Recognize and handle phishing attempts

Process to check the Reputation of any Email:

- Check the Email carefully
- Don’t click the Enter button or any URL and Attachment
- Right click on URL or copy the URL
- Do the header analysis in order to know the email is spoofed or not
- Check IP URL Reputation
- If there is any attachment then do not open it. Save the mail and analyze directly to sandbox
- Check all the websites and Sandbox carefully and decide whether its malicious or not

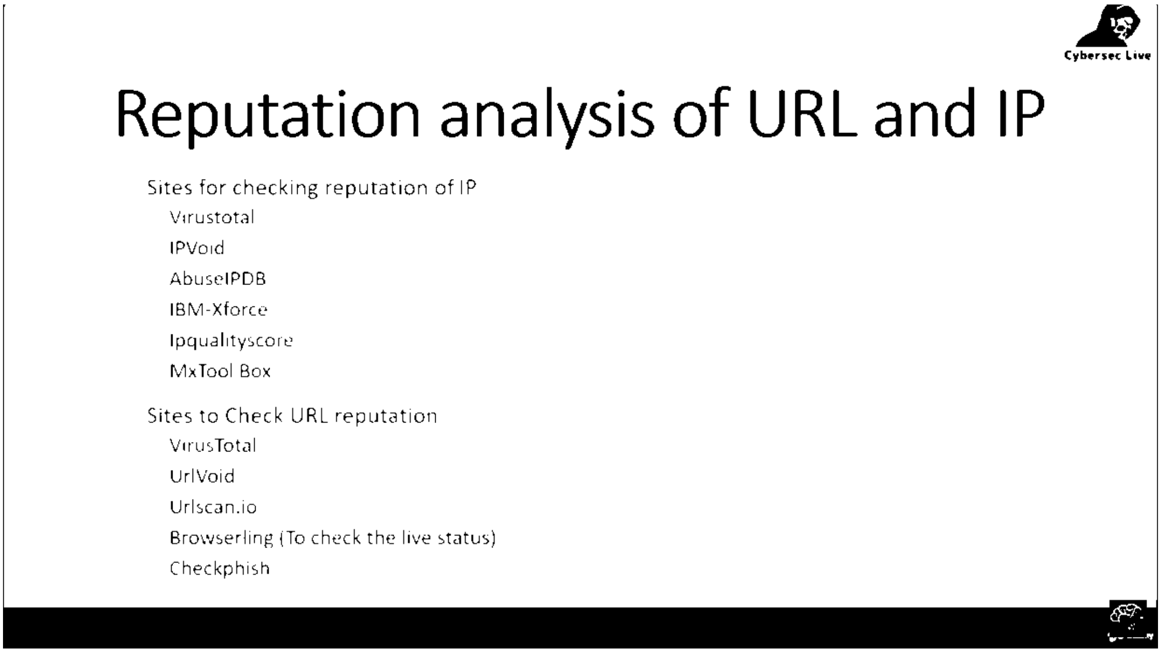
Header Analysis:

- Tools for Header analysis:
  - https//:mxtoolbox.com/
  - https//:mailheader.org/
  - https//:mha.azurewebsites.net/
  - Abuseripdp

- **DMARC :** Domain Base Message Authentication, Reporting and Conformance
  DMARC helps mail administrators prevent hackers and other attackers from spoofing their organization and domain
- **DKIM :** Domain Key Identifier Mail
  DKIM helps to protect email senders and recipients from spam, spoofing and and phishing.
- **SPF :** Sender Policy Framework

It prevents spammers from sending message on behalf of your domain
550 spf check failed

Reputation analysis of URL and IP

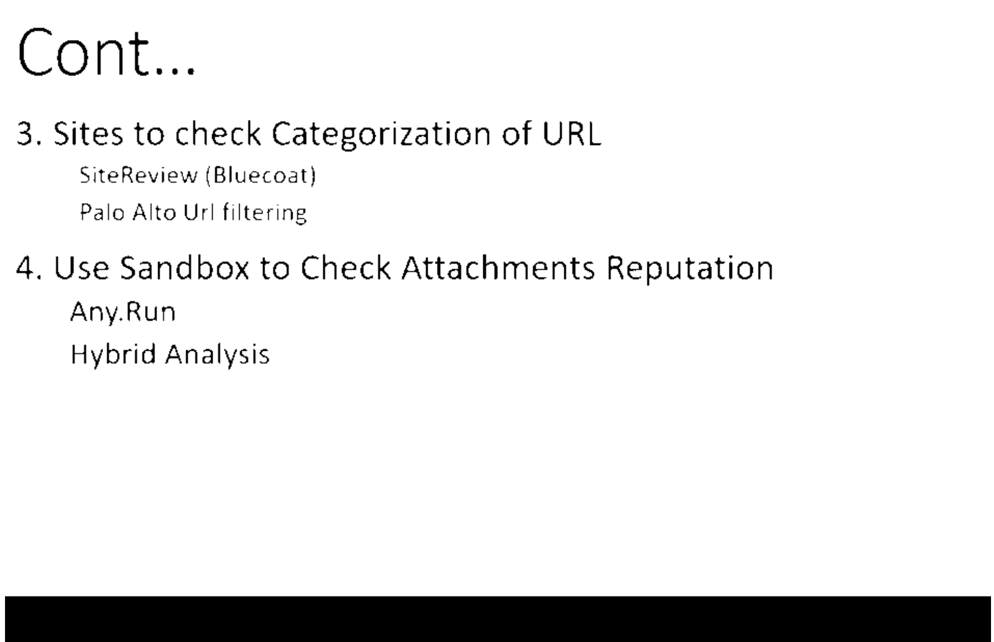


Cybersec Live

Reputation analysis of URL and IP

Sites for checking reputation of IP
- Virustotal
- IPVoid
- AbuseIPDB
- IBM-Xforce
- Ipqualityscore
- MxTool Box

Sites to Check URL reputation
- VirusTotal
- UrlVoid
- Urlscan.io
- Browserling (To check the live status)
- Checkphish



Cont...

3. Sites to check Categorization of URL
   - SiteReview (Bluecoat)
   - Palo Alto Url filtering
4. Use Sandbox to Check Attachments Reputation
   - Any.Run
   - Hybrid Analysis

Email Analysis on SandBox

- Any.Run Sandbox Analysis Application
- Hybrid Analysis Application