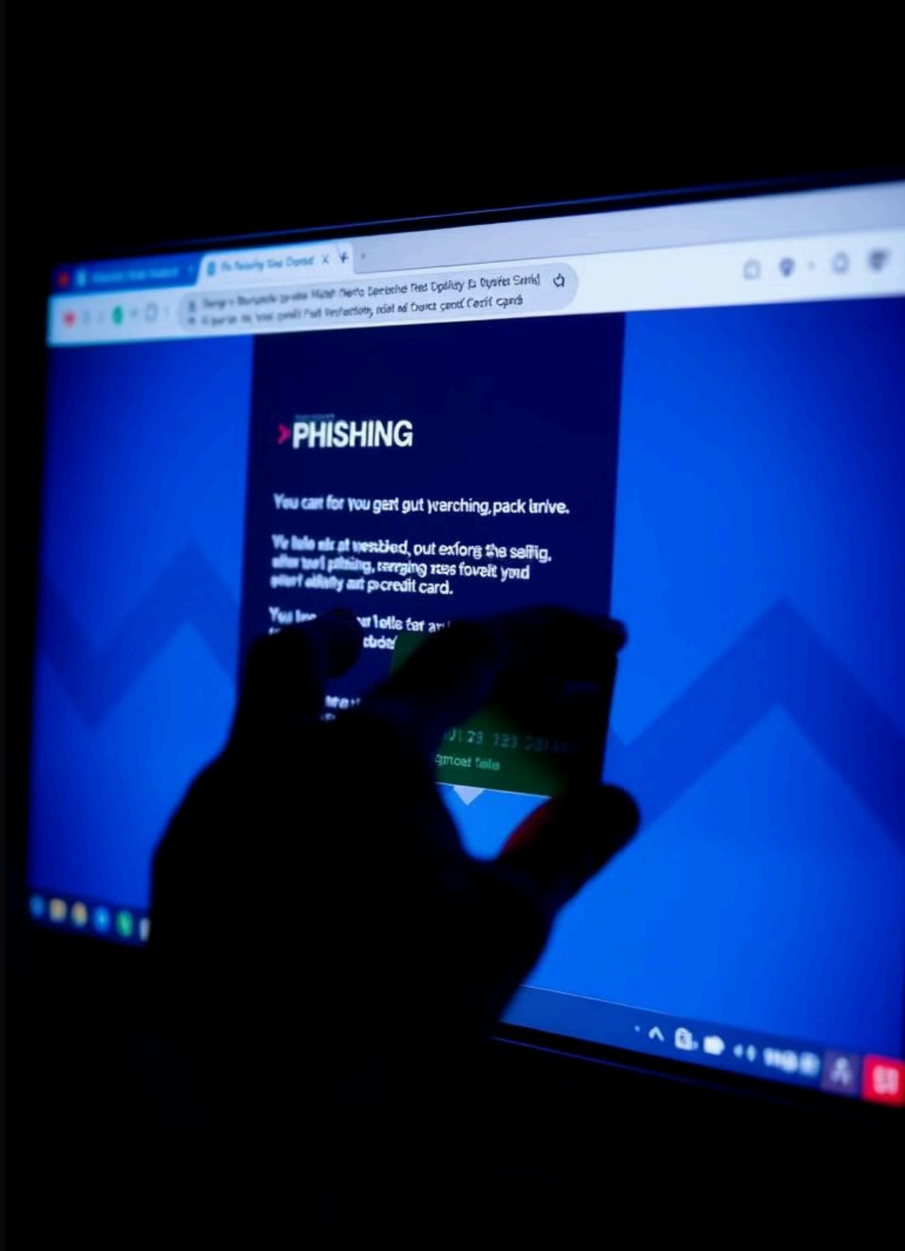
# Phishing: A Guide to Online Security

Phishing is a cybercrime that deceives unsuspecting individuals into revealing sensitive information, often through fraudulent emails, text messages, or websites.

BY: SUNDRAM KUMAR



# Common Phishing Tactics

## Spoofed Emails

Phishers often mimic legitimate organizations or individuals by creating emails that look like they're from a trusted source. This can involve using logos, branding, and email addresses that closely resemble the real thing.

## Urgency and Fear

Phishers use urgent language and create a sense of fear or panic to pressure victims into taking immediate action. They might claim your account is compromised or that you need to update your information immediately.

## Social Engineering

Phishers employ social engineering techniques to manipulate victims into clicking on malicious links or providing sensitive information. They might use emotional appeals, flattery, or create a false sense of trust.

# Recognizing Phishing Attempts

1 **Check the Sender**

Verify the sender's email address and look for inconsistencies or misspelled words in the domain name. If it doesn't match the official website, be wary.

2 **Suspicious Links**

Hover over links before clicking to see the actual URL. If it looks different from the intended destination or appears suspicious, don't click it.

3 **Unusual Requests**

Be cautious about emails or messages asking for sensitive information like passwords, credit card numbers, or personal details. Legitimate companies rarely request such information via email.

4 **Grammar and Spelling**

Phishing attempts often have poor grammar, spelling errors, or unusual formatting. While these aren't foolproof indicators, they can be a red flag.

# Protecting Yourself from Phishing

### Strong Passwords

Use unique and complex passwords for all your accounts. Avoid using the same password for multiple websites.

### Be Cautious with Emails

Don't open suspicious emails, even if they appear to be from someone you know. Verify the sender before clicking on any links or attachments.

### Check Website Security

Look for the HTTPS protocol in the address bar and a padlock icon to ensure the website is secure. Be cautious of websites with outdated or missing security features.

### Be Aware of Text Messages

Be wary of texts that ask for personal information or direct you to unfamiliar websites. Don't reply to messages that appear suspicious.

# Phishing Targeting Businesses

1

## CEO Fraud

Phishers target executives by impersonating trusted contacts or vendors. They may request wire transfers or other financial actions, causing significant financial losses.

2

## Data Breaches

Phishing emails targeting employees can compromise sensitive data like customer information, financial records, and intellectual property. This can damage reputation and lead to legal consequences.

3

## Malware Infection

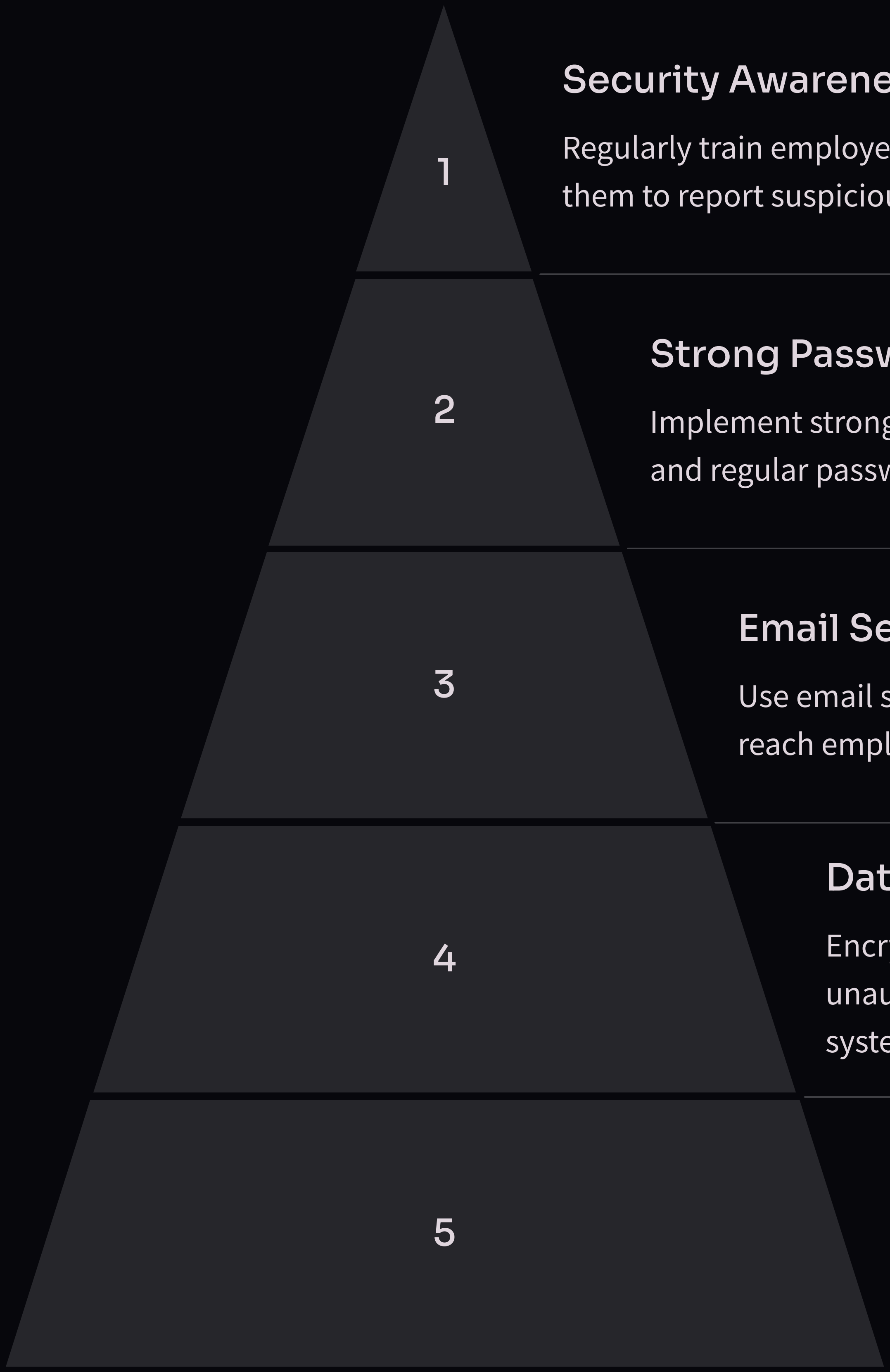
Phishing emails often contain malicious attachments or links that infect computers with malware. This can steal data, disrupt operations, and require costly remediation efforts.

4

## Business Disruption

Phishing attacks can cause widespread disruption to business operations. Employees may be unable to access critical systems or data, leading to delays and lost productivity.

# Preventing Phishing in the Workplace



### Security Awareness Training

Regularly train employees on identifying and preventing phishing attacks. Encourage them to report suspicious emails and messages.

### Strong Password Policies

Implement strong password policies, including the use of complex passwords and regular password changes. Encourage the use of a password manager.

### Email Security Filters

Use email security filters to block spam and phishing emails before they reach employees' inboxes. Implement layered security measures.

### Data Encryption

Encrypt sensitive data both at rest and in transit to prevent unauthorized access. Use multi-factor authentication for critical systems.

### Incident Response Plan

Develop a clear incident response plan to handle phishing attacks effectively. This plan should outline steps for detection, containment, and remediation.

# Reporting Phishing Incidents

1

## Report to Your Organization

If you receive a phishing email or message at work, immediately report it to your IT department or security team.

2

## Report to Authorities

In some cases, you may also need to report phishing incidents to law enforcement agencies, such as the FBI or local police.

3

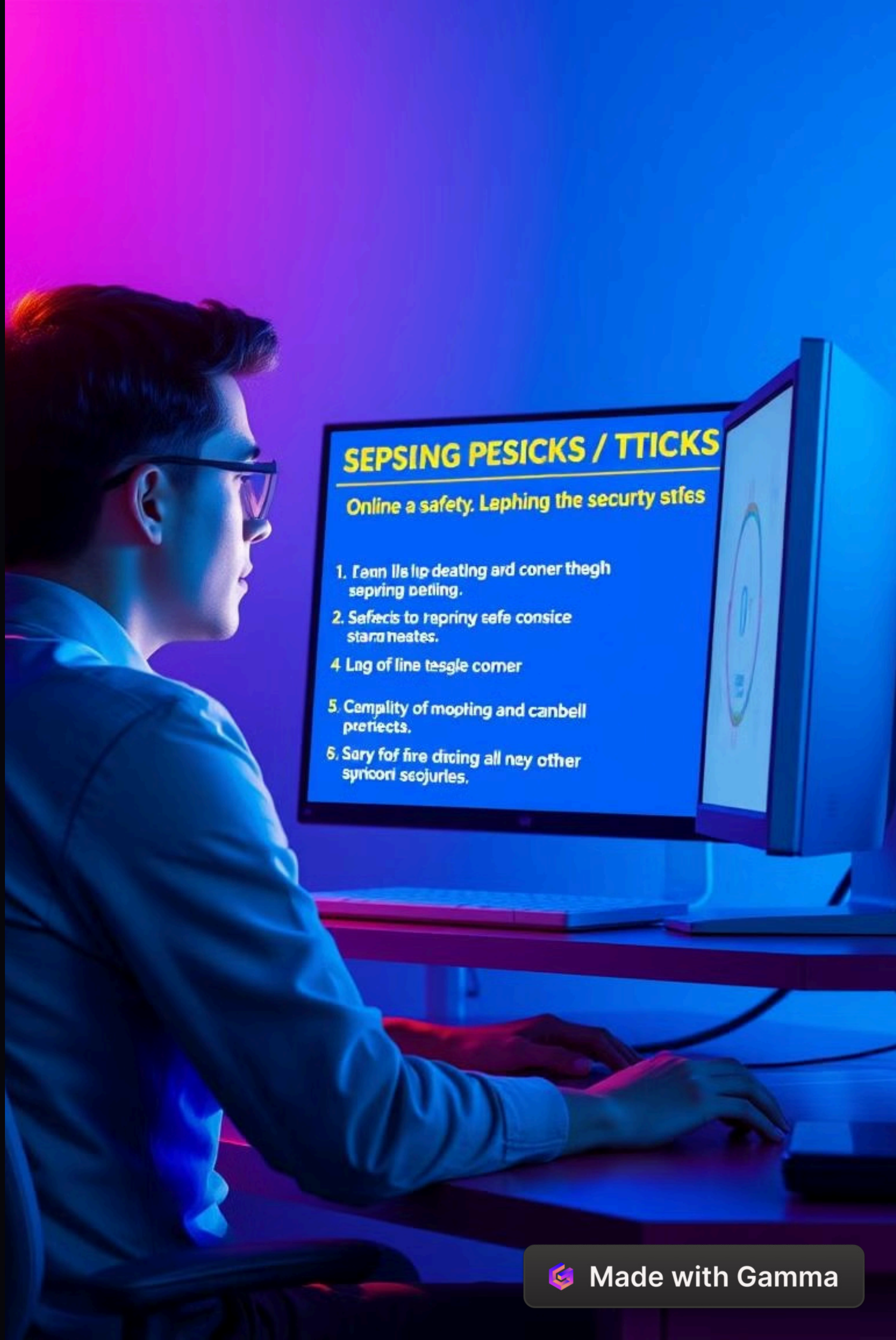
## Report to the Service Provider

If you encounter phishing on a specific website or platform, report it to the service provider. They may be able to take action to remove the phishing content.

# Conclusion and Resources

Phishing is a persistent threat, but by staying vigilant and implementing appropriate safeguards, we can protect ourselves and our organizations from falling victim to these attacks. The resources below can provide valuable insights and guidance to enhance your online security.

- US-CERT: [https://www.us-cert.gov/](https://www.us-cert.gov/)
- Anti-Phishing Working Group: [https://www.antiphishing.org/](https://www.antiphishing.org/)
- National Cyber Security Alliance: https://staysafeonline.org/


SEPSING PESICKS / TTICKS
Online a safety. Lephing the securty stfes
1. Ƭenn Ils lip deating ard coner thegh sepving peting.
2. Safecis to repriny sefe consice starmeates.
4 Lng of line tesgle comer
5. Compilty of mopting and canbell pretiects.
6. Sary fof fire dircing all ney other synicori seojurles.