understanding

PHISHING ATTACKS

a guide to cybersecurity awareness

Presented by: **Sheikh Iyad**
Cybersecurity Workshop - CodeAlpha
15th December 2025

WHAT IS **PHISHING**?

Phishing is a form of social engineering where attackers deceive individuals into providing personal information, such as passwords or financial details. It often spreads through emails, messages (SMS), and phone calls, posing significant cybersecurity risks.

Example: A fake email from your bank asking you to verify your account details.

HOW DOES **PHISHING** WORK?

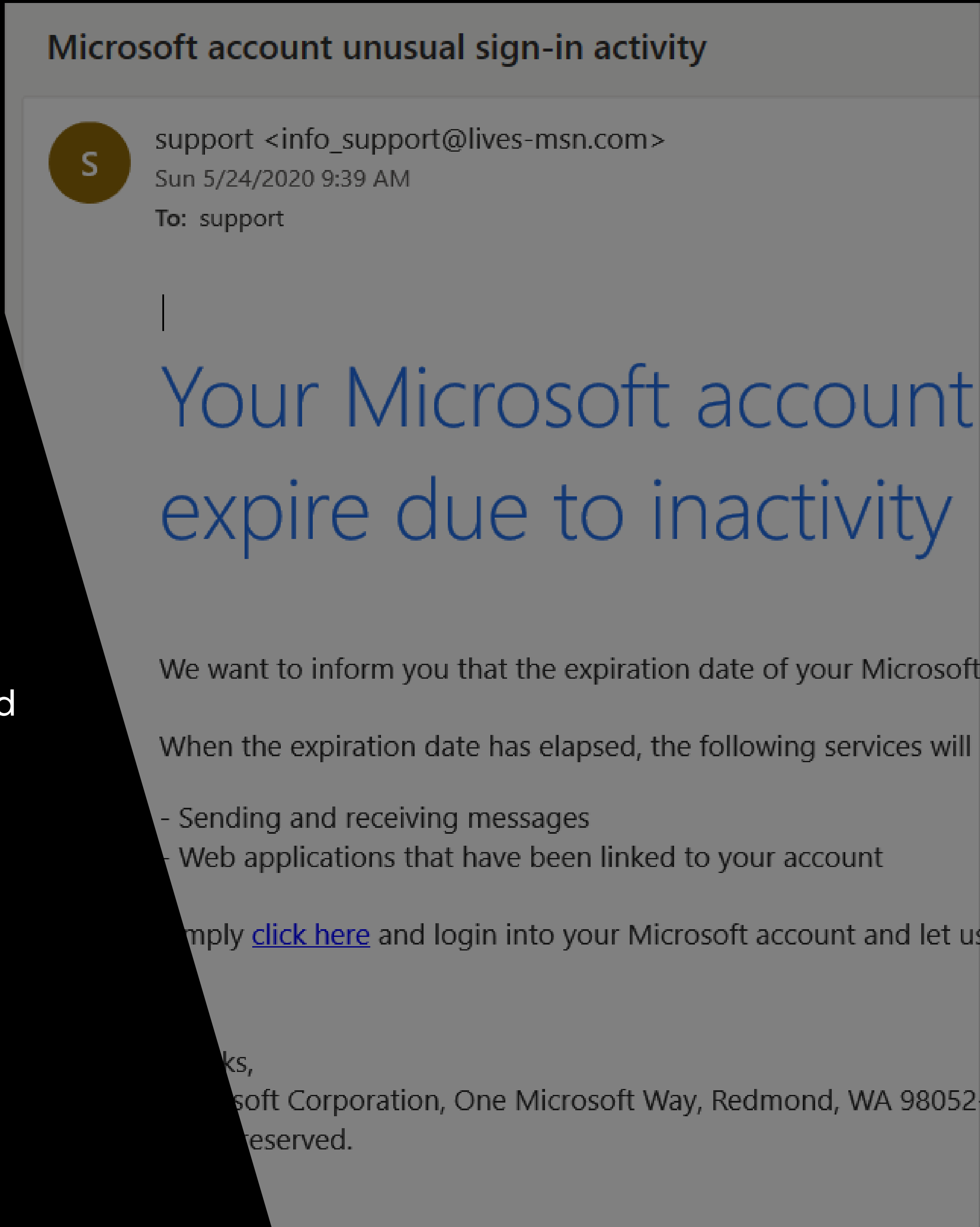
The attacker uses these **common phases** to deceive the victim:

1. Bait
2. Hook
3. Capture

1. Baiting: The attacker prepares an email or SMS and sends it to the victim.

2. Hooking: The attacker convinces his victim to click on a specific link where all the data can be entered.

3. Capturing: When the victim enter their data on the false link, all the data is captured and sent to the attacker.



Microsoft account unusual sign-in activity

S support <info_support@lives-msn.com>
Sun 5/24/2020 9:39 AM
To: support

Your Microsoft account expire due to inactivity

We want to inform you that the expiration date of your Microsoft

When the expiration date has elapsed, the following services will

- Sending and receiving messages
- Web applications that have been linked to your account

mply click here and login into your Microsoft account and let us

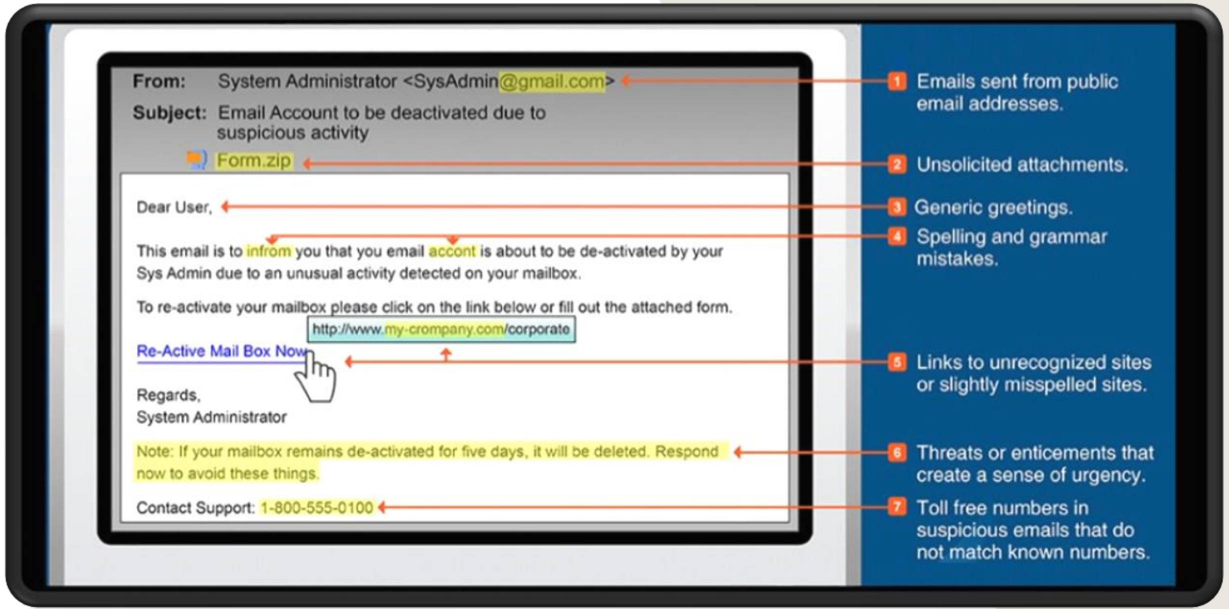
ks,
soft Corporation, One Microsoft Way, Redmond, WA 98052
eserved.

HOW TO RECOGNIZE **PHISHING?**

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. You might get an unexpected email or text message that looks like it’s from a company you know or trust, like a bank or a credit card or utility company. Or maybe it’s from an online payment website or app. The message could be from a scammer, who might be demanding these.

To spot a phishing email, check for:

- <u>bad grammar</u> and <u>spelling mistakes</u>.
- Emails with an <u>Unfamiliar Greeting</u> or <u>Salutation.</u>
- Suspicious Attachments (files like .exe, .zip, .7z, .bat)
- Emails Demanding Urgent Action



From: System Administrator <SysAdmin@gmail.com>
Subject: Email Account to be deactivated due to suspicious activity
Form.zip

Dear User,

This email is to infrom you that you email accont is about to be de-activated by your Sys Admin due to an unusual activity detected on your mailbox.

To re-activate your mailbox please click on the link below or fill out the attached form.

http://www.my-crompany.com/corporate

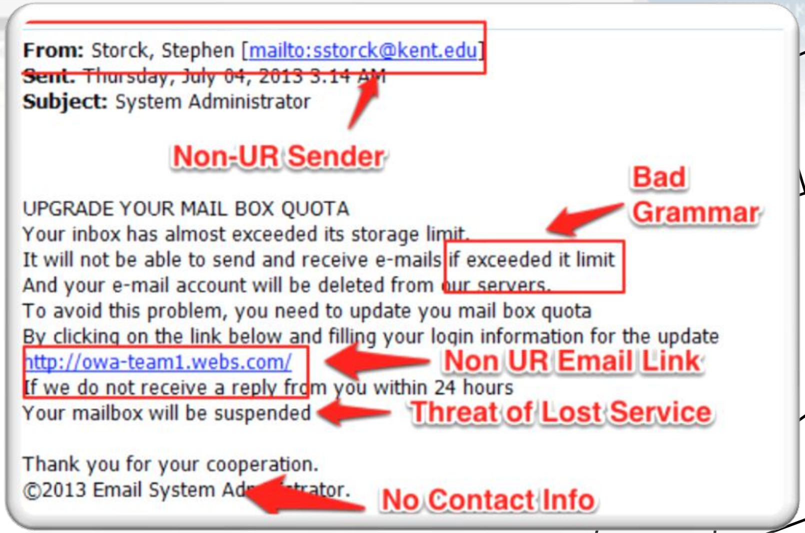
Re-Active Mail Box Now

Regards,
System Administrator

Note: If your mailbox remains de-activated for five days, it will be deleted. Respond now to avoid these things.

Contact Support: 1-800-555-0100

1. Emails sent from public email addresses.
2. Unsolicited attachments.
3. Generic greetings.
4. Spelling and grammar mistakes.
5. Links to unrecognized sites or slightly misspelled sites.
6. Threats or enticements that create a sense of urgency.
7. Toll free numbers in suspicious emails that do not match known numbers.



From: Storck, Stephen [mailto:sstorck@kent.edu]
Sent: Thursday, July 04, 2013 3:14 AM
Subject: System Administrator

UPGRADE YOUR MAIL BOX QUOTA
Your inbox has almost exceeded its storage limit.
It will not be able to send and receive e-mails if exceeded it limit
And your e-mail account will be deleted from our servers.
To avoid this problem, you need to update you mail box quota
By clicking on the link below and filling your login information for the update
http://owa-team1.webs.com/
If we do not receive a reply from you within 24 hours
Your mailbox will be suspended

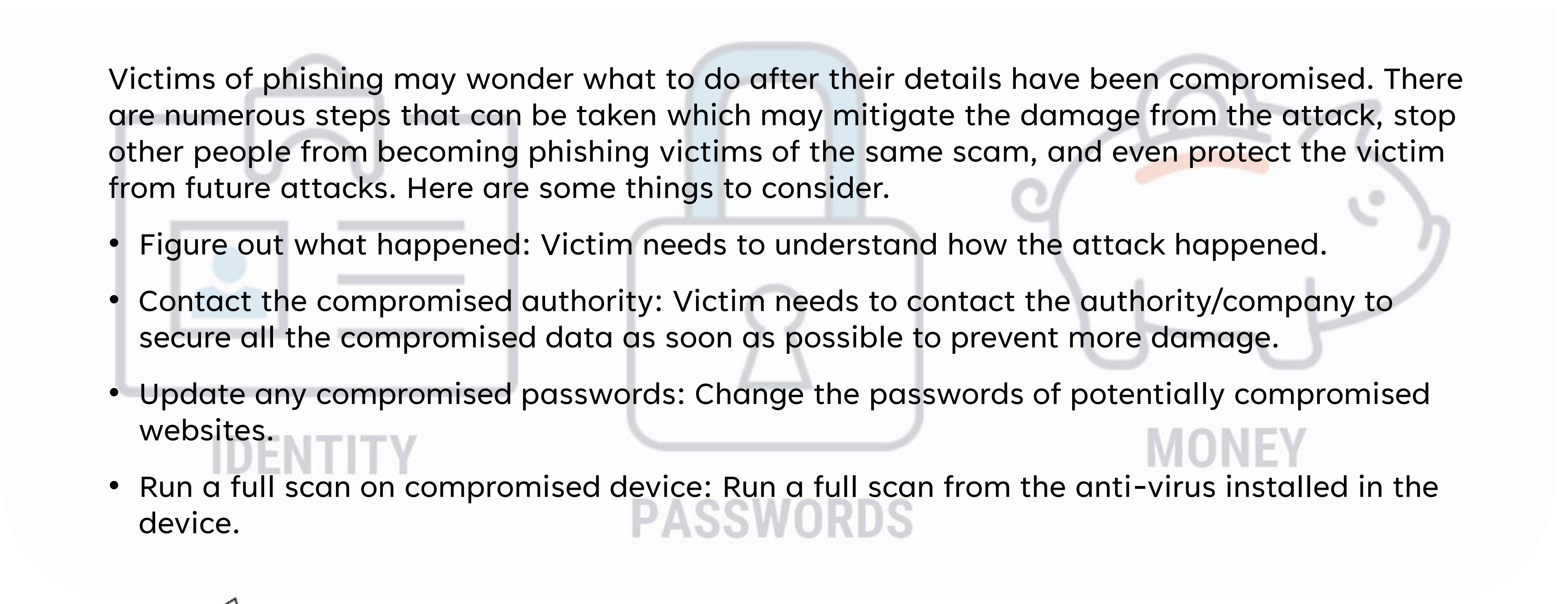
Thank you for your cooperation.
©2013 Email System Administrator.

AVOIDING **PHISHING** EMAILS

Your email spam filters might keep many phishing emails out of your inbox. But scammers are always trying to outsmart spam filters, so extra layers of protection can help. Here are four ways to protect yourself from phishing attacks.

- Avoid emails from bank as many as you can, visit your local bank if there’s any action required.
- Visit official sites directly and look if any action is required.
- Protect your computer by using security software.
- Protect your cell phone by setting software to update automatically.
- Protect your accounts by using multi-factor authentication.
- Protect your data by backing it up.

WHAT TO DO IF YOU GOT **PHISHED**?



Victims of phishing may wonder what to do after their details have been compromised. There are numerous steps that can be taken which may mitigate the damage from the attack, stop other people from becoming phishing victims of the same scam, and even protect the victim from future attacks. Here are some things to consider.

- Figure out what happened: Victim needs to understand how the attack happened.
- Contact the compromised authority: Victim needs to contact the authority/company to secure all the compromised data as soon as possible to prevent more damage.
- Update any compromised passwords: Change the passwords of potentially compromised websites.
- Run a full scan on compromised device: Run a full scan from the anti-virus installed in the device.

CONCLUSION

Phishing attacks are one of the most common cyber threats today, targeting individuals and organizations alike. The key to staying protected is **awareness and vigilance**.
By recognizing phishing attempts and understanding their tactics, you can safeguard your personal information and help prevent cybercrime.

Key Takeaways:

- **Think before you click** – Avoid suspicious links and attachments.
- **Verify the source** – Always double-check emails and messages from unknown senders.
- **Secure your accounts** – Use strong passwords and enable multi-factor authentication (MFA).
- **Stay updated** – Be aware of the latest phishing techniques.

Remember, **cybersecurity is a shared responsibility**. Stay informed, stay alert, and help spread awareness to keep the digital world safer for everyone.

Thank you