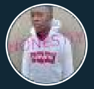
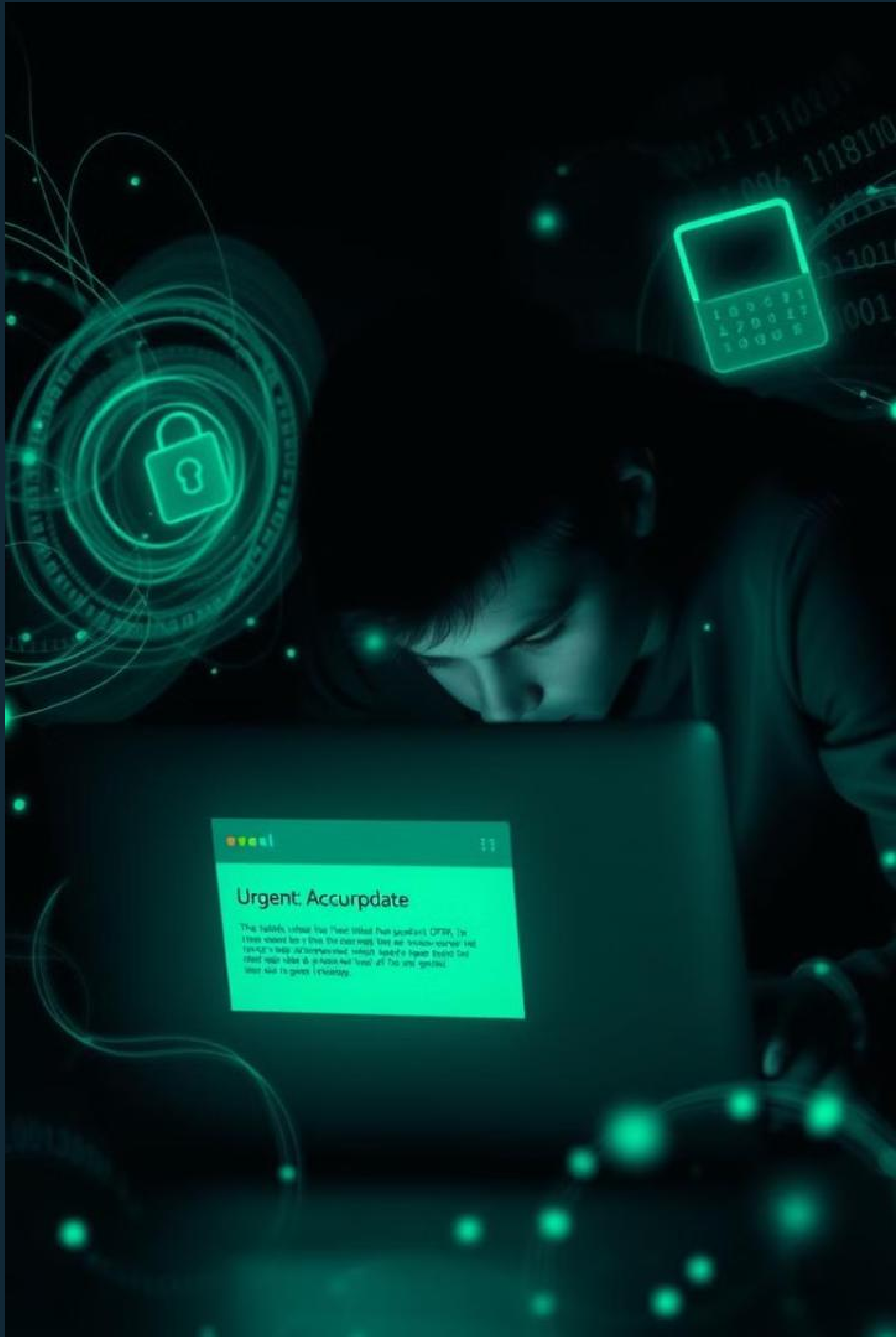
# Understanding Phishing Attacks

Phishing is a type of social engineering attack where cybercriminals attempt to trick individuals into revealing sensitive information or performing actions that compromise security. This presentation will equip you with the knowledge to identify and avoid phishing threats.



by Theoneste Dufitimana



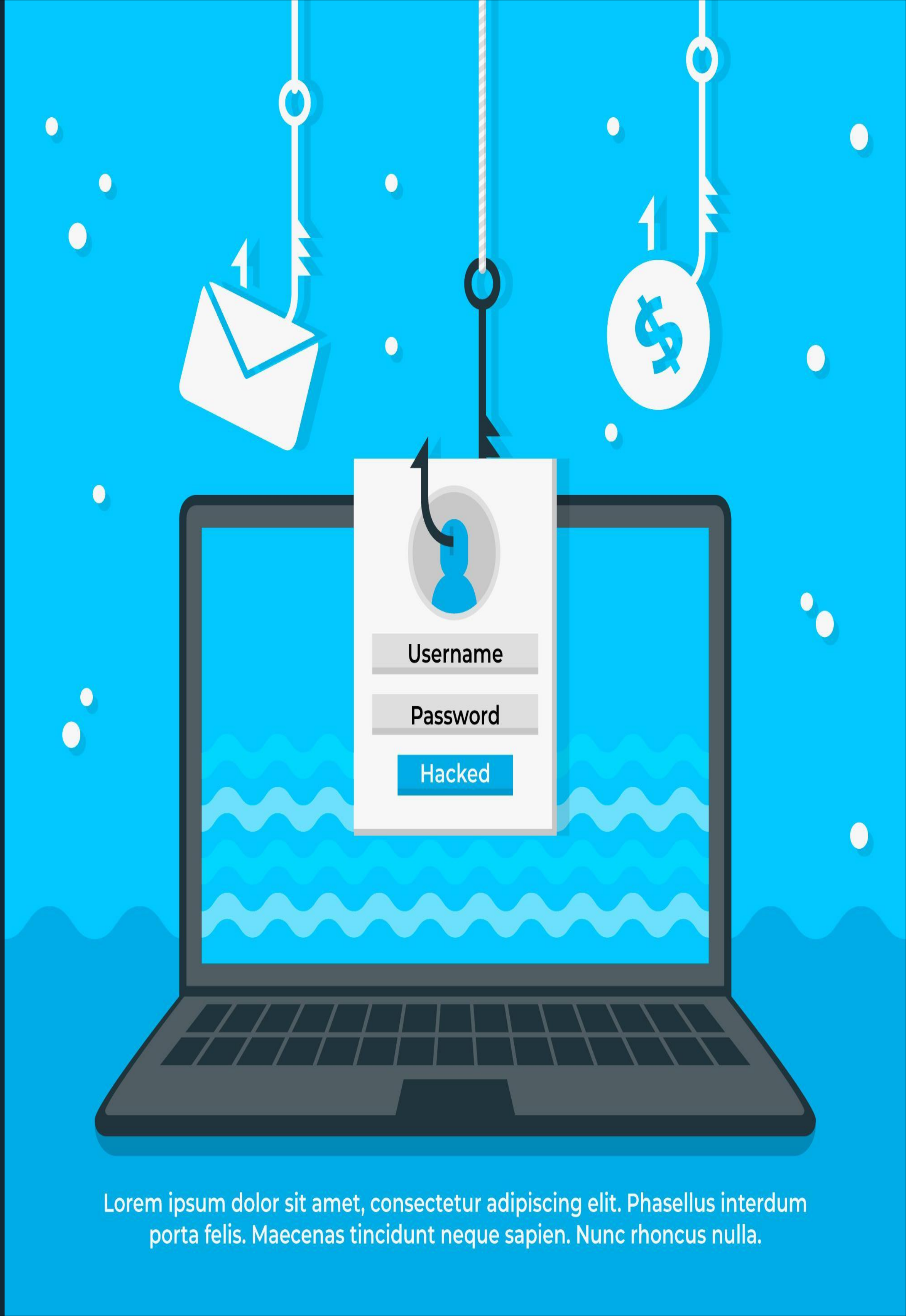
# How Does Phishing Work?

In a phishing attack, an attacker often:

1. Creates a fake message or website that looks legitimate.

2. Uses urgent language or fear tactics to prompt immediate action.

3 . Tricks the victim into clicking on a link, downloading a file, or entering personal information.


Username
Password
Hacked
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus interdum porta felis. Maecenas tincidunt neque sapien. Nunc rhoncus nulla.

# Common Phishing Tactics

1 **Impersonation**

Phishers often impersonate trusted organizations or individuals to appear legitimate.

2 **Urgency and Fear**

Phishing emails often create a sense of urgency or threaten consequences to pressure victims.

3 **Malicious Links and Attachments**

Phishing messages may contain links or attachments designed to steal data or infect devices.

4 **Social Engineering**

Phishers manipulate human psychology to exploit victims' trust and curiosity.

# Identifying Phishing Emails

### Sender Address

Look for subtle variations in the sender's email address that don't match the claimed source.

### Generic Greetings

Phishing emails often use generic greetings like "Dear customer" instead of personalized salutations.

### Poor Grammar and Spelling

Phishing messages frequently contain grammatical errors and typos, indicating a lack of quality control.

# Phishing Website Red Flags

1

### Suspicious URLs

Phishing sites often use domain names that are slightly different from the legitimate website.

2

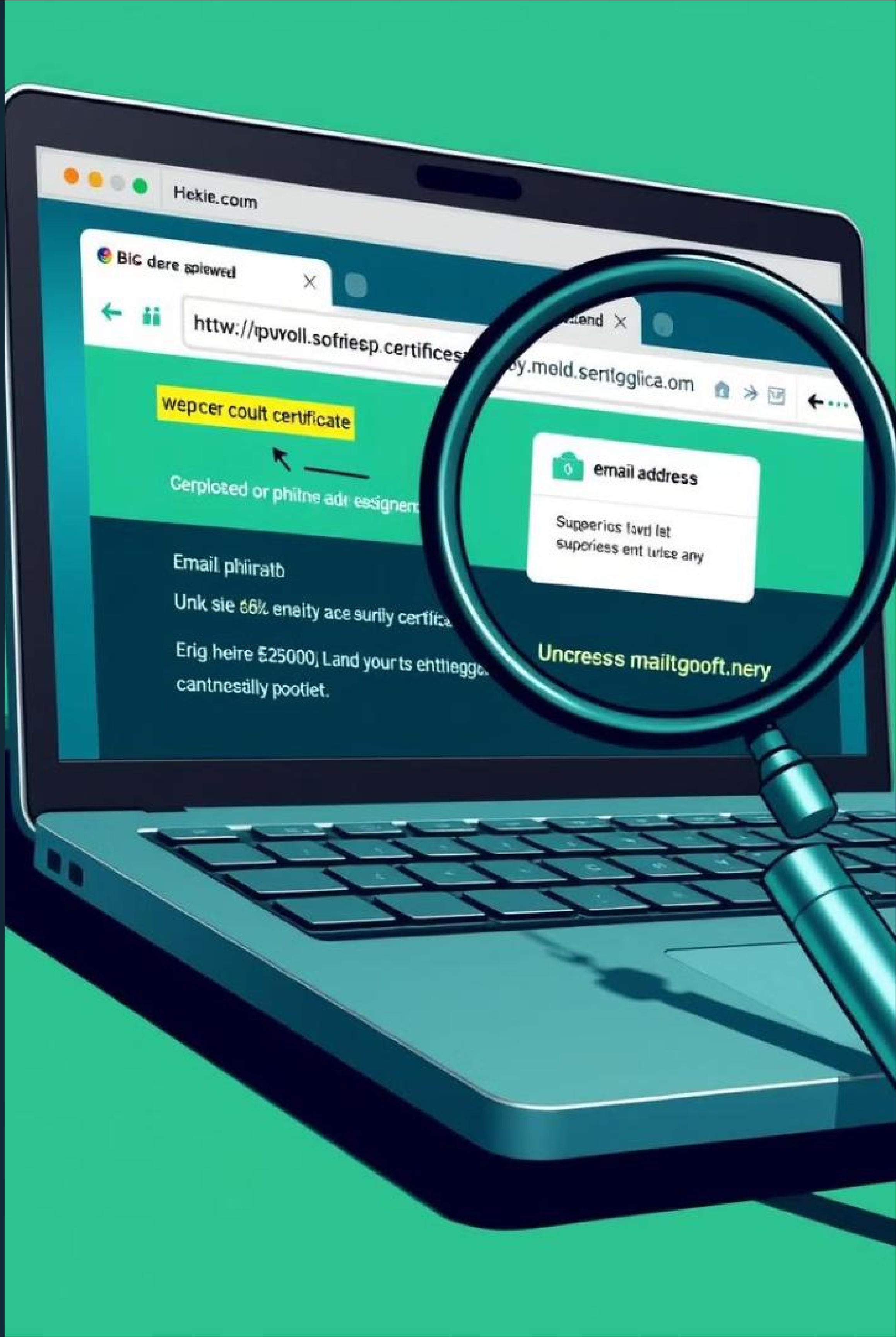
### Lack of HTTPS

Legitimate websites typically have a secure "https://" prefix, which is missing on phishing sites.

3

### Poor Design

Phishing sites may have a cluttered, unprofessional, or outdated appearance compared to the real website.



# Social Engineering Awareness

### Observe

Be aware of your surroundings and potential social engineering attempts.

### Analyze

Critically evaluate requests for information or action, even from trusted sources.

### Protect

Safeguard your personal and organizational information to prevent exploitation.

# Protecting Yourself from Phishing

1

### Be Cautious

Approach all unsolicited messages and requests with skepticism.

2

### Verify Authenticity

Independently confirm the legitimacy of any suspicious communication or website.

3

### Utilize Security Features

Enable two-factor authentication and keep software and devices up-to-date.

# Reporting Suspected Phishing

## Forward Phishing Emails

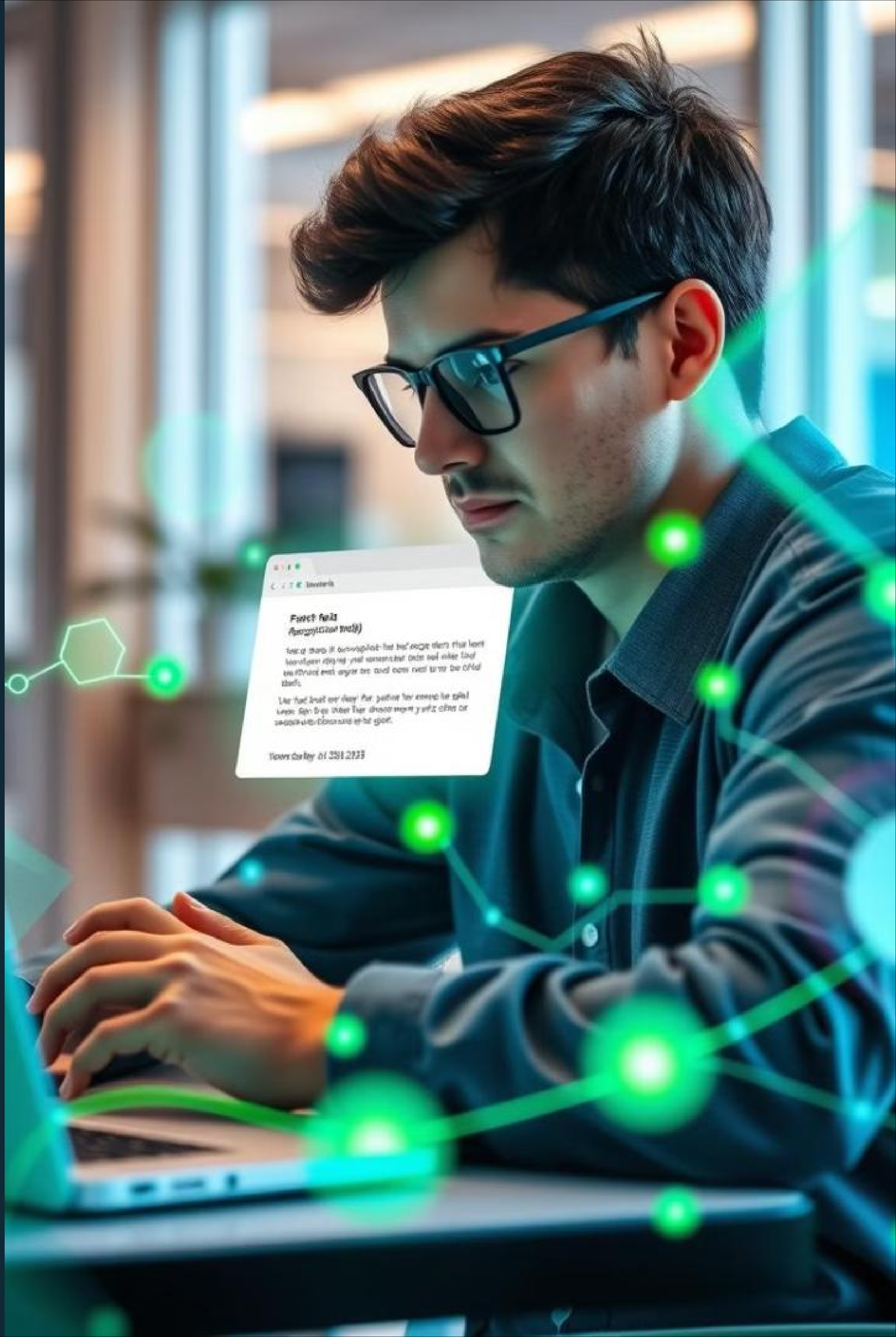
Report suspicious emails to your organization's IT or security team.

## Flag Phishing Websites

Notify the relevant authorities or website owners about suspected phishing sites.

## Provide Feedback

Share your experience and insights to help improve phishing detection and prevention.



# Conclusion and Key Takeaways

1

### Stay Vigilant

Continuously be on the lookout for phishing attempts and social engineering tactics.

2

### Educate Yourself

Regularly update your knowledge on the latest phishing trends and best practices.

3

### Report Incidents

Notify the appropriate authorities and share your experiences to aid in the fight against phishing.