, such as usernames, passwords, credit card numbers, or other types of credentials.
- In the context of phishing, social engineering refers to the psychological manipulation that takes place.
- Rather than using technical hacking techniques, cybercriminals exploit human behavior to deceive the target.

Types of Phishing Attacks

- **Email Phishing:** Deceptive emails that mimic legitimate sources, often containing links or attachments that lead to malicious websites or downloads.

- **Spear Phishing:** Targeted attacks aimed at specific individuals or organizations, using personalized information to increase credibility.

- **Vishing:** Phishing via voice calls, where scammers impersonate trusted entities to obtain sensitive information over the phone.

Types of Phishing Attacks contd…

- **Whaling:** This is a type of phishing attack that specifically targets senior executives and high-profile targets. The content of a whaling phishing attempt often revolves around executive issues like company-wide decisions or sensitive financial matters.

- **Smishing:** Phishing via SMS or text messages, tricking recipients into clicking malicious links or disclosing information.

Signs of a Phishing Attempt

- **Urgency:** Phishing emails often create a sense of urgency to prompt immediate action.
- **Suspicious Links:** Check links by hovering over them to reveal the actual URL, which may differ from what is displayed.
- **Generic Greetings:** Phishing emails may use generic greetings like "Dear Customer" instead of addressing you by name.
- **Spelling and Grammar Errors:** Legitimate organizations typically have professional communication, while phishing emails often contain errors.
- **Requests for Personal Information**: Be cautious of emails requesting sensitive data like passwords, Social Security numbers, or financial details.

Why it’s important for you to follow phishing guidance actively

- **Personal Information Security**: Phishing scams are designed to steal sensitive data such as credit card details, social security numbers, and login credentials. Active vigilance can prevent unauthorized access to your personal information, protecting you from identity theft.
- **Financial Protection:** Phishing attacks often lead to financial fraud. By understanding and applying phishing guidance, you can avoid fraudulent transactions, saving you from financial losses.
- **Maintaining Privacy:** Falling for a phishing attack can lead to privacy breaches, exposing your personal communications, photos, and other private data.

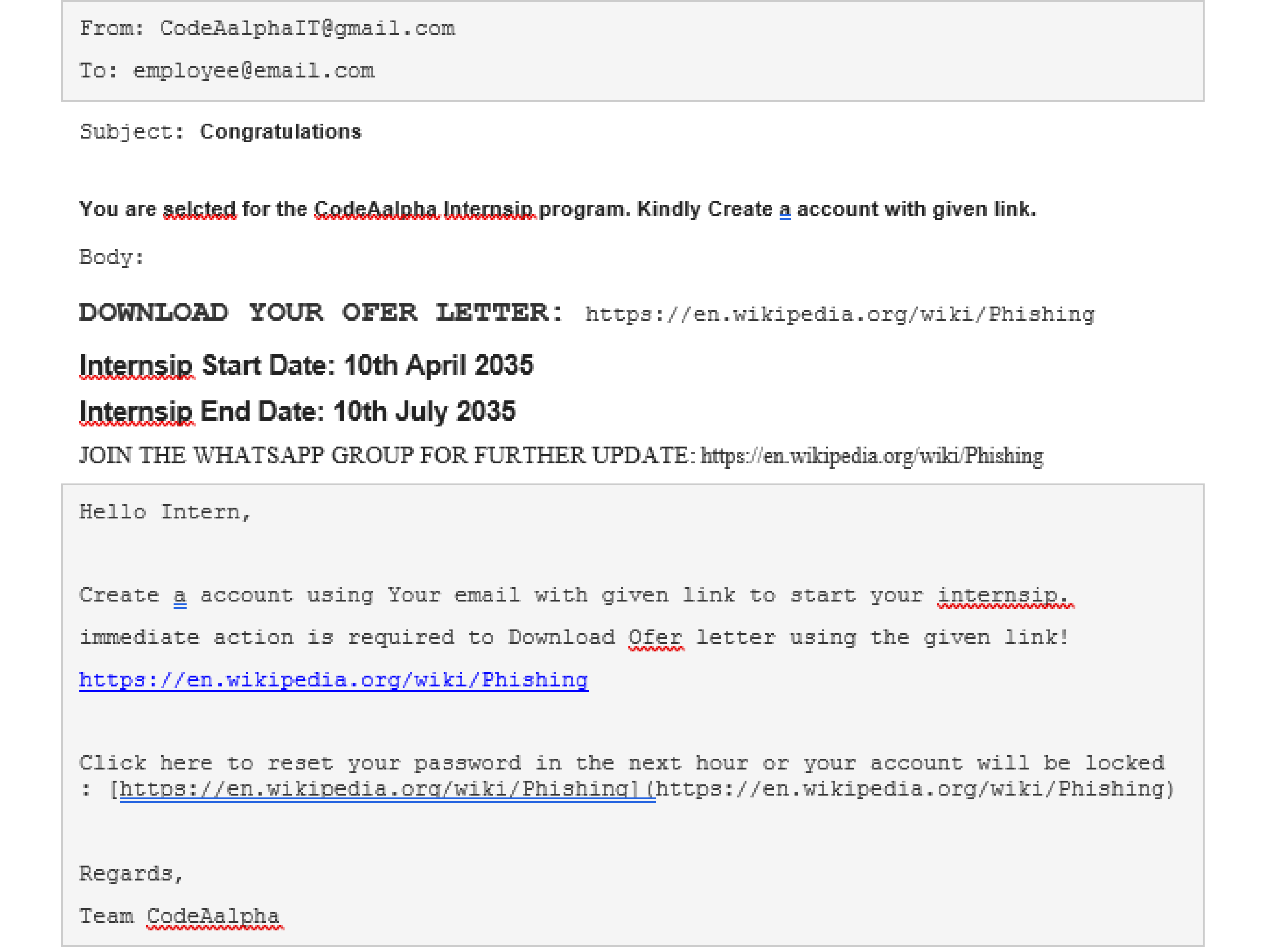
Preventing and Responding to Phishing Attacks

- **Check the Email Address:** Phishing emails often come from email addresses that resemble genuine company addresses but are slightly altered or misspelled.
- **Check for Spelling and Grammar:** Many phishing emails have spelling or grammatical errors. While legitimate companies can occasionally make mistakes, multiple errors are a warning sign.
- **Avoid Clicking Links in Emails**: If an email asks you to log in to an account, manually type the website’s address into your browser instead of clicking the link.
- **Verify a Site’s Security**: Ensure the site is secure before entering any information. Look for “https://” in the URL – the “s” stands for secure.

Preventing and Responding to Phishing Attacks (contd…)

- **Install Anti-Phishing Toolbars:** Some browsers offer free anti-phishing toolbars. These toolbars match where you are going with lists of known phishing sites and will alert you.
- **Use Firewalls:** Use a desktop firewall and a network firewall. This combination provides a double layer of defense against phishing attacks.
- **Regularly Check Your Accounts**: Regularly check your bank, credit, and debit card statements to ensure that all transactions are legitimate.
- **Use Two-Factor Authentication (2FA):** Always enable 2FA when it's available. It adds an extra layer of security by requiring additional verification.

Example of Phishing Mail



From: CodeAalphaIT@gmail.com

To: employee@email.com

Subject: **Congratulations**

You are selcted for the CodeAalpha Internsip program. Kindly Create a account with given link.

Body:

DOWNLOAD YOUR OFER LETTER: https://en.wikipedia.org/wiki/Phishing

Internsip Start Date: 10th April 2035

Internsip End Date: 10th July 2035

JOIN THE WHATSAPP GROUP FOR FURTHER UPDATE: https://en.wikipedia.org/wiki/Phishing

Hello Intern,

Create a account using Your email with given link to start your internsip.

immediate action is required to Download Ofer letter using the given link!

https://en.wikipedia.org/wiki/Phishing

Click here to reset your password in the next hour or your account will be locked : https://en.wikipedia.org/wiki/Phishing

Regards,

Team CodeAalpha

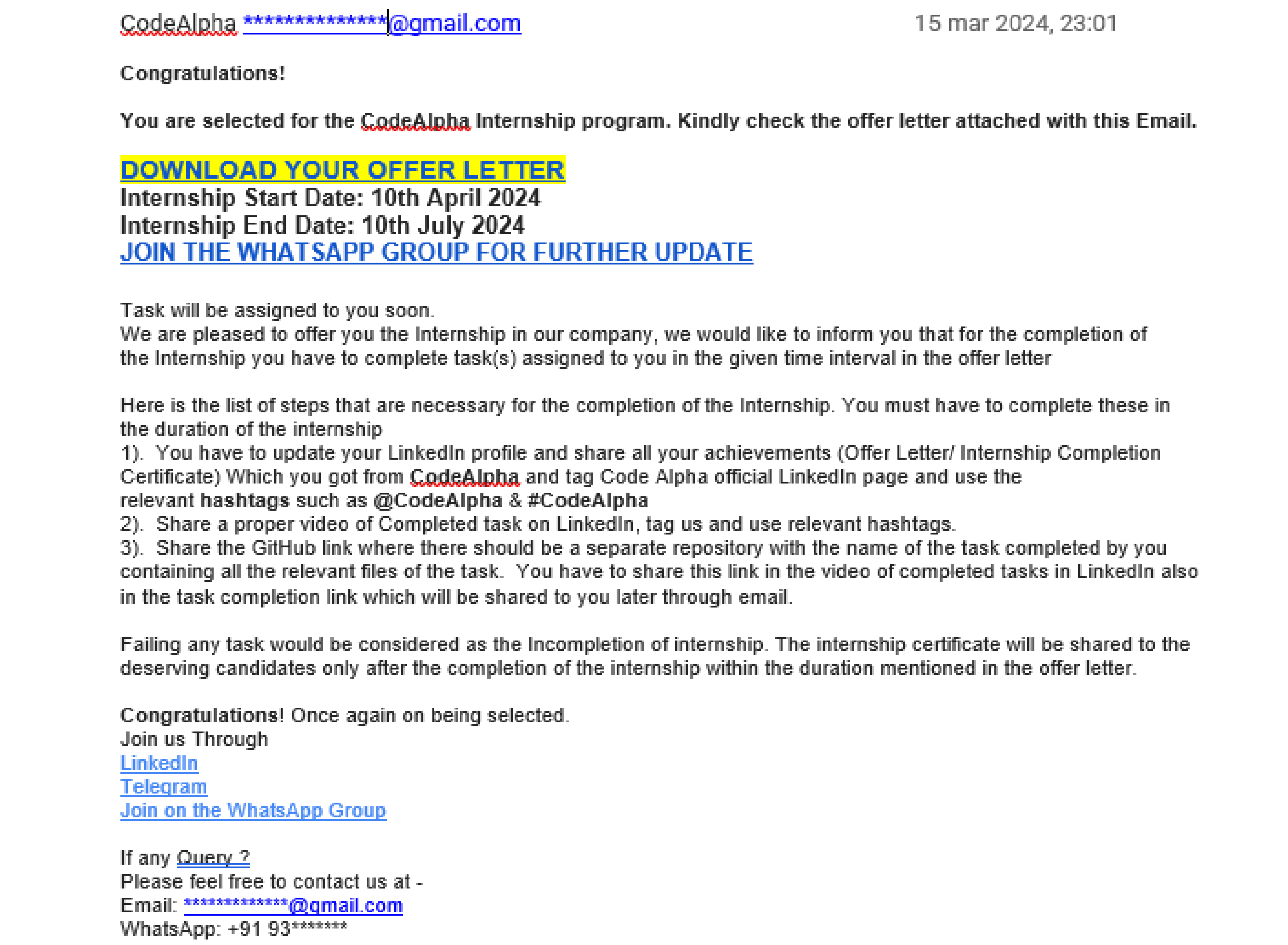
Example of Phishing Mail: Errors in Mail

- The sender's email address is suspicious: CodeAalphaIT@gmail.com. Double ‘a’ in Alpha.
- Spelling errors: "selcted" instead of "selected," "Internsip" instead of "Internship," "account" instead of "an account," "ofer" instead of "offer."
- Inconsistent formatting: The use of excessive capitalization in "YOUR OFER LETTER" and "CREATE A ACCOUNT" is unprofessional.
- Suspicious links: The links provided lead to the Wikipedia page on phishing, indicating potential malicious intent.
- Urgency: The email creates a sense of urgency by emphasizing "immediate action" required to download the offer letter and reset the password.

Example of Phishing Mail: Errors in Mail (contd..)

- Lack of personalization: The email addresses the recipient as "Hello Intern" instead of using their name, indicating a generic or mass-sent message.
- Grammar errors: "Create a account" should be "Create an account," and "Your email with given link" should be "Your email with the given link."
- No official contact information: Legitimate internship programs usually provide official contact information for inquiries or assistance, which is lacking in this email.
- Use of free email service: Legitimate companies typically use their domain-specific email addresses rather than Gmail or other free email services.

Original Mail



CodeAlpha ****************@gmail.com 15 mar 2024, 23:01

Congratulations!

You are selected for the CodeAlpha Internship program. Kindly check the offer letter attached with this Email.

DOWNLOAD YOUR OFFER LETTER
Internship Start Date: 10th April 2024
Internship End Date: 10th July 2024
JOIN THE WHATSAPP GROUP FOR FURTHER UPDATE

Task will be assigned to you soon.
We are pleased to offer you the Internship in our company, we would like to inform you that for the completion of the Internship you have to complete task(s) assigned to you in the given time interval in the offer letter

Here is the list of steps that are necessary for the completion of the Internship. You must have to complete these in the duration of the internship
1). You have to update your LinkedIn profile and share all your achievements (Offer Letter/ Internship Completion Certificate) Which you got from CodeAlpha and tag Code Alpha official LinkedIn page and use the relevant **hashtags** such as **@CodeAlpha** & **#CodeAlpha**
2). Share a proper video of Completed task on LinkedIn, tag us and use relevant hashtags.
3). Share the GitHub link where there should be a separate repository with the name of the task completed by you containing all the relevant files of the task. You have to share this link in the video of completed tasks in LinkedIn also in the task completion link which will be shared to you later through email.

Failing any task would be considered as the Incompletion of internship. The internship certificate will be shared to the deserving candidates only after the completion of the internship within the duration mentioned in the offer letter.

Congratulations! Once again on being selected.
Join us Through
LinkedIn
Telegram
Join on the WhatsApp Group

If any Query ?
Please feel free to contact us at -
Email: ***************@gmail.com
WhatsApp: +91 93********

Phishing Simulation Exercises

- Conduct simulated phishing exercises within your organization to test employees' awareness and response to phishing attacks.
- Provide varying levels of difficulty and sophistication in simulated phishing emails to test employees' ability to discern between genuine and malicious messages.
- Offer feedback and educational resources to employees who fall for simulated phishing emails, reinforcing learning and promoting a culture of cybersecurity awareness and improvement.

Reporting Phishing Attempts

- Encourage employees to report phishing attempts promptly to the appropriate channels, such as IT support or security teams.
- Implement clear reporting procedures and provide guidance on what information to include in reports.
- Ensuring that employees know where and how to report suspicious emails promptly.
- Implement a robust incident response plan to investigate reported phishing attempts swiftly, mitigate potential risks, and prevent further exploitation of organizational resources.

Conclusion

- Phishing attacks continue to evolve, posing a significant threat to individuals and organizations.
- By staying informed, exercising caution, and following best practices, we can collectively mitigate the risks associated with phishing.
- Thank you for completing Phishing Awareness Training. Stay vigilant and help keep our digital environment secure

THANK YOU