

Deploying Discreet Infrastructure For

Targeted Phishing Campaigns



#Whoami

Sreehari Haridas

- Cyber Security Engineer, UST Global TVM.
- Bug Bounty Hunter
- Capture The Flag Player
- Got 50+ Hall of fames from Different companies.
- 6th Place Globally in Hackthebox.eu Capture The Flag Platform.
- Core member at Defcon Trivandrum. (<https://dc0471.org>)
- Operator at Red Team Village. (<https://redteamvillage.org>)
- Volunteer at Kerala Police Cyberdome.
- <https://twitter.com/sr33h4ri>



Outline

- ❖ Phishing
- ❖ Phishing infrastructure setup
- ❖ Gophish setup
- ❖ Identify the phishing email
- ❖ Preventing from phishing attacks



What is Phishing?

- ❖ Phishing can be explained as an activity, which involves sending emails from seemingly reputable sources with the purpose to obtain personal information or influence email receivers.
- ❖ Phishing practices combines both social engineering and technical skills.
- ❖ Phishing attacks varies in its form, it could be an attachment within the email that loads malicious software into the computer or it could be a link to an illicit website.



Types of Phishing

- ❖ Spear Phishing
- ❖ Whaling
- ❖ Clone Phishing
- ❖ Voice Phishing
- ❖ SMS Phishing



Most common methods of phishing

- ❖ Spoofed Login Pages
- ❖ Impersonation
- ❖ Malicious attachments
- ❖ Messenger apps
- ❖ Phishing with shared files



Typical framework of phishing attacks

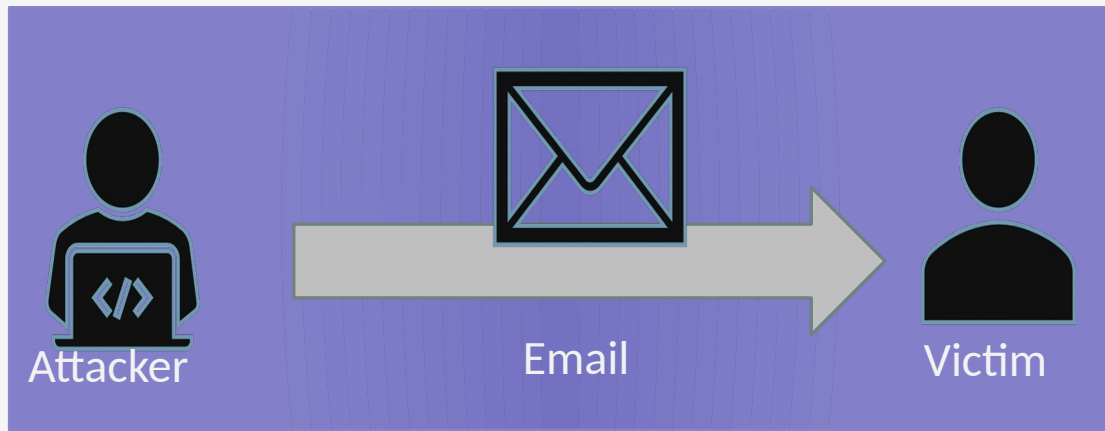


Figure 1: Victim receives phishing email

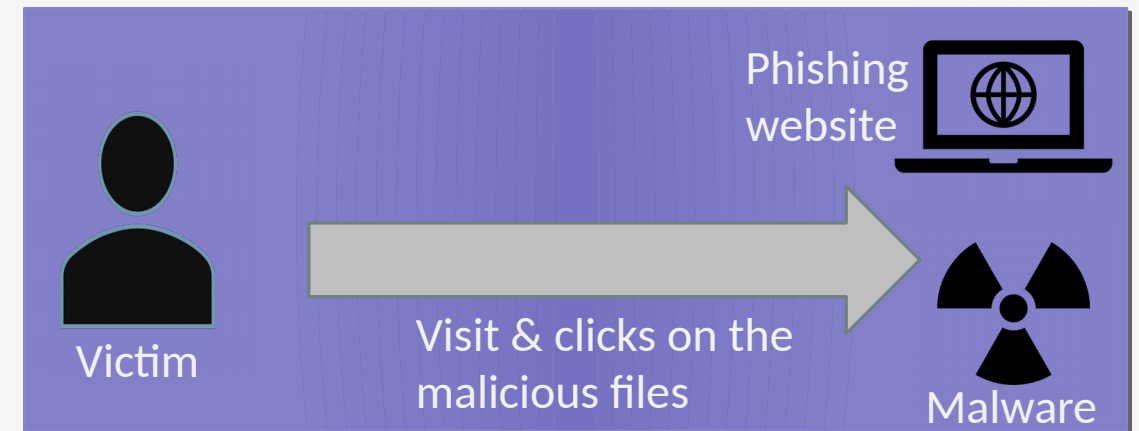
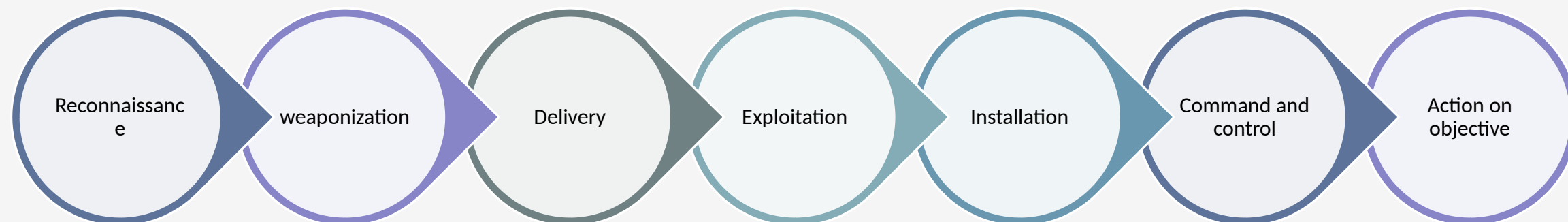


Figure 2: Victim fall into the suggested action

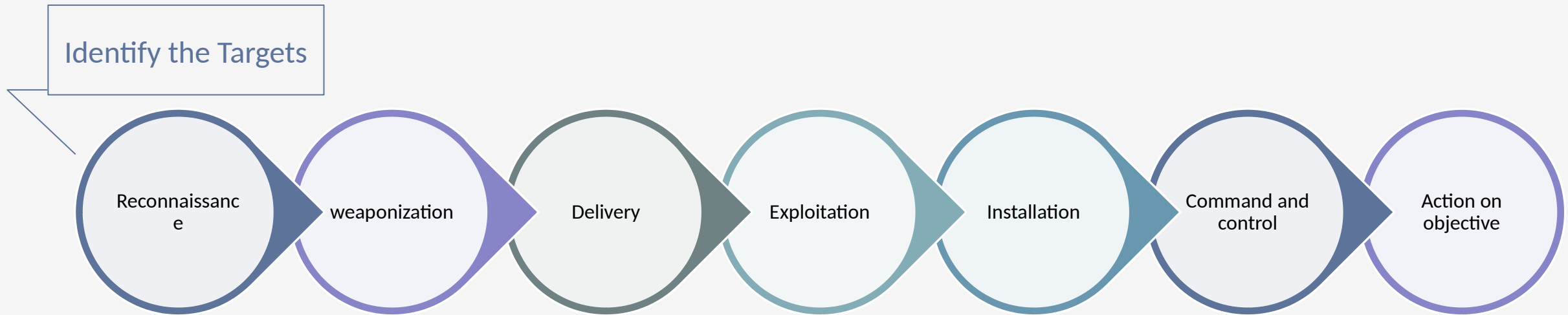


Figure 3: Critical information/Data stolen

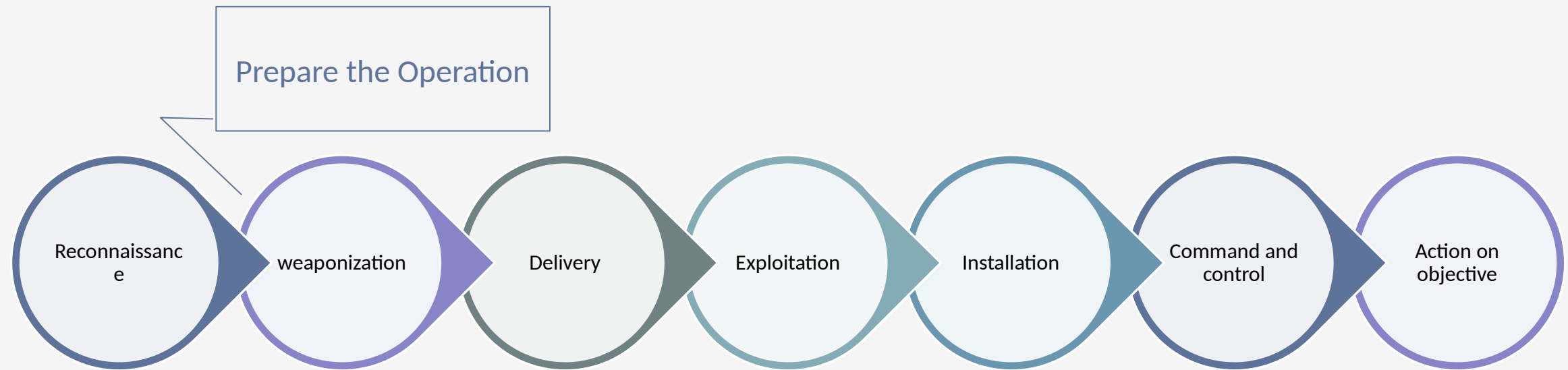
Let's look into the cyber kill chain.



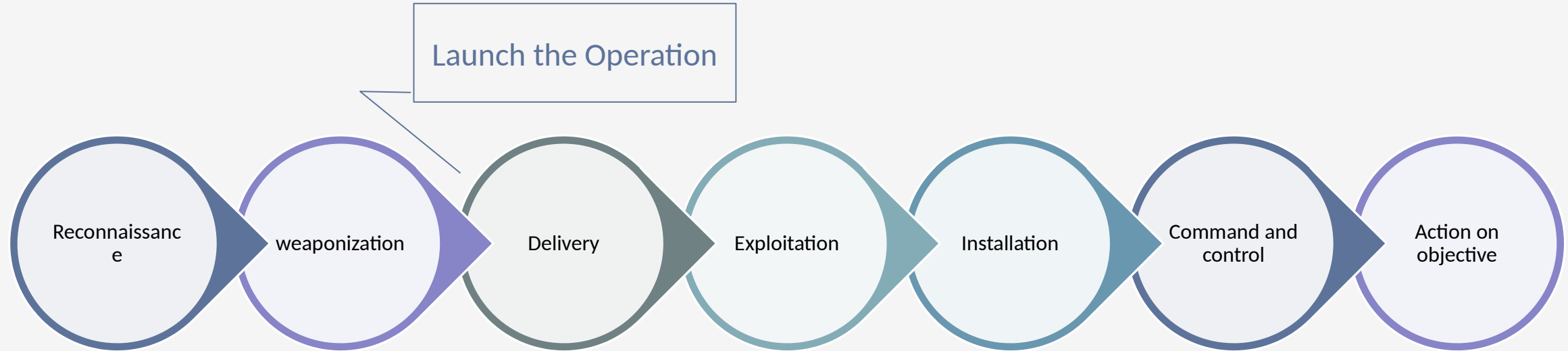
Let's look into the cyber kill chain.



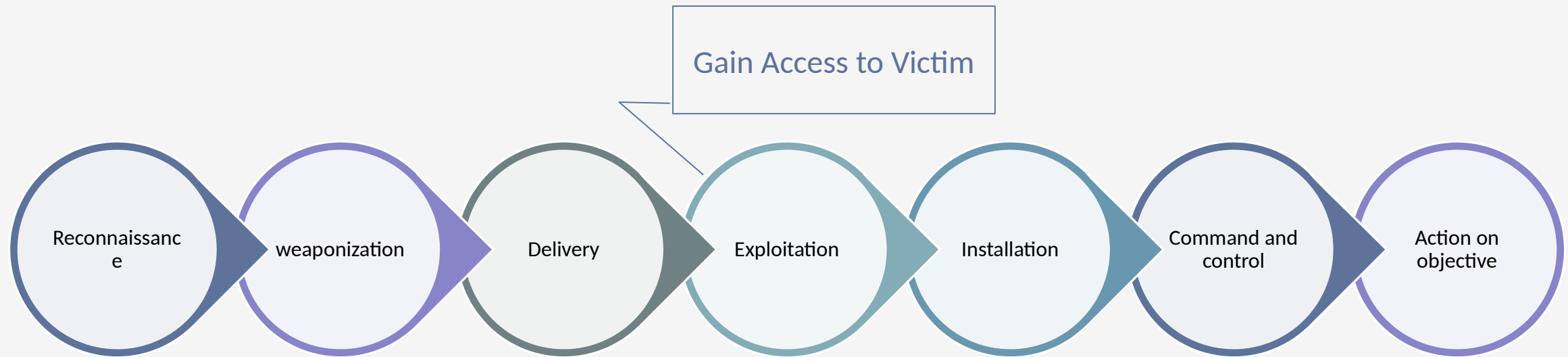
Let's look into the cyber kill chain.



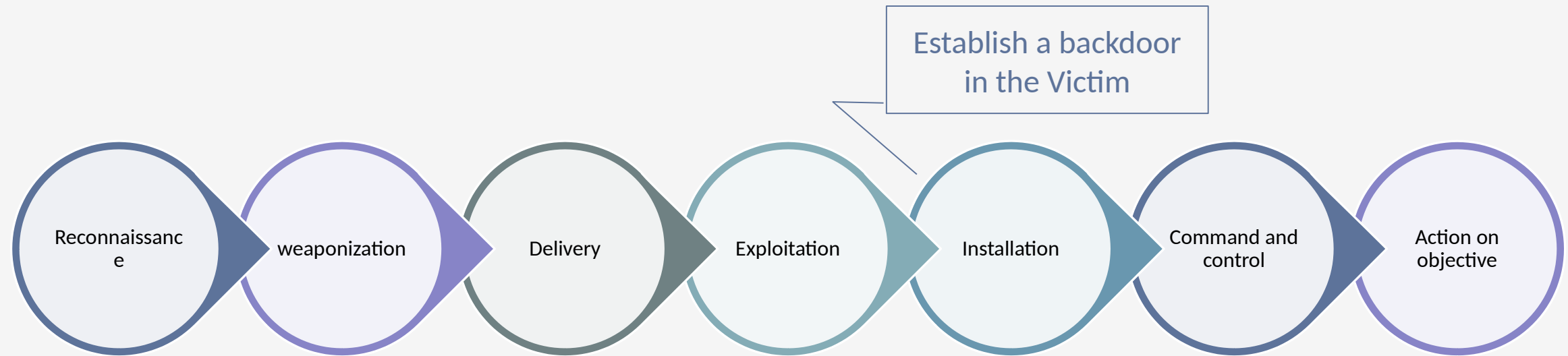
Let's look into the cyber kill chain.



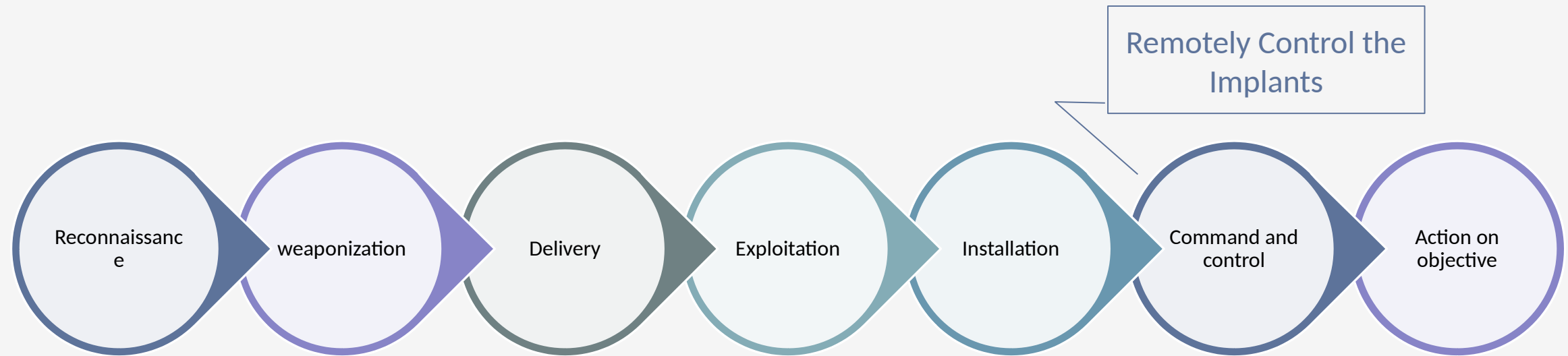
Let's look into the cyber kill chain.



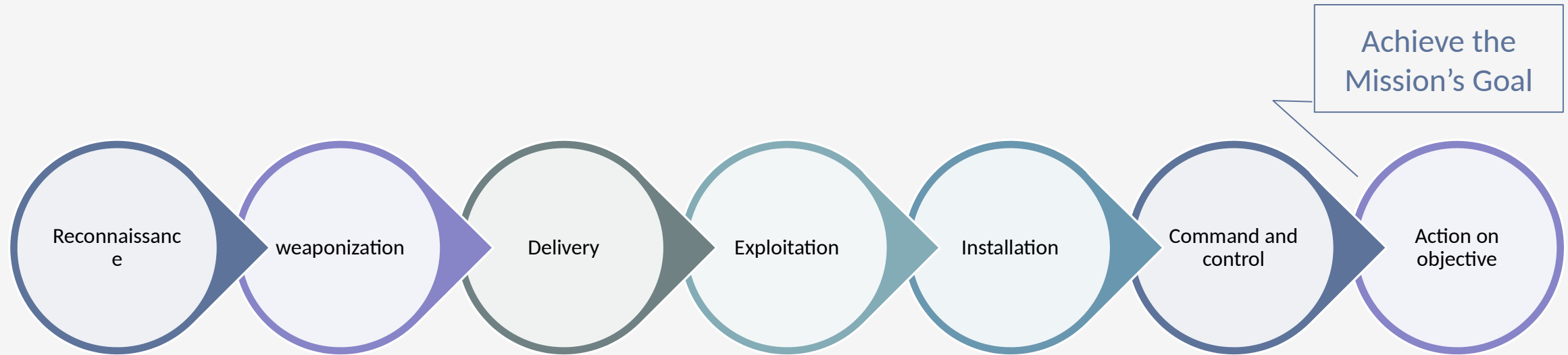
Let's look into the cyber kill chain.



Let's look into the cyber kill chain.



Let's look into the cyber kill chain.



Phishing campaign execution process

- ❖ Get the exact Hardware
- ❖ Setup the infrastructure.
- ❖ Order a domain.
- ❖ Inform authorities.
- ❖ Do a test run.
- ❖ Start the campaign.
- ❖ Evaluate the results.

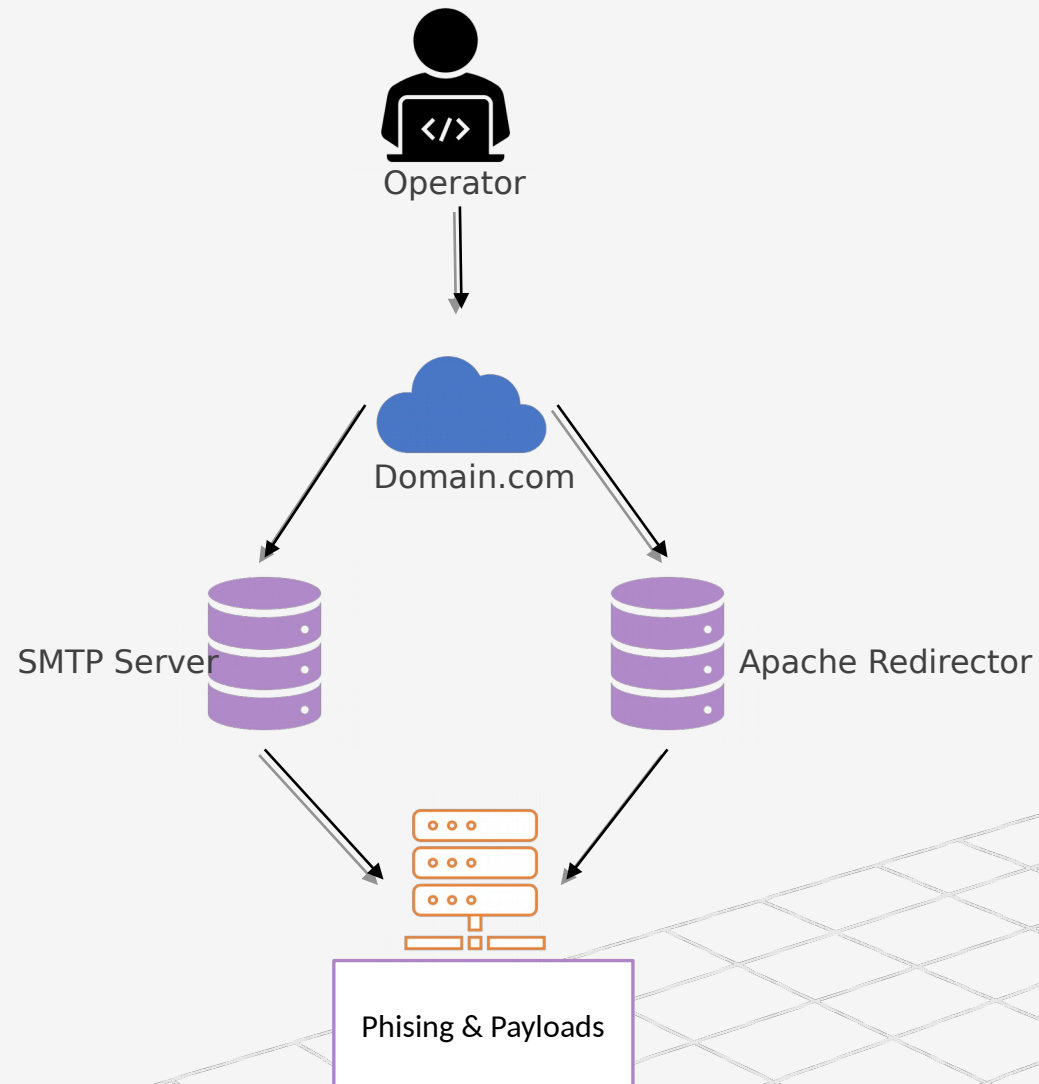


Phishing Setup

- ❖ Easy Web-Based Phishing
- ❖ Cobalt Strike Phishing
- ❖ Phishing Frameworks:
 - Gophish
 - Lucy
 - Phishing frenzy
 - SET



Phishing Infrastructure.



Phishing Infra setup.

- ❖ Create your own mail server or Use SMTP services.
- ❖ Try to buy expired domains from expireddomains.net
- ❖ Collect all the details and start generating sending profiles.
- ❖ Create the web server that the targets will be asked to get to in the phishing email.
- ❖ Try to make the phishing web page looks legit.
- ❖ Make sure the domain is categorized.
- ❖ Use Letsencrypt SSL certificate to make the website looks more promising.
- ❖ Create landing page, decoy pages, etc.



Phishing Infra setup ctd.

- ❖ Implement phishing redirectors
- ❖ Make sure the below options are followed to get a 10/10 domain reputation:
 - setting up SPF records
 - setting up DKIM
 - setting up DMARC
 - setting up encryption
 - configuring postfix as a relay
 - sanitizing email headers to obfuscate the originating email server (the phishing server)



Phishing Infra setup ctd.

❖ Malicious Document payloads:

- To create macro-based payloads (Metasploit, Cobalt Strike, Empire, etc.)
- Obfuscate with VBad <https://github.com/Pepitoh/VBad>
- Also, check LoLBins: <https://lolbas-project.github.io/>
- And maybe Invoke-DOSfuscation could be handy: <https://github.com/danielbohannon/Invoke-DOSfuscation>
- <https://outflank.nl/blog/2019/05/05/evil-clippy-ms-office-maldocassistant/>
- <https://outflank.nl/blog/2019/10/30/abusing-the-sylk-file-format/>
- Embedded OLE Objects



Phishing Infra setup ctd.

❖ Final steps:

❑ Create email templates, personalize, update with malicious links

- Email templates can be anything between plain and very complex
- Several templates online, especially from marketers (good at bypassing spam filters)
- Always a good idea to personalise malicious links and landing page, too
- Always test your email prior to sending, have used mail-tester.com with good success so far

❑ Send and wait

- Phishing requires patience
- Unless you want to combine it with vishing or smishing.

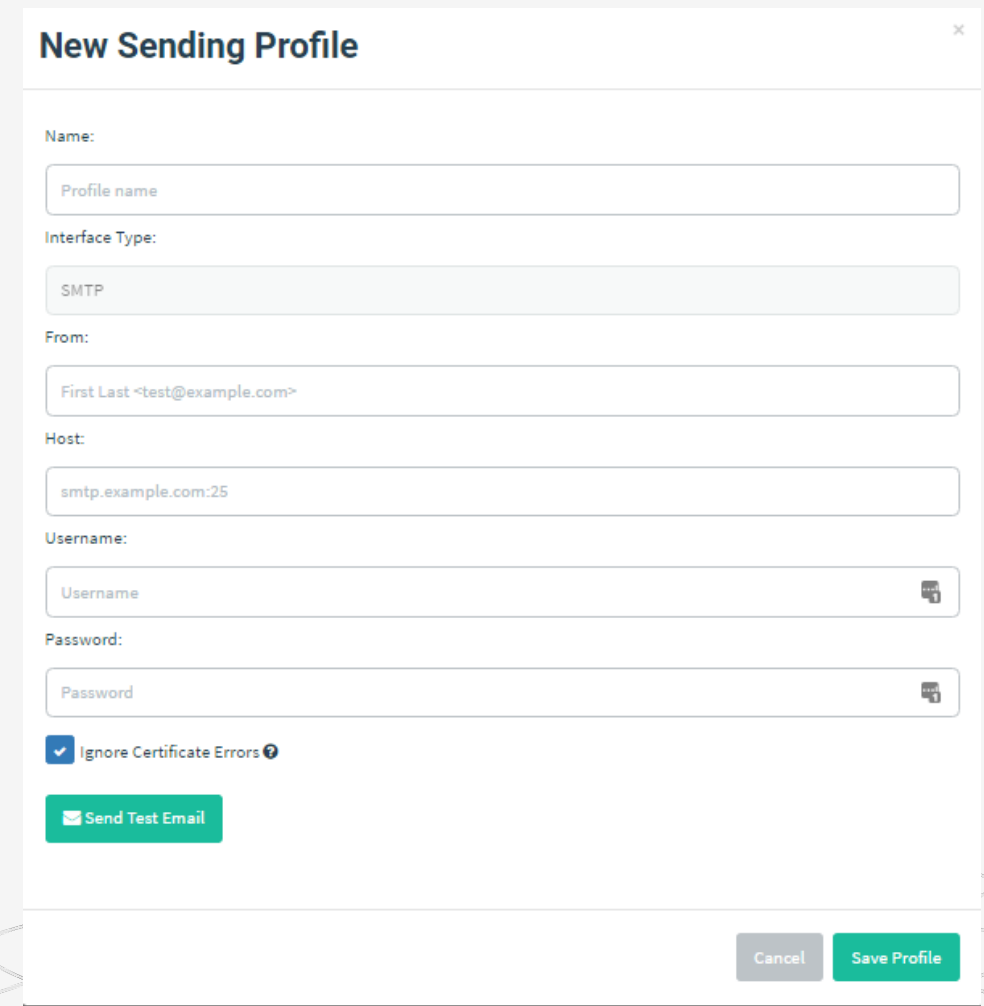


Phishing Infra setup ctd.

❖ Gophish setup:

Creating new SMTP profile

1. Under "Sending Profiles" create a new profile
2. Add a fitting name
3. For "Interface Type" choose "SMTP"
4. For "From" type your mail address
5. For "Host" type in the Hostname or IP address of your mail server
6. For "Username" type in the smtp username
7. For "Password" type in the smtp password
8. Send a test mail using the according button at the end of the form
9. Tick the box "Ignore Certificate Errors" if you run into any problems when sending a test mail



New Sending Profile

Name:
Profile name

Interface Type:
SMTP


From:
First Last <test@example.com>



Host:
smtp.example.com:25

Username:
Username

Password:
Password

☒ Ignore Certificate Errors ?

 Send Test Email

 Cancel  Save Profile

Phishing Infra setup ctd.

❖ Gophish setup ctd.:

Creating Templates

1. To create a template, first navigate to the “Email Templates” page and click the “New Template” button.

New Template

Name:


Subject:

Plaintext

☒ Add Tracking Image

Show entries

Search:

Name 

Phishing Infra setup ctd.

❖ Gophish setup ctd.:

Creating Landing pages

New Landing Page

Name:

Page name

Import Site

HTML

X Copy Paste Undo Redo ABC- = < > Image Table List Omega Expand Source

B I S Ix Bulleted Numbered Indented Outdent Quote Styles Format ?

☐ Capture Submitted Data ?

Cancel

Save Page



Phishing Infra setup ctd.

❖ Gophish setup ctd.:

2. Creating Groups

New Group

Name:

Group name

+ Bulk Import Users

First NameLast NameEmailPosition

+ Add

Show 10 entries

Search:

First Name	Last Name	Email	Position
No data available in table			

Showing 0 to 0 of 0 entries

PreviousNext

CloseSave changes

Phishing Infra setup ctd.

❖ Gophish setup ctd.:

Creating New Campaign

1. Go to campaigns -> "New Campaign"
2. Pick a name
3. Choose the email template and landing page
4. Enter the URL
5. Pick the time when the emails will be sent to your targets
6. Choose the sending profile
7. Choose the according group

New Campaign

Name:

Email Template:

Landing Page:

URL: ?

Launch Date

Send Emails By (Optional) ?

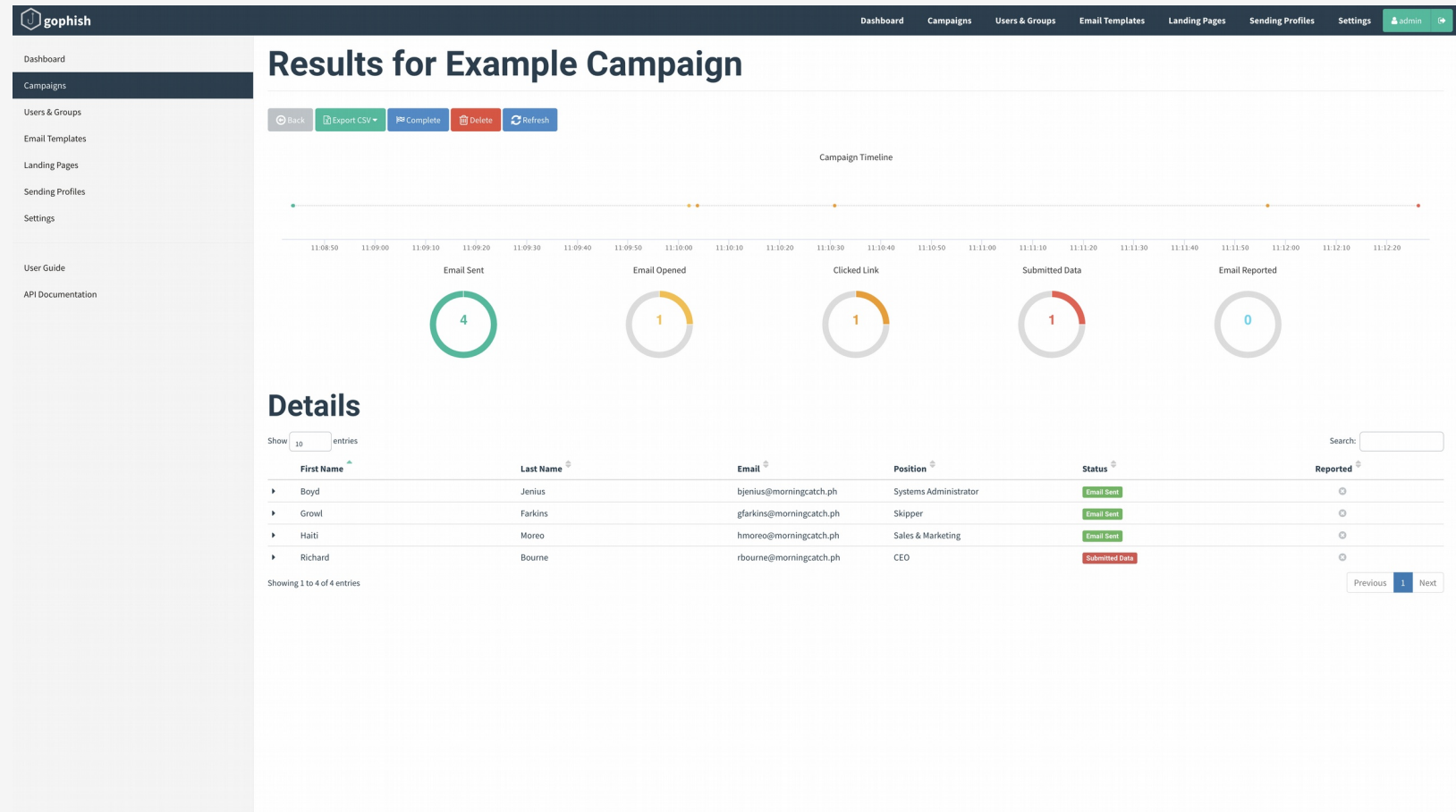
Sending Profile:

Groups:

Phishing Infra setup ctd.

❖ Gophish setup ctd.:

1. Evaluate the results



Some real world examples.

❖ Link manipulation:

Link Manipulation

Manipulating the links for example www.facb00k.com

Instead of www.facebook.com

Misspelled URLs or sub domains are common tricks used by attacker



Paul Moore
@Paul_Reviews



Follow

Can you spot the difference?

lloydsbank.co.uk


lloydsbank.co.uk


#phishing #scam #caseSensitive #security

Some real world examples.

❖ An interesting tactics by the attacker

Voicemail from WIRELESS CALLER [REDACTED]

 Wireless Caller: [REDACTED]
To: [REDACTED]

 You forwarded this message on [REDACTED]
If there are problems with how this message is displayed, click here to view it in a web browser.

EXTERNAL EMAIL - Do not click any links or open any attachments unless you trust the sender and know the content is safe.


This sender is trusted.

You have a new voice message from +4 [REDACTED] (33 seconds).. On August [REDACTED]

[Play VNM](#)

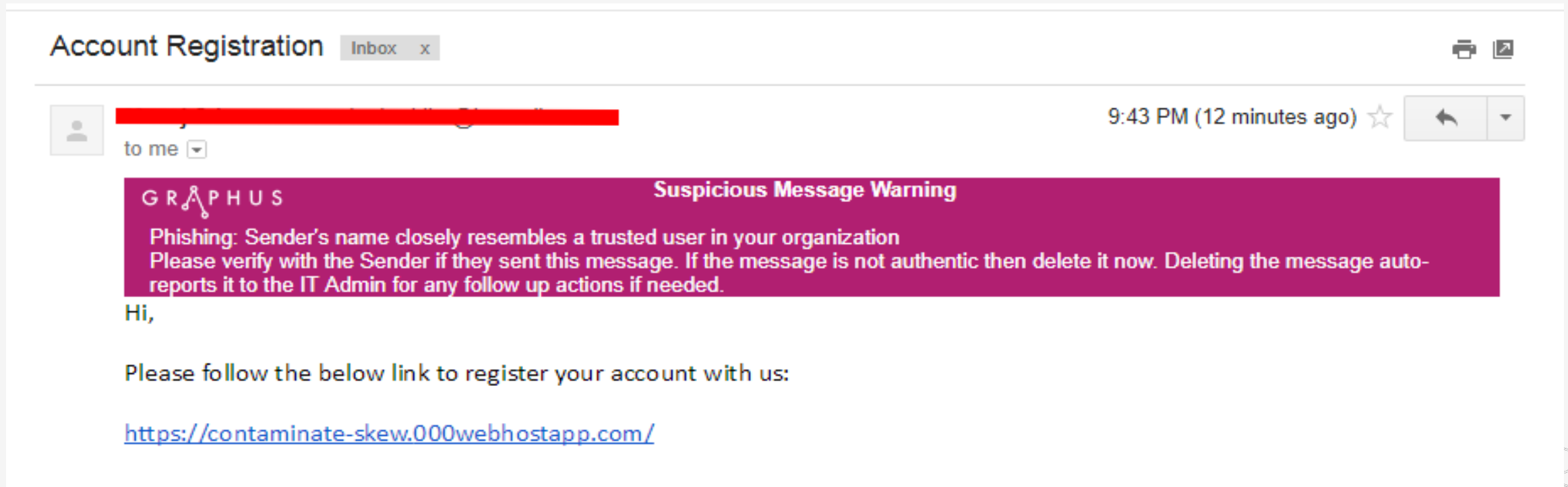
Message encryption by [REDACTED]

Copyright © 2020.
Privacy Policy



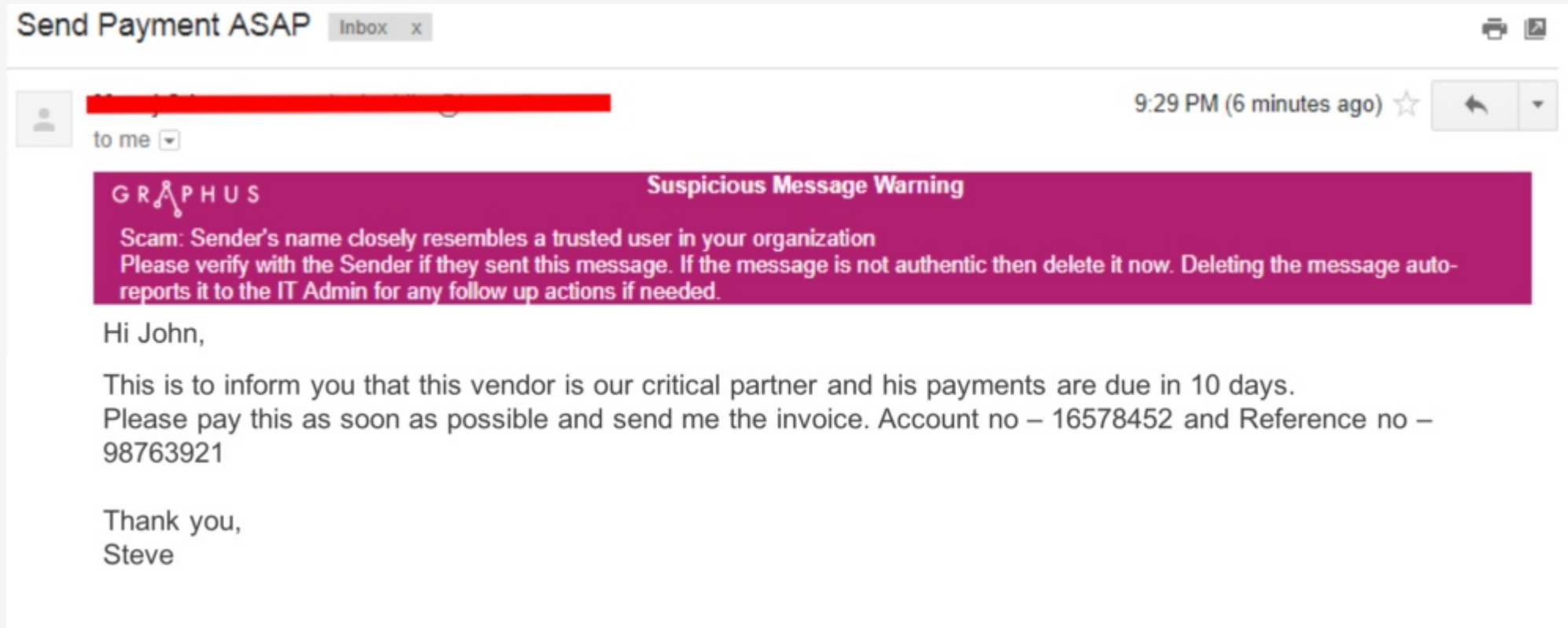
Some real world examples.

- ❖ The emails look like they are legitimate but typically not very personal.



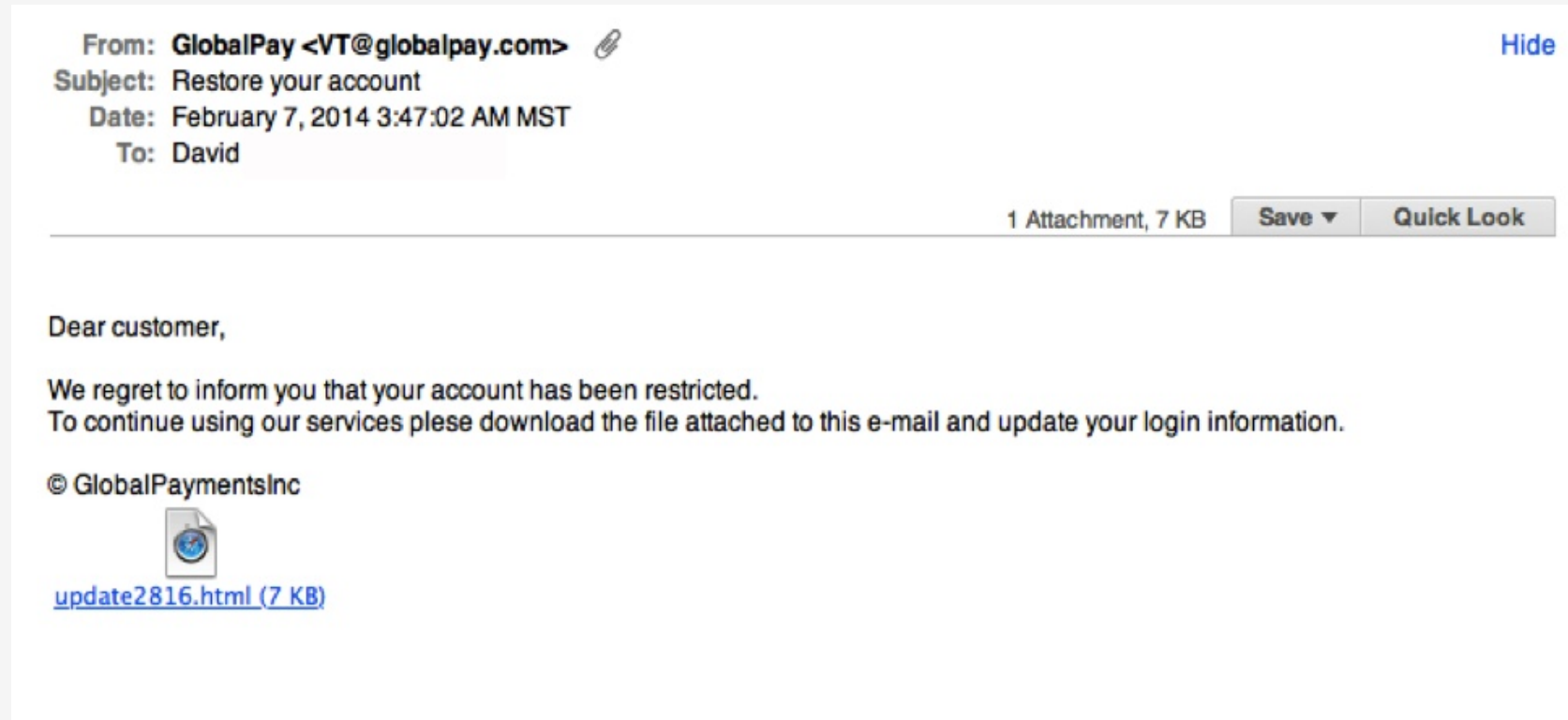
Some real world examples.

- ❖ Spear phishing, on the other hand, is more personal and directed at specific individuals.



How to identify a phishing mail.

- ❖ companies will not ask for your sensitive information via email.



How to identify a phishing mail.

- ❖ The message is sent from a public email domain or not from a genuine sender.

----- Forwarded Message -----

From: PayPal <paypal@notice-access-273.com>

To:

Sent: Wednesday, January 25, 2017 10:13 AM

Subject: Your Account Has Been Limited (Case ID Number: PP-003-153-352-657)

PayPal

Dear Customer,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What the problem's?

We noticed some unusual activity on your PayPal account.

As a security precaution to protect your account until we have more details from you, we've place a limitation on your account.

How you can help?

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account.

To help us with this and to find out what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

[Log In](#)

[Help](#) | [Contact](#) | [Security](#)

This email was sent to you, please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking Help at the bottom of any PayPal page.

© 2016 PayPal Inc. All rights reserved



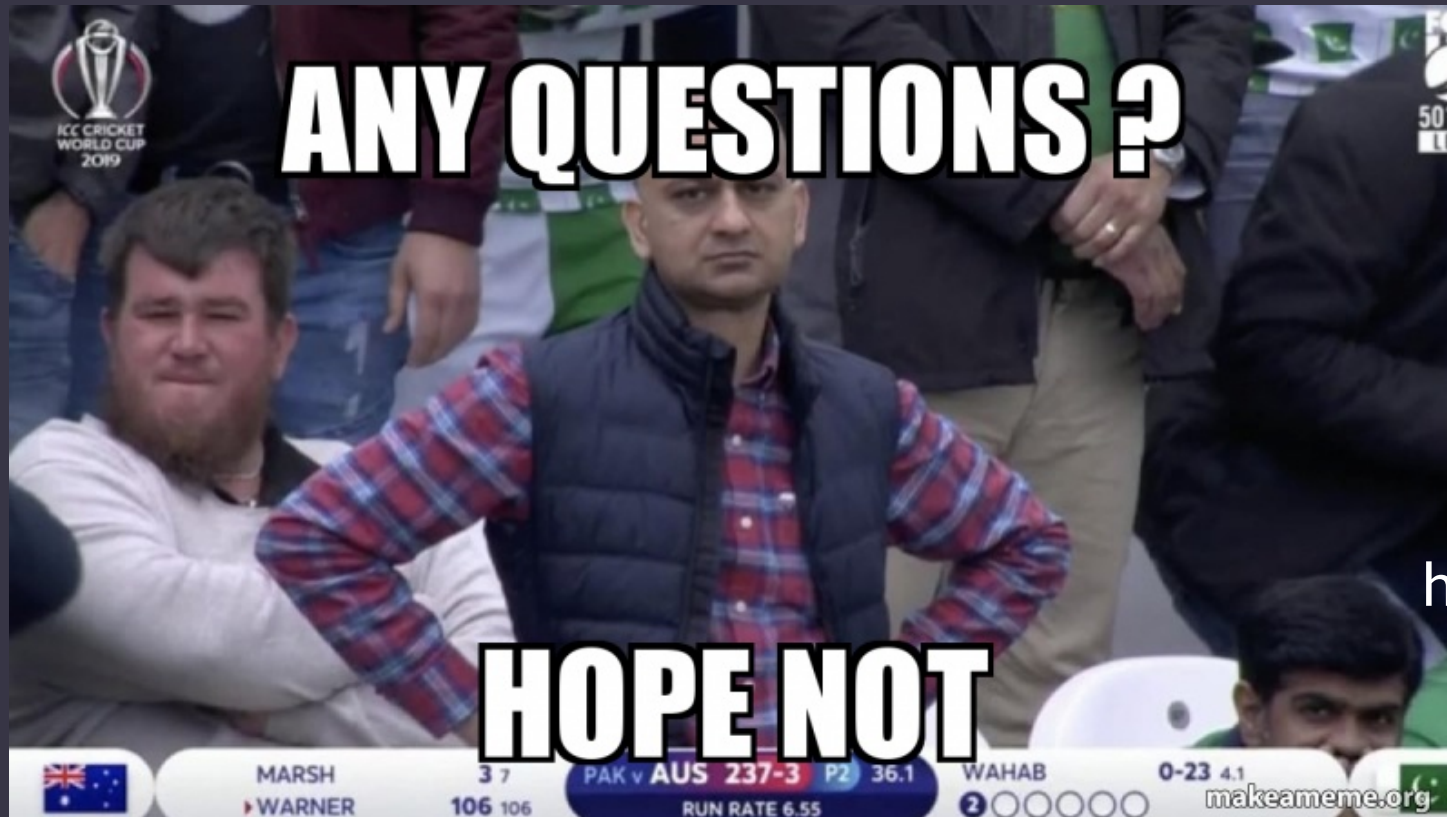
How to identify a phishing mail.

- ❖ The email will be poorly written.
- ❖ Includes suspicious attachments or links.
- ❖ The domain name is misspelt.

How to prevent Phishing

- ❖ Keep Informed About Phishing Techniques.
- ❖ Think Before You Click!.
- ❖ Install an Anti-Phishing Toolbar.
- ❖ Verify a Site's Security.
- ❖ Check Your Online Accounts Regularly.
- ❖ Keep Your Browser Up to Date.
- ❖ Use Firewalls & Antiviruses.
- ❖ Be Wary of Pop-Ups.
- ❖ Never Give Out Personal Information.
- ❖ Look for the “s” in https://website.com
- ❖ Set up two-factor authentication.
- ❖ Trust your gut instincts





QA?

<https://twitter.com/sr33h4ri>

<https://linkedin.com/in/sreehari-haridas>



Join our Discord channel for more support!

[Discord.gg/RAvKMU9](https://discord.gg/RAvKMU9)



Thank You!