national health authority

सत्यमेव जयते

Cyber Suraksha Dishanirdesh || Vol 21

Targeted Phishing Campaign by Malicious Actors

What is phishing?

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.

Covid-19 targeted phishing

CERT-In has issued an advisory warning potential phishing attack with emails stating 'free COVID-19 testing for all residents of Delhi, Mumbai, Hyderabad, Chennai and Ahmedabad' misleading users to provide personal information.

How to identify a phishing email ?

Sender Address

- Ask yourself, do I know the sender?
- Does the sender's domain look suspicious? Example, pnjay.gov.in

Subject Line

- Ask yourself, would the sender use this subject line?
- Common subject lines for phishing include Request, Follow up, Urgent/Important, Payment status, Invoice due or even 'Re:' to imitate an ongoing conversation.

Attachments

- Ask yourself, am I expecting an attachment from the sender?
- Verify the sender before clicking on attachments like purchase orders, unpaid invoices, urgent voice mail, updated employee policy etc

Language

- Ask yourself, does the email include spelling or grammatical errors.
- An email from a legitimate organization usually is well written
- If it looks like an email from a person you know, check if the language seems out of ordinary for the sender

Hyperlinks

- Ask yourself, does the link include a misspelling or slightly modified version of a known URL?
- Is there a sense of urgency to click on the link immediately to avoid a negative consequence of gain something of value?

How to mitigate ?

- Report any email received from **ncov2019@gov.in** to the security team immediately.
- Do not open attachments or URLs received over emails, rather than go to the organization's website directly for any information (e.g. To seek any info/ updates on COVID-19, please visit the official Ministry of Health website https://www.mohfw.gov.in/). Follow only trusted sources.
- Disable macros and ActiveX
- Use strong passwords which cannot be hacked by brute-force.
- Use proper antivirus so that unwanted executions don't take place.
- Check the integrity of the URL before disclosing any information.
- Beware of phishing domains and false URLs.

What should you do if you suspect a phishing email?

- If you suspect an email to be a phishing attempt, do not click on any links or attachments in the email. Report the email to Information Security Team @ it.securityincident@nha.gov.in

With Regards
NHA-IS-Team