रक्षा मंत्रालय
MINISTRY OF
DEFENCE

CISO NEWSLETTER

Issue 05, Vol 1

FOREWORD

In an ever evolving digital world, almost all of us use internet on a daily basis. It is important as users that we are aware of latest cyber security threats which can affect personnel on a daily basis.

The CISO newsletter is one such means of providing basic background and overview of various cyber security issues, guidelines and best practices which; if followed religiously by all personnel of the Ministry, will ensure reduction in cyber security incidents/ compromises.

The present newsletter deals specifically about one such cyber threat i.e. **PHISHING**. Despite being an exhaustive topic, with lot of technical information, the newsletter has been made in a simplistic manner so that it is understandable to all users within the Ministry irrespective of their profile, educational qualification.

In the present edition of the newsletter, a phishing attack scenario has been included as so as to give readers a method for self-assessment of their level of understanding of email phishing methods and how to prevent such incidents at home or at work place.

All personnel in the Ministry are requested to go through the contents of the newsletter and forward their voluble feedback and suggestions for further improvement.

(Vishal Gagan)
CISO, DoD

CISO NEWSLETTER

PHISHING

Phishing is the attempt to obtain sensitive information such as user names, passwords and financial details often for malicious reasons, by masquerading/ deceiving as a trustworthy entity in an electronic communication.

HOW DOES PHISHING WORK

Phishing starts with fraudulent emails/SMS/URLs that are carefully crafted such that you open them without any suspicion. The message is made to look as though it comes from a trusted sender. If the attacker succeeds, victim is coaxed into providing confidential information, often on a scam website.

These types of cyber attacks open the door for attackers to enter into your system and access confidential data like bank account details, credit card numbers, passwords, etc.

Once the information is obtained, the phishers immediately send or sell it to people who misuse them.

Sometimes, phishing not only results in loss of information but also injects malware into the victim's (Individual/ Organization) computer or phone.

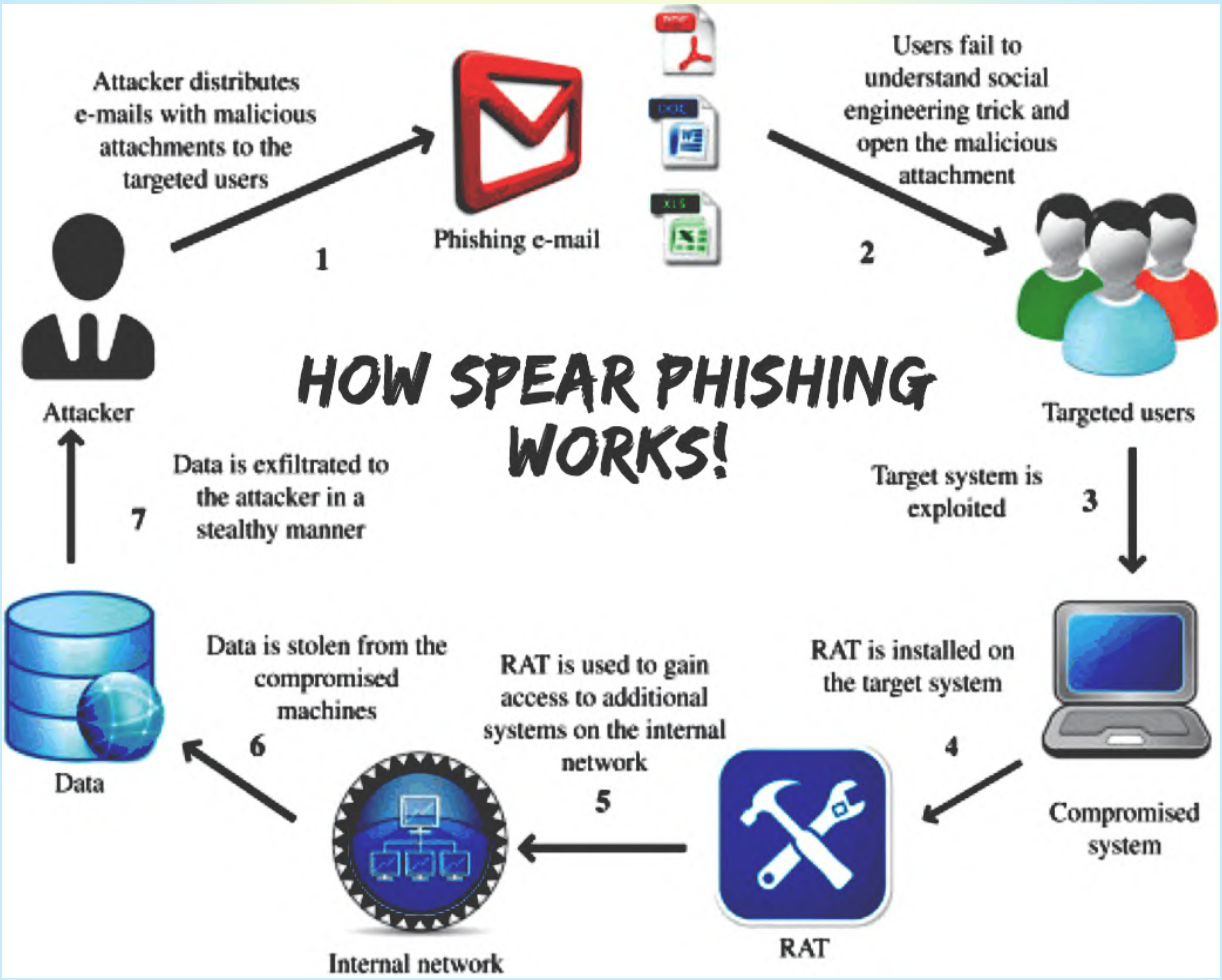
Once infected, phishers gain control over devices, through which they can send emails and messages to other people connected through the server.

CISO NEWSLETTER

SPEAR PHISHING

Spear Phishing. Spear phishing is typically targeted in nature, and the emails are carefully designed to target a particular user/ company/ organisation.

These attacks have a greater risk because phishers do a complete social profile research about the user and their organization through their social media profiles/ other websites.



CISO NEWSLETTER

SPEAR PHISHING ATTEMPT PROGRESSION

1. **Gathering information on targets**. Spear-phishing starts with identifying key and high-value individuals These people are targets because **their credentials and the data** they have access to are of most value in the organization.
2. **Creating convincing emails**. With information about their targets, attackers then craft the emails so that they seem legitimate enough to get intended targets to open an attachment or click a link. Spear phishers can create emails so realistic that they appear to come from a trusted source and ask for information that the source would normally request.
3. **Hiding their origin**. Attackers can spoof email sender addresses or compromise a legitimate email to make it look as if the email came from a trusted domain
4. **Delivery of payload**. The link will send the user to a malicious URL or compromised reputable domain that takes the user's credentials as he or she logs in.
5. **Avoid Detection**.The attack tries to hide itself throughout the process. Methods that attackers use to avoid detection include polymorphism and shortened or obfuscated URLs to prevent blacklist detection.

CISO NEWSLETTER

OBSERVED PHISHING INSTANCES

Example 1

From: "KL Baranwal IDSE" <klbaranwal27975-cgo@gov.in>
To: < Hidden recipients>
Sent: Saturday, June 27, 2020 11:31:26 PM
Subject: National Informatics Centre Email Expiration Notice

Dear Sir
NIC Email account will expire soon to continue using it please confirm by logging into your account using link below.
Click Here To Confirm

Thanks & Regards

KL Baranwal

Messaging Administrator, National Informatics Centre
Ministry of Electronics & Information Technology

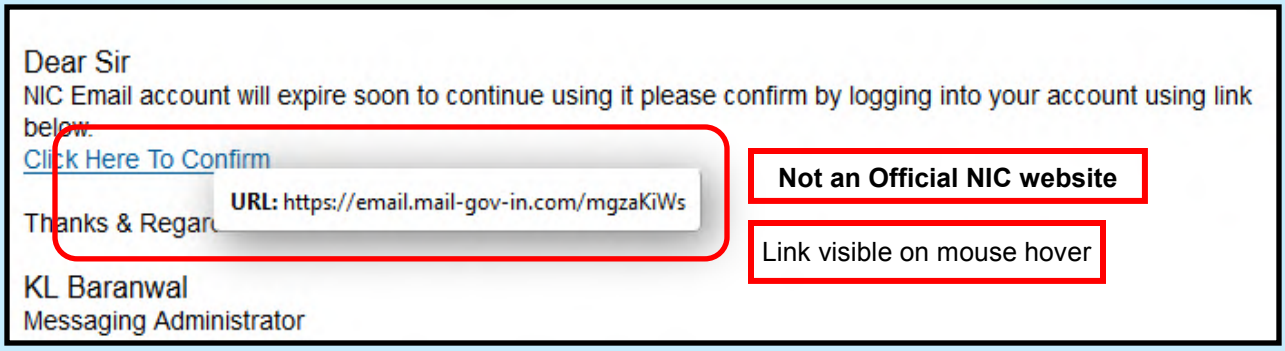
Analysis.

1. This is a typical phishing email which is sent to either compromise your password or entice you to link on a malicious link which may then install malware on your host machine.

2. **Possible Flags**.

(a) **Unrecognized 'From' address** - 'klbaranwal27975-cgo@gov.in' may not the official email id of NIC administrator.

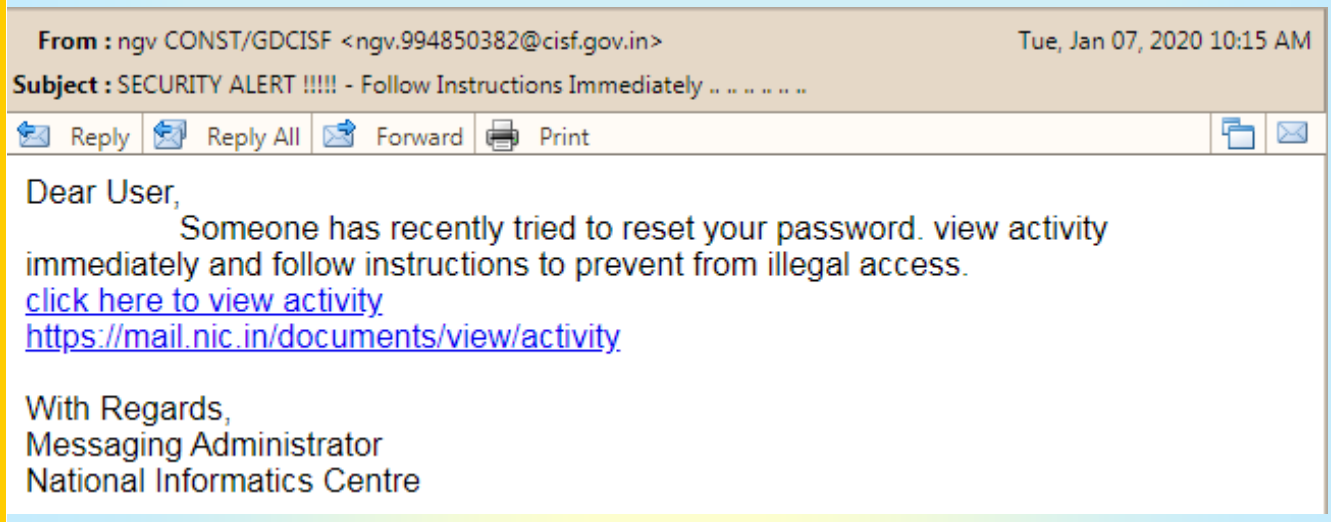
(b) **The link redirects to the non-legitimate website**.



CISO NEWSLETTER

MORE PHISHING EXAMPLES

Example 2.



From : ngv CONST/GDCISF <ngv.994850382@cisf.gov.in> Tue, Jan 07, 2020 10:15 AM
Subject : SECURITY ALERT !!!!! - Follow Instructions Immediately .. ..
Reply | Reply All | Forward | Print

Dear User,
Someone has recently tried to reset your password. view activity immediately and follow instructions to prevent from illegal access.
click here to view activity
https://mail.nic.in/documents/view/activity

With Regards,
Messaging Administrator
National Informatics Centre

Analysis.

Flags.

(1) Unknown email address - despite being .gov.in

(2) Email requesting immediate action - urgency depiction.

(3) Generic email - May have been forwarded to multiple users. Non genuine Link - May be malicious or a link to a fraudulent website.

CISO NEWSLETTER

SPOT A PHISHING SCAM/ EMAIL

CISO NEWSLETTER

CYBER CRIMINALS EXPLOITING COVID-19 PANDEMIC FOR PHISHING

Cyber criminals are trying variety of phishing campaigns and taking advantage of the heightened focus on COVID-19 to distribute malware, steal credentials, and scam users for money. The attacks are using the corona virus as a lure to try to trick distracted users capitalize on the fear and uncertainty. The details of various methods are being used by cyber criminals are:

i) **Impersonating popular apps** - Attackers impersonating (Aarogya Setu, Microsoft Teams, Zoom, Google Meet, WHO etc to first lure the victims and then send them links such as "relief package", "safety tips during corona", "corona testing kit", "corona vaccine", "payment and donation during corona".

CISO NEWSLETTER

CYBER CRIMINALS EXPLOITING COVID-19 PANDEMIC FOR PHISHING

Scam emails - Claiming they were looking to sell Corona virus cures or face masks or asking for investments in fake companies that claimed to be developing vaccines or in the form of donation requests for fake charities are another popular phishing methods that have seen taking advantage of Corona virus.

CISO NEWSLETTER

ANTI PHISHING MEASURES

i) Never click on the links in an E-mail: Never click on the links in an email because they might be a fake link to a website that might be harmful. It is better to type your own web address rather than clicking on it.

ii) Website is secure: It is best to check whether the website is secure enough to trust before entering any data on the website. The easy way is to see whether or not the URL is locked by the green padlock. Better option would be to check for site reputation using provided by a licensed total security software.

iii) Update your computer security: Always update your computer's security software and OS since as updates at times may block certain attacks of this kind.

iv) Verify HTTPS on Address Bar: Whenever a person is conveying confidential information online, he or she must confirm that the address bar reads “HTTPS” and not the standard “HTTP.” The “S” confirms that the data is being conveyed through a legitimate, secured channel.

v) Keep yourself up to date: Various government organization websites like CERT-IN, C-DAC, Cyberdost (MHA’s Twitter handle) regularly post updates in respect of Cyber Security. Apart from this, several blogs and articles are written daily, and it is best to keep updated with the latest Cyber Security measures, through any authenticated blog, news or social media platforms.

CISO NEWSLETTER

ANTI PHISHING MEASURES

vi) Never Enter Sensitive Information in a Pop Up Window Pop up windows represent another tool used by phishers with illicit agendas. An important tactic to prevent phishing attacks is to never enter information into a pop up window. In fact, a person is best served restricting pop up windows all together, except at those sites that an individual knows to be trustworthy.

vii) Regularly monitor your account: It is best to check your bank/ e-mail accounts regularly to keep a track of your transactions.

viii) Install and Maintain a Reliable Firewall: Another best practice to avoid phishing attacks is installation and maintenance of a reliable firewall. A firewall protects against the introduction of malicious codes onto a computer.

ix) Keep Antivirus Protection Current: Although keeping antivirus protection up to date may seem like a patently obvious strategy, a surprising number of people fail to take this very basic step. The reality is that identity thieves and other criminals constantly are changing their schemes. Therefore, maintaining current antivirus protection is an invaluable first line of defense against phishing attacks.

x) Utilize Anti-Spam Software: Use of Anti-spam software is that it can provide some degree of protection against phishing attacks. This type of software naturally filters out a good amount of phishing emails that would otherwise end up in an inbox.

CISO NEWSLETTER

REFERENCES

1. https://www.cdac.in/
2. https://cert-in.org.in/
3. https://www.cybercrime.gov.in/
4. Info graphic material available on Internet

Incidents related to Cyber Crime in New Delhi may be reported at the following

Website.
http://www.cybercelldelhi.in/

For online registration of complaints, visit the url https://www.cybercrime.gov.in/

HELPDESK

CISO Office : 011-23015444
Cyber Cell : 011-23794783
E-Mail ID : cybercell-mod@gov.in

Concept : Gp Capt Bhattacharya
Lt Col VK Jha
Content : Sub SP Singh

Prepared by : Sgt Sukumar Reddy