**Day 2**

I find this information by using “MxToolBox” tool.

| **Test** | **Result** |  |
| --- | --- | --- |
| [Status Problem](https://mxtoolbox.com/problem/mx/dns-record-published?page=prob_mx&action=mx:amaz0n-security.com&showlogin=1&hidepitch=0&hidetoc=1) | DNS Record Published | DNS Record not found |
| [Status Problem](https://mxtoolbox.com/problem/mx/dmarc-record-published?page=prob_mx&action=mx:amaz0n-security.com&showlogin=1&hidepitch=0&hidetoc=1) | DMARC Record Published | No DMARC Record found |
| [Status Problem](https://mxtoolbox.com/problem/mx/dmarc-policy-not-enabled?page=prob_mx&action=mx:amaz0n-security.com&showlogin=1&hidepitch=0&hidetoc=1) | DMARC Policy Not Enabled | It is recommended to use a quarantine or reject policy. To enable BIMI, it is required to have one of these at 100%. |

Suspicious Link :- <http://amazon.verify-account.com>

In this link they use http protocol. By using this protocol they can easily capture Login Credentials and Passwords.

“Urgent: Your Account Has Been Suspended” By using this sentence they want rapid action from end user.

“\*Attachment:\*\* invoice.zip” By clicking on this link of invoice they trying to phishing.

**Conclusion :-** By clicking suspicious links in email risk is very high. HTTP sites are vulnerable. So hackers can easily intercept or read your information.