# Phishing: A Guide for HR

Phishing is a type of cybercrime where attackers use deceptive tactics to trick individuals into revealing sensitive information, such as passwords or financial details. This presentation aims to educate you on how to identify and avoid phishing attempts, ensuring your personal and professional information stays secure.

by Alamin Elyass

# Common Phishing Tactics

1

### Spoofed Emails

Attackers create emails that mimic legitimate companies or organizations, using similar logos, branding, and email addresses.

2

### Urgency and Fear

Phishing emails often create a sense of urgency or fear, urging you to take immediate action, such as clicking a link or providing personal information.

3

### Social Engineering

Attackers may use social engineering techniques to manipulate their targets, building trust and exploiting human weaknesses to gain access to sensitive information.

4

### Malware Distribution

Phishing emails can deliver malicious software, such as viruses or spyware, to steal data or compromise your device.

# Identifying Phishing Emails

## Suspicious Sender

Check the sender's email address carefully for misspellings or unusual domain names.

Pay attention to the sender's name and whether it aligns with the company or organization it claims to represent.

## Unusual Links

Hover over links in the email to preview the destination URL. If the URL looks different from the expected one or seems suspicious, avoid clicking it.

If the link is asking you to log in, verify the link's authenticity by checking the official website directly.

## Urgent Requests

Be cautious of emails that create a sense of urgency, demanding immediate action or threatening consequences if you don't respond.

Legitimate companies usually don't ask for sensitive information through email and often use secure channels for important communications.

# Protecting Yourself from Phishing

1

### Educate Yourself

Stay informed about phishing tactics and best practices for protecting yourself online.

2

### Be Skeptical

Approach emails with a critical eye, especially those that seem too good to be true or create a sense of urgency.

3

### Use Strong Passwords

Create strong, unique passwords for your online accounts and use a password manager to help you keep track of them securely.

4

### Enable Two-Factor Authentication

Two-factor authentication adds an extra layer of security to your accounts, requiring an additional code or confirmation step to log in.

5

### Keep Software Updated

Ensure that your operating system and software are up to date with the latest security patches to protect against vulnerabilities.

# Real-World Phishing Examples

## Fake Bank Emails

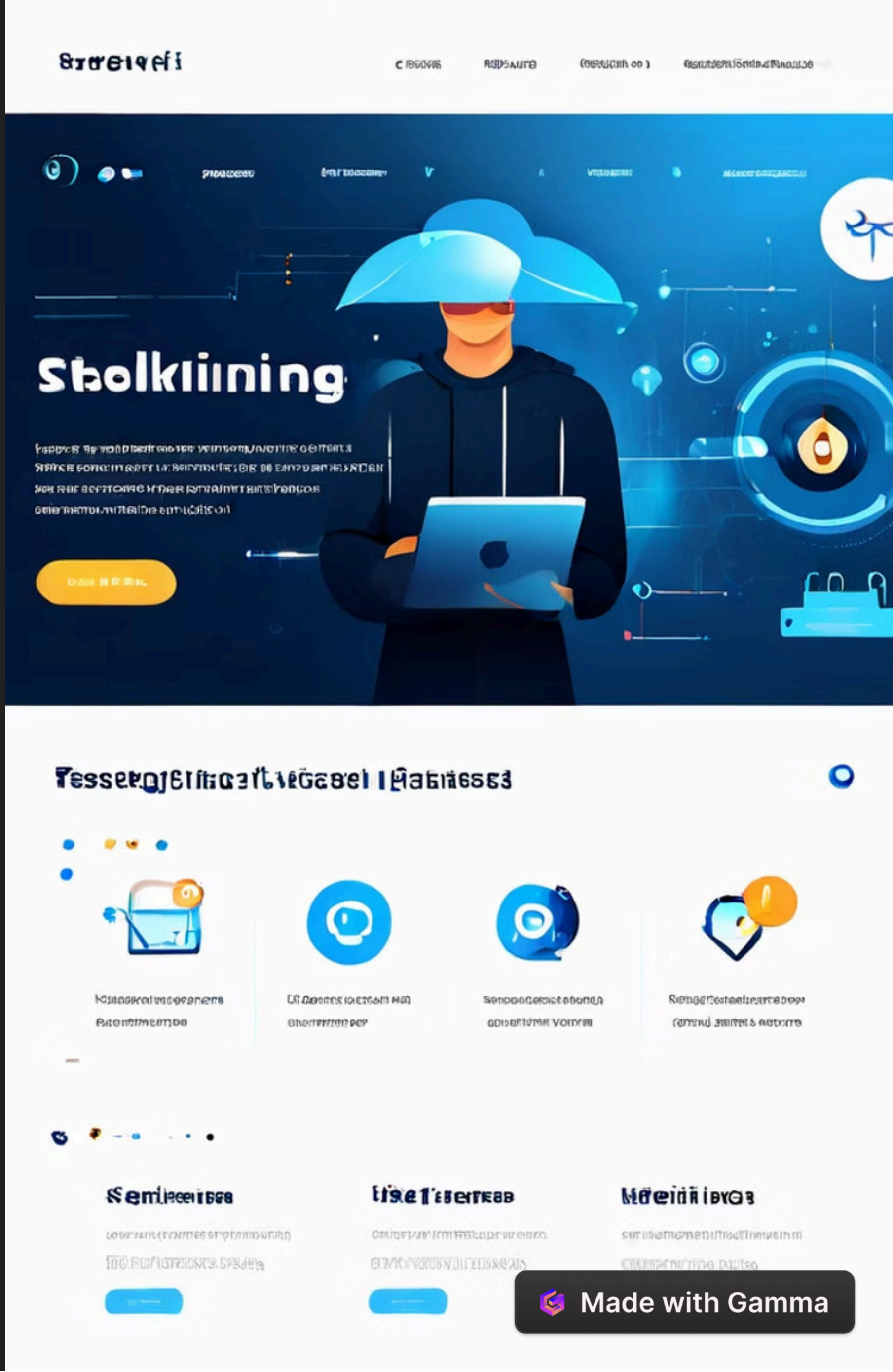
Attackers may send emails that appear to be from your bank, requesting you to update your account information or verify suspicious activity. These emails often contain fake links that redirect you to a phishing website.

## Social Media Scams

Phishing attacks can occur on social media platforms, where attackers may create fake profiles or use legitimate ones to spread malicious links or content.

## Fake Job Offers

Attackers may create fake job postings to collect personal information from unsuspecting job seekers. These postings may request you to submit your resume or complete a fake application form.



# Responding to a Phishing Attempt

1

### Do Not Click Links

Never click on links or attachments in suspicious emails. If you are unsure about an email's legitimacy, do not interact with it.

2

### Do Not Provide Information

Never provide personal information, such as your passwords, credit card numbers, or social security number, in response to a suspicious email.

3

### Report the Email

If you suspect an email is a phishing attempt, report it to your IT department or the appropriate authorities.

4

### Change Your Passwords

If you have accidentally clicked on a link or provided information to a phishing email, change your passwords immediately and contact your bank or credit card company if necessary.

# Reporting Phishing Incidents

| | |
|---|---|
| Company IT Department | Report suspected phishing emails to your company's IT department. They can investigate the incident and take appropriate action. |
| Anti-Phishing Working Group (APWG) | The APWG is a global organization that works to combat phishing and other online threats. You can report phishing incidents to the APWG through their website. |
| Federal Trade Commission (FTC) | The FTC is a government agency that protects consumers from unfair business practices, including phishing scams. You can report phishing incidents to the FTC through their website. |

# Staying Vigilant and Informed

### Be Skeptical

Always be cautious about emails and online communications, especially those that seem suspicious or urgent.

### Use Strong Passwords

Create strong, unique passwords for your online accounts and use a password manager to help you keep track of them securely.

### Stay Updated

Stay informed about phishing tactics and best practices for protecting yourself online. Follow cybersecurity blogs, news sources, and industry reports to stay current.

### Enable Security Features

Enable two-factor authentication on your accounts, use antivirus software, and keep your operating system and software updated.