CIS Governance Division
Cyber and Information Security Group,
National Informatics Centre,
A-Block, CGO Complex, Lodhi Road,
New Delhi - 110003 India
csg-advisory@nic.in

NIC-CISG/2024-10/547
Dated: 24-10-2024
Severity: High

Security Advisory in view of recent Vishing attacks

A. Description:

Voice phishing, commonly known as "vishing," is an increasingly prevalent form of social engineering attack where attackers use phone calls or voice messages to manipulate individuals into revealing sensitive information, such as login credentials, Personally Identifiable Information (PII), or financial details. In recent months, there has been an increase in vishing attacks targeting government officials to compromise confidential information and gain unauthorized access to government systems.

B. Tactics used in Vishing Attacks:

1. **Impersonation**: Attackers may impersonate trusted entities such as senior government officials, law enforcement agencies, or technical support personnel.
2. **Urgency**: Calls often convey a sense of urgency, coercing targets into revealing information by implying severe consequences for non-compliance.
3. **Technical Jargon**: Attackers may use complex technical language to confuse or intimidate targets, making them more likely to comply.
4. **Caller ID Spoofing**: Attackers manipulate caller ID information to make the call appear as if it is coming from a legitimate government number.

C. Cyber Security Precautions to be Undertaken:

- Always verify the caller's identity through official government channels before sharing sensitive information. Call back the organization or individual using publicly available contact information.
- Government officials should never share sensitive or confidential information over the phone and ensure only secured communication channels are used.
- Be suspicious of any unsolicited calls asking for personal or confidential information, especially when the caller is creating urgency or panic to pressure compliance. Take time to verify the information they provided.
- Conduct regular awareness training sessions on vishing attacks and social engineering tactics to ensure that all officials are aware of the latest trends, attack scenarios, and defence mechanisms.

- Be aware that Caller ID information can be easily spoofed. Do not trust the legitimacy of the caller based solely on the displayed number. Cross-check any caller claiming to represent an official agency with official records.
- Always download updates and patches from the Official website or Repositories of the OEM. Never download the updates/patches from any unauthorized third-party websites.
- Disable PowerShell in Windows based servers and client machines
- Don't store or exchange any sensitive information or credentials through third party messaging Apps/Email and social media.
- Be very vigilant while opening any attachments especially from unknown IDs.
- Don't store any credentials or passwords on your phone or computer
- Don't Use the same credentials on multiple websites/applications/servers/client machines
- Don't install any browser plugins or toolbars on the machine which is used for accessing the NDC
- Adhere to all Advisories published by NIC-CERT, Application Security and Cyber Information Security Group
- Take prompt action on any security issues pointed out by NIC-CERT/Application Security/Cyber Security –Divisions.
- In case of any security incident kindly report it to NIC-CERT at: **incident@nic-cert.nic.in**
  Everyone is requested to ensure strict adherence to the above-mentioned guidelines.