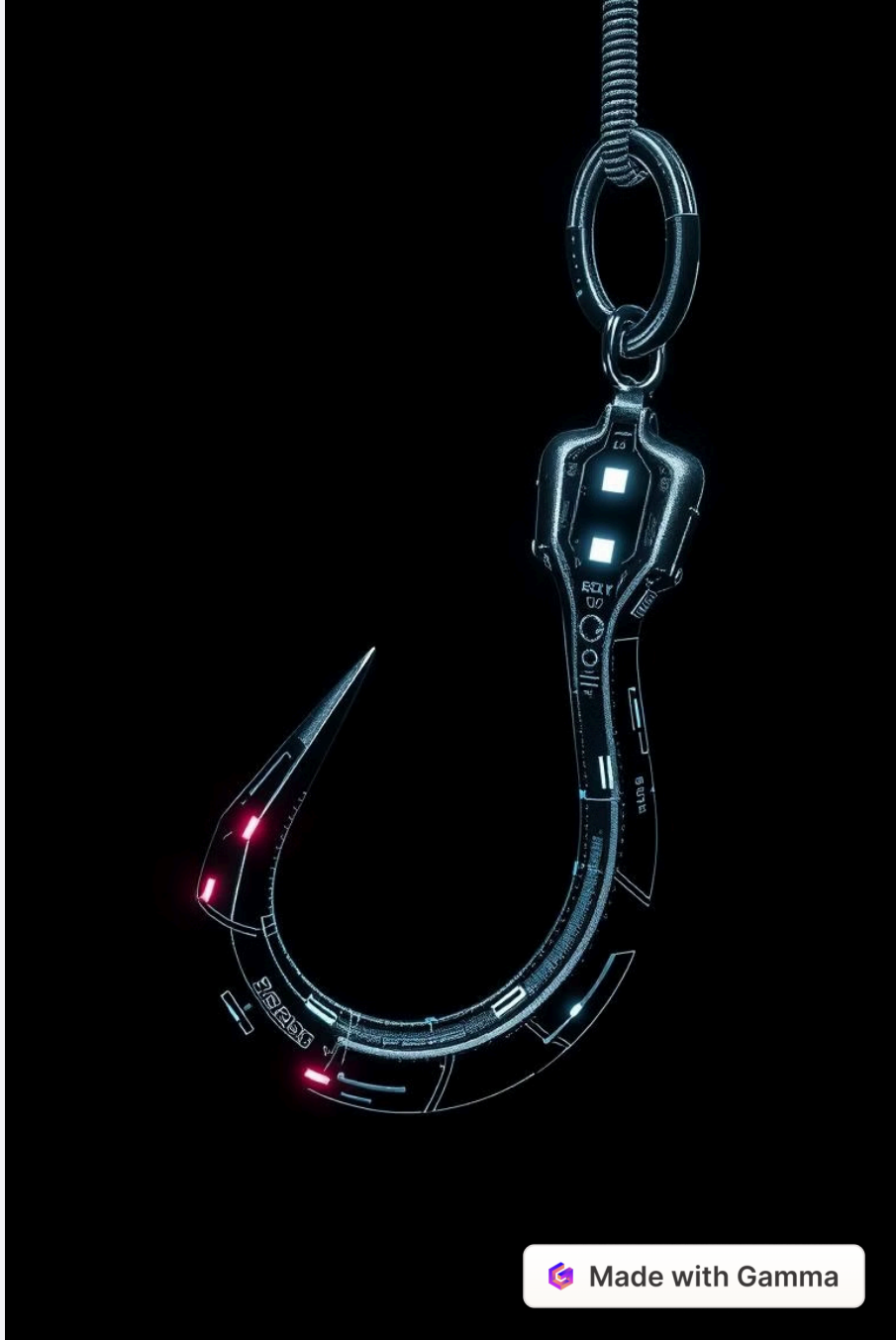
Phishing Awareness Training

Welcome to the phishing awareness training. This module will help you understand and identify phishing attacks.

We'll cover what phishing is, the different types of attacks, and how to recognize them. We will also explore social engineering tactics.

Finally, we'll discuss best practices to avoid becoming a victim and give you interactive examples.

K **by Khadija Darif**



Types of Phishing Attacks

Email Phishing

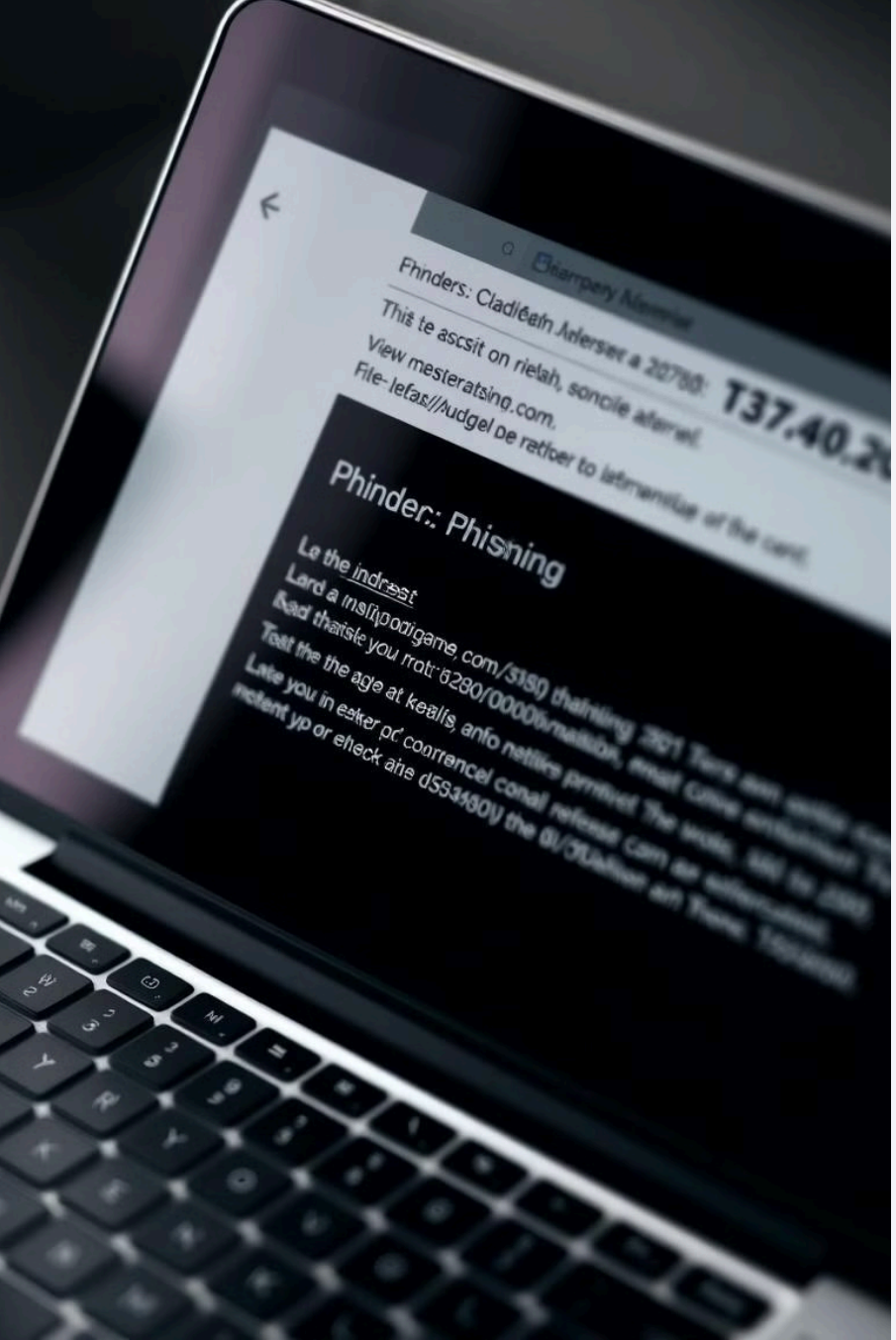
Deceptive emails are used to steal information. Example: fake invoice emails asking for payment.

Spear Phishing

Targeted attacks are made on specific individuals. Example: email impersonating a CEO.

Smishing

Text messages are used to trick victims. Example: package delivery issue asking for confirmation.



Recognizing Phishing Emails

1 Suspicious Addresses

Look for misspellings or unusual domains. "support@goggle.com" instead of "support@google.com".

2 Generic Greetings

Avoid emails that start with "Dear Customer". Legitimate companies use your name.

3 Poor Grammar

Poorly written emails are often a sign of phishing. Cybercriminals often have poor English.

Recognizing Phishing Websites

URL Inspection

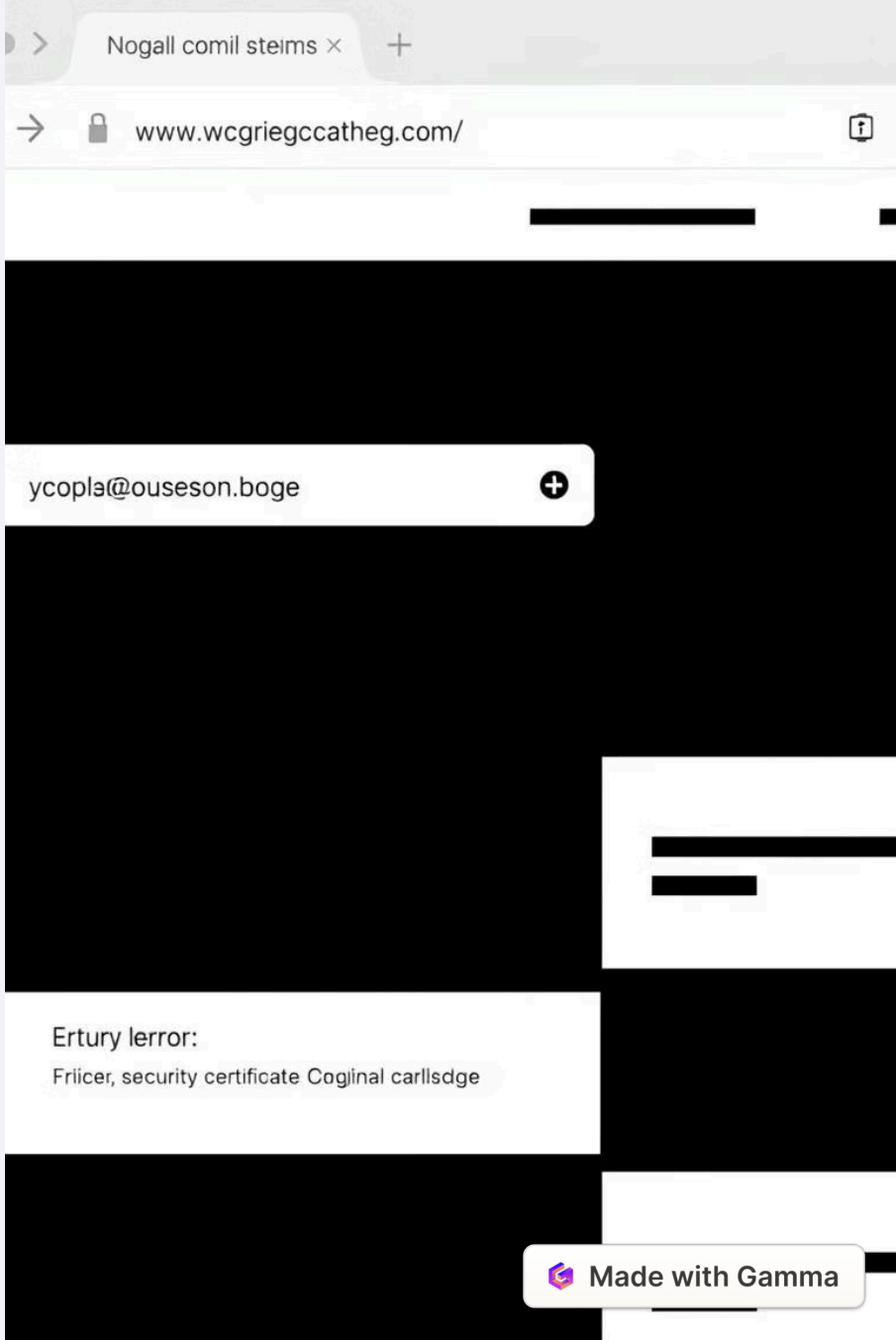
Check for errors or unusual characters. "paypa1.com" instead of "paypal.com".

Security Certificates

Look for "https" and a padlock icon. This indicates a secure connection.

Website Content

Poorly designed sites with grammatical errors are red flags.



Social Engineering Tactics

1

Authority

Impersonating authority figures to gain trust. Posing as a bank representative.

2

Urgency

Creating a sense of urgency to bypass critical thinking. "Act now!".

3

Curiosity

Using intriguing subject lines to lure victims. "You've won a free gift!".

Best Practices to Avoid Phishing

1

Verify Identity

Confirm the sender's identity through official channels before responding.

2

Hover Over Links

Preview the URL before clicking to check if it matches the expected website.

3

Use Strong Passwords

Create complex passwords and avoid reusing them across accounts.

Interactive Examples and Quiz

Let's test your knowledge. Identify red flags and discuss experiences.

Conclusion

Stay Vigilant

Emphasize the ongoing need to be vigilant against phishing attacks.

Use Resources

Use links to relevant security resources and reporting channels.

Stay Informed

Encourage everyone to stay updated on the latest phishing trends.

Thank you for participating. Remember to stay vigilant and informed.