DSCI
PROMOTING DATA PROTECTION

OCTOBER 2020

NATIONAL CYBER SECURITY AWARENESS MONTH

#STAYCYBERSAFE

CYBERATTACK & FRAUD AWARENESS INFOGRAPHIC

PHISHING

Phishing uses fraudulent email messages designed to impersonate a legitimate person or organization and trick the recipient into downloading harmful attachments or divulging sensitive personal information.

Modus Operandi

- Cybercriminals either send random emails or launch targeted attacks against known email IDs.
- The email is designed to impersonate like it came from a legitimate source & urges to act.
- The recipient is tricked to download malwares, click links, or disclose account numbers, passwords, official data, etc.
- Cybercriminals get access to your computer/-network to launch ransomware/malware or use shared info to defraud money out of bank accounts.

How to Stay Safe

- Do not open suspicious emails or attachments claiming to be from well-known organizations, if you aren't expecting it.
- Verify URLs by hovering the cursor over links. If the URL doesn't match the link text or looks strange, it may be spoofed.
- Check for red flags, such as strange email addresses, grammatical mistakes or misspellings.
- Never share personal or financial information to anyone through emails.
- Use strict spam filtering for official and personal emails.

SOCIAL ENGINEERING

Cybercriminals forge a host of manipulating attempts using technology to trick users into giving away sensitive personal information. Few examples are vishing, pretexting, smishing, quid pro quo (impersonate support staff), etc.

Modus Operandi

- Fraudsters investigate the background of their intended targets and launch campaigned attacks.
- Mostly happens on call asking you to click on links, donate money, update account details, etc.
- They psychologically manipulate the victim taking advantage of their natural reactions.
- If followed, the user themselves reveal confidential information and gives access to financial data or sensitive information.

How to Stay Safe

- The golden rule is to avoid inbound customer service/technical service calls or email support requests.
- In case any tech support is needed, initiate it from your end after checking contact details from official websites only.
- Never entertain calls from people posing as bank representatives. Banks never call and ask for CVV/PIN/OTP. Never share.
- In case a remote co-worker calls and asks for account credentials or official information, keep the IT Security team in loop and do as instructed.
- Stay away from offers too good to be true.

DIGITAL PAYMENT FRAUDS

Digital Payment frauds are various methods cybercriminals forge to dupe users of their money by either tricking the victim pay & lose money on their own or share financial information to let them access & spindle money.

Modus Operandi

- **UPI Fraud:** Fraudsters call and in the pretext of sending money, sends a 'Money Request' instead and asks you to enter UPI PIN.
- **KYC Fraud:** Fake SMS or call received threatening to block bank account/wallet citing KYC non-compliance. Fraudsters call to facilitate the KYC process and trick users to get financial data.
- **Remote Access Fraud:** Fraudsters send link containing remote access apps like AnyDesk, QuickSupport or TeamViewer which when installed, gains access to the victim's phone/-computer.
- **Social Media Fraud:** Fraudsters spread fake customer care numbers of banks & wallet/UPI platforms on Social Media. If users call on such numbers, fraudsters pose as official representatives and dupe money.

How to Stay Safe

- UPI PIN is only needed to SEND money. Never enter UPI PIN when expecting a payment.
- Never entertain calls from people posing as bank representatives asking for your card/wallet/bank account information.
- Disconnect calls asking for KYC verification or bank account/card blocking.
- Do not search for Bank/UPI customer care numbers on search engines or social media. Always visit the official website.
- Never share any PIN/OTP/password ever on call/email/SMS.

REMOTE ACCESS TROJAN (RAT)

RAT is a malware program that allows cybercriminals to gain administrative control over the target computer. Once enabled, the intruder can do anything from accessing login credentials to stealthily acquire financial details.

Modus Operandi

- Cybercriminals send infected codes via email attachments, malicious online advertisements, free games, offers, and software 'cracks'.
- Once a user clicks or unknowingly installs it, the host system is compromised.
- Criminals use it to access and control the compromised devices and steal information from them. It usually interacts with and manages the Windows Registry.
- The intruder may also use it to distribute RATs to other vulnerable computers in the network.

How to Stay Safe

- Use only official websites and links to download applications.
- Enforce strong access control, enable MFA (multifactor authentication) .
- Avoid opening attachments received from unknown sources & use spam filters.
- Install software updates & patch vulnerabilities as soon as made available.
- To stay safe from RATs, follow the same measures to prevent malwares/ ransomwares.

RANSOMWARE

Ransomware is a type of malware that restricts users from accessing the system and demands to pay ransom in order to regain access.

Modus Operandi

- Cybercriminals load malwares within email attachments, fake websites, offers, etc. which when clicked/accesses by users unknowingly get installed on their systems.
- The ransomware encrypts various file formats with different file extensions.
- They steal credentials/sensitive information and block the user out of the system.
- Advanced ransomwares are designed to evade anti VM or Sandbox, so they can't be analysed by security researchers.

How to Stay Safe

- Protect your personal/official devices with licensed Antivirus.
- Install ad blockers to combat exploit kits such as Fallout that are distributed via malicious advertising.
- Lock Remote Desktop Protocol, if not in use or follow RDP best practices such as rate limiting, MFA, etc.
- Configure strong firewalls & VPN must have capability to test basic security protocols before connection.
- Deploy effective backup strategies including keeping the backup safe; so that they can be used to recover lost data in the event of an infection.

Follow NCSAM Campaign to know more Best Practices & #STAYCYBERSAFE

Presented by: Data Security Council of India