What Should You Do When You Receive a Phishing Email?:

When that suspicious email lands in your inbox, follow these steps:

- Pause: Take a breath and don't panic.
- Inspect the Sender: Verify the sender's legitimacy.
- Analyze the Content: Look for red flags like urgent requests, misspellings, or suspicious links.
- Don't Click: Avoid clicking on any links or downloading attachments.
- Report: Report the phishing attempt to your IT/security team.
- Educate Yourself: Stay informed about phishing tactics and prevention.

Remember, vigilance is your best defense against phishing attacks! Stay safe out there.

List of Phishing Email Analysis Tools for 2024, along with their functionalities and purposes:

1. Email Header Analysis:

   - MXToolbox: Detects phishing attempts, spam, malware, and impersonation scams. https://lnkd.in/gxaGmWcg
   - Google MessageHeader: Provides insights into email headers. https://lnkd.in/gn6DdfcA
   - MailHeader: Analyzes email headers for security threats. https://mailheader.org/
   - Azure Header Analyzer: Assesses email header information. https://lnkd.in/gsMav4i6
   - Gaijin: A tool for email header analysis. https://lnkd.in/ejZzmqjA

2. URL / IP Reputation Check:

   - Virustotal: Scans URLs and IPs for threats. https://lnkd.in/gNqxtn4d
   - Talosintelligence: Identifies malicious domains and IPs. https://lnkd.in/g7uWdC5q
   - AbuseIPdb: Checks IP reputation. https://www.abuseipdb.com/
   - WebCheck: Verifies website safety. https://web-check.xyz/
   - CyberGordon: Offers IP and domain information. https://cybergordon.com/
   - Bright Cloud: Assesses URL reputation. https://lnkd.in/enQGqx9W
   - IPinfo: Retrieves IP details. https://ipinfo.io/
   - Test a site: Tests websites for security issues. https://lnkd.in/e4bkm5Eq

3. Visualization Tools: (Visualize a malicious URL without visiting the site.)

   - URLScan: Visualizes malicious URLs without visiting them. https://urlscan.io/

- URL2PNG: Generates screenshots of URLs. https://www.url2png.com/
- CheckPhish: Visualizes phishing URLs. https://lnkd.in/ejERWRXV

4. File / Attachment / Malware Analysis:

    - VirusTotal: Analyzes files and URLs for malware. https://lnkd.in/gNqxtn4d
    - Anyrun Sandboxing: Executes files in a sandboxed environment. https://any.run/
    - Hybrid-Analysis Sandboxing: Provides dynamic analysis of files. https://lnkd.in/gaRGY8kB
    - Joesandbox: Analyzes suspicious files. https://lnkd.in/gTJJ9GiC
    - Cuckoo Sandbox: Automated malware analysis. https://cuckoo.cert.ee/
    - CapeSandbox: Malware detonation platform. https://lnkd.in/eqzpANqK
    - VMRay: Advanced malware analysis. https://lnkd.in/gDytZZgz
    - Triage: Investigates suspicious files. https://tria.ge/dashboard

5. Whois Domain Record:

    - Centralops: Retrieves domain information. https://centralops.net/co/
    - DomainTools: Performs reverse IP lookup. https://lnkd.in/epc5M4PE
    - Whois: Provides domain registration details. https://www.whois.com/

6. Phishing Analysis Tools: Automatically Collecting Artifacts

    - Phish Tool: Collects artifacts from phishing emails. https://www.phishtool.com/
    - EML analyzer: Analyzes email files. https://lnkd.in/eRa3B52Y
    - CyberChef: Tool for data manipulation and analysis. https://lnkd.in/gVjZywKu

7. Miscellaneous:

    - Browser Sandbox: Safely test URLs in a sandboxed browser. https://lnkd.in/gjA-QqdX
    - Thunderbird (EML Opener): Opens EML files. https://lnkd.in/gBfPbqas
    - eM Client (EML Opener): Another EML file viewer. https://www.emclient.com/
    - Phishtank: Collaborative phishing database. https://phishtank.org/
    - OpenPhish: Repository of known phishing URLs. https://lnkd.in/d-6GcqxP
    - Phishunt: https://phishunt.io/
    - Haveibeenpwned: https://lnkd.in/gvbzhceV
    - Simulate any Browser: https://lnkd.in/gSTacMQi

8. Email Analysis Tutorial

    - Phishunt: https://phishunt.io/ Youtube: https://lnkd.in/d97nqbNY
    - Email Header Analysis PDF: https://lnkd.in/eH76CJz8
    - Social Eng. Red Flags: https://lnkd.in/ep3mYE5s

9. What should you do: https://lnkd.in/g9Tzpmbs
   (When You Receive a Phishing Email?)

Remember to stay vigilant and use these tools to protect yourself and your organization from phishing threats!

#cybersecurity #phishing #ransomware #phishingemails #phishingattackprevention #businessemailcompromise #blueteam

#redteam #infosec #soc #forensic #malwares #malware #malwareanalysis #ioc #threatintelligence #threathunting #cyberdefense #computersecurity