CYBER SECURITY AWARENESS

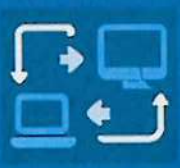
READY RECKONER FOR NAVAL VETERANS

USE STRONG PASSWORDS

Choose passwords that are hard to guess

BEWARE OF PHISHING

Do not click on suspicious links or attachments



SECURE YOUR DEVICES

Enable firewalls and use antivirus software

REPORTING

Report any suspicious activities or incidents on www.cybercrime.gov.in or 1930

THE GOLDEN RULE

THINK BEFORE YOU CLICK

**References have been drawn from MHA/I4C Handbook*

IMPORTANT GUIDELINES

Introduction

As members of the veteran community, your association with the Indian Navy continues to carry weight, both in pride and in responsibility. The digital landscape today is a battlefield where threats are stealthy, persistent, and evolving. This Ready Reckoner is issued to keep you informed, alert, and secure in the cyber domain.

Your Identity is Powerful - Even Beyond Service

- Even in retirement, your background, connections and ties to defence community may make you a potential target for cyber threats.
- Avoid sharing Personal Indentifiable Information (PII) and service-related information on Social Media Platforms.
- Do not engage in casual discussions about past postings, operations, or personnel—even with "fellow veterans" online unless verified.

A curated list of common methods used in cyber frauds and attacks, along with clear Dos and Don'ts has been compiled as a ready reckoner for the veteran community.

INDEX

INDEX

KYC Scam

KYC Fraud involves cybercriminals exploiting identity verification processes to steal personal information, commit identity theft, or access financial accounts illegally. This can lead to significant financial losses and reputational damage for individuals, businesses, and financial institutions. Common tactics include tricking people, forging documents, and creating fake identities.

Dos

- **Verify Requests:** Contact your bank or financial institution directly to confirm any KYC update requests.
- **Use Official Contacts:** Obtain contact numbers or customer care details only from the official website or trusted sources.
- **Report Incidents:** Inform your bank or financial institution immediately if you suspect any cyber fraud.
- **Check KYC Update Methods:** Enquire with your bank about the available methods for updating KYC details.

Don'ts

- **Protect Credentials:** Never share your account login details, card information, PINs, passwords, or OTPs with anyone or on unauthorised websites/apps.
- **Secure Documents:** Do not share KYC documents or their copies with unknown or unidentified individuals or organisations.
- **Avoid Suspicious Links:** Do not click on suspicious or unverified links received via mobile or email.

Phishing

Phishing is a common cybercrime tactic that deceives victims into clicking on fake links. These links appear as emails or websites from trusted sources but redirect users to fraudulent sites designed to steal sensitive data, such as login credentials, personal information, or financial details. Phishing can also install malware, giving cybercriminals unauthorised access to your device. Some identifiable Red Flags could be unfamiliar sender addresses, urgent language asking for action (for eg., 'Reset Password Now'), suspicious links or attachments.

Dos

- **Be Suspicious:** Treat unexpected messages from known sources with caution.
- **Check URLs:** Hover over links to reveal the genuine destination and spot discrepancies.
- **Verify Senders:** Contact the sender through a trusted method if you're unsure about a message's authenticity.
- **Update Regularly:** Keep your software and systems up-to-date to close security gaps.
- **Phishing Report:** Alert the relevant authorities or platforms if you encounter phishing attempts.

Don'ts

- **Avoid Clicking Links:** Don't click on suspicious links; delete messages from unknown senders immediately.
- **Unsubscribe & Block:** Unsubscribe from emails with suspicious links and block the sender's email.
- **Visit Official Websites:** Always go directly to the official website for financial transactions and verify website security (HTTPS with a padlock).

Deepfake Cybercrime

Cybercriminals are now using advanced artificial intelligence (AI) to create fake videos or voice recordings that look and sound real. They take real clips and change them to trick people. These fakes are shared through social media, messages, and emails. Often, they target well-known people or those in positions of power. The goal is to fool others, change their opinions, or spread lies. In some cases, these criminals pretend to be from the defence forces to ask for money or stir up strong emotions among the public.

Dos

- **Stay Informed:** Learn about deepfake technology and its risks.
- **Verify Content:** Always check the authenticity of media before sharing or believing it.
- **Use Trusted Sources:** Rely on reputable platforms for news and updates.
- **Report Suspicious Content:** Alert authorities or platforms if you find potential deepfakes.

Don'ts

- **Don't Share Unverified Media:** Avoid spreading content without checking its truthfulness.
- **Don't Trust Suspicious Sources:** Stay away from unreliable sources that may share deepfakes.
- **Don't Trust Blindly:** Be cautious of content that seems exaggerated or emotional.
- **Don't Ignore Privacy:** Review privacy settings and limit the personal info you share online

Online Shopping Fraud

Online Shopping Fraud is a cybercrime where fraudsters deceive victims into making illegitimate purchases. They create fake websites or manipulate legitimate platforms, offer deals that are too good to be true, and steal personal and financial information, leading to financial losses and mistrust in online marketplaces.

Dos

- **Compare Prices:** Compare prices on different e-commerce websites.
- Use Cash-on-Delivery: If a website seems suspicious, opt for the cash-on-delivery payment method.
- **Choose Verified Sellers:** Prefer buying from "Verified" or "Trusted" sellers on e-commerce websites.
- **Verify Offers:** Be cautious of offers that seem too good to be true.
- **Secure Transactions:** Remember, you never need to enter a PIN, password, or OTP to receive money.
- **Use strong, unique passwords.**

Don'ts

- **Compare Prices:** Compare prices on different e-commerce websites.
- **Use Cash-on-Delivery:** If a website seems suspicious, opt for the cash-on-delivery payment method.
- **Choose Verified Sellers:** Prefer buying from "Verified" or "Trusted" sellers on e-commerce websites.
- **Verify Offers:** Be cautious of offers that seem too good to be true.
- **Secure Transactions:** Remember, you never need to enter a PIN, password, or OTP to receive money.

Mobile Application Scam

Cybercriminals create **Fake Mobile Banking Apps** that closely resemble legitimate ones, using similar logos and interfaces. These apps are distributed through unofficial channels like third-party app stores or phishing links. Once installed, they steal your banking credentials and personal data, leading to financial fraud

Dos

- **Download from Official Stores:** Always download banking apps from trusted sources like Google Play Store or Apple App Store or bank websites.
- **Verify App Authenticity:** Check the developer details and read reviews before installing any banking app.
- **Keep Software Updated:** Ensure your phone's OS and security software are always current.
- **Enable Two-Factor Authentication (2FA):** Add an extra layer of security to your accounts.
- **Regularly Monitor Bank Accounts:** Review your bank account statements regularly for any unauthorised transactions.

Don'ts

- **Don't Download from Unofficial Links:** Avoid clicking on links or downloading apps from suspicious emails or websites.
- **Don't Enter Sensitive Info in Unknown Apps:** Never share banking details in unfamiliar apps or sites.
- **Don't Jailbreak Your Device:** Rooting your device makes it vulnerable to malware and attacks.
- **Don't Share Credentials:** Never share your banking PIN or OTP with anyone, even if they claim to be support staff.

Spam/Vishing Calls

Spam/Vishing Calls (voice phishing) are a deceptive form of cybercrime. Fraudsters use social engineering to trick victims into revealing sensitive information, like personal or financial data. They often impersonate legitimate entities, such as banks or government agencies, using tactics like caller ID spoofing and urgency to gain trust and steal information.

Dos

- **Use Call Blockers:** Install call-blocking apps and report spam calls.
- **Be Cautious:** Exercise caution when answering calls from unknown numbers.
- **Spread Awareness:** Educate others about common phone scams.
- **Enable Security:** Use voicemail passwords for added protection.

Don'ts

- **Don't Share Personal Info:** Never provide personal or financial information to unknown callers.
- **Don't Trust Caller ID:** Caller ID can be spoofed, so don't rely on it.
- **Avoid Unknown Numbers:** Don't return calls from unfamiliar or international numbers.
- **Protect Your Data:** Genuine institutions never ask for sensitive info like usernames, passwords, or OTPs. Never share these, even with family.

Quishing

Quishing Scams are on the rise. The scammer lure victims with promises of deals or convenience by asking to scan QR codes but ultimately initiate unauthorised financial transactions. Malicious codes can redirect users to phishing sites, steal login credentials, or transfer money directly to the scammer's account.

Dos

- **Scan Trusted Sources:** Only scan QR codes from official websites or verified businesses.
- **Verify Before Acting:** Scammers often create urgency—take your time to verify.
- **Report Suspicious Codes:** If you suspect a scam, report the code to the legitimate source and relevant authorities.

Don'ts

- **Be Cautious with Payments:** Avoid scanning QR codes with payment apps, as they may contain embedded account details for fraudulent transfers.
- **Don't Scan to Receive Money:** Never scan QR codes to receive funds. Legitimate transactions don't require scanning codes or entering banking details like m-PIN or passwords.
- **Avoid Unknown Sources:** Don't scan codes from emails, texts, or unfamiliar sources.

SMS, Email & Call Scams

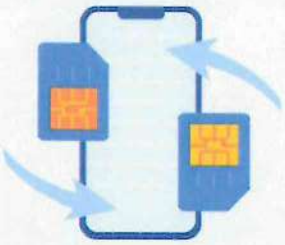
SMS, Email, and Call Scams are used by fraudsters to deceive victims with fake offers . They impersonate trusted NBFCs by using their logos and fake IDs, gaining credibility. Scammers may send counterfeit sanction letters or cheques, asking for upfront payments. Once the payment is made, the fraudsters disappear with the money.

Dos

- **Verify Authenticity:** Always cross-check sender details and contact official sources directly.
- **Report Suspicious Messages:** Forward any fake messages to official reporting channels and warn others.

Don'ts

- **Don't Trust Unsolicited Offers:** Never trust loan offers via phone, email, or text without verification.
- **Don't Share Sensitive Info:** Avoid giving personal or financial details without confirming the legitimacy of the offer.
- **Don't Click Links or Open Suspicious Emails:** Don't click on links or open emails from unknown sources with attachments or links.
- **Don't Pay Upfront Fees:** Genuine lenders don't require upfront payments for loan processing.



SIM Swapping

SIM Swapping is a cybercrime where fraudsters transfer your phone number to their SIM card. This gives them access to your calls, texts, and two-factor authentication codes, enabling identity theft, account hijacking, and financial fraud. Scammers often pose as network staff offering upgrades or benefits to trick you into revealing personal details.

Dos

- **Enable 2-Factor Authentication:** Add extra security to your accounts.
- **Use Strong PINs:** Set unique and hard-to-guess PINs for your accounts and SIM.
- **Stay Updated:** Keep your phone's software and apps regularly updated.
- **Report Suspicious Activity:** Contact your network provider immediately if you notice unusual activity or lose your SIM.

Don'ts

- **Protect Information:** Never store sensitive data or share OTPs with strangers via calls or texts.
- **Use Strong PINs:** Avoid easily guessable PINs for your accounts.
- **Report SIM Loss:** Notify your network provider immediately if your SIM card is lost.
- **Monitor Activity:** Watch for unusual mobile activity or extended loss of network access and act promptly.
- **Secure Credentials:** Never share identity details linked to your SIM card.

Money Mules

Money Mules are individuals, knowingly or unknowingly, used to launder illegally obtained funds. Scammers persuade them to receive and transfer stolen money in exchange for commissions. These funds are moved across multiple accounts to obscure the fraudster's identity. Involvement in such activities, whether intentional or not, is illegal and carries severe legal consequences.

Dos

- **Scrutinise Job Offers:** Be cautious of unsolicited jobs involving money transfers. Research the company's or individual's legitimacy.
- **Guard Financial Information:** Never share bank account details or personal information with unknown parties.
- **Report Suspicious Activity:** Contact authorities if you suspect a money mule scheme.

Don'ts

- **Don't Share Accounts:** Never let others use your account to receive or transfer funds.
- **Refuse Commissions:** Reject offers to handle unauthorised money for a fee.
- **Know the Risks:** Transferring illegitimate funds can lead to serious legal action.

Juice Jacking

Juice Jacking is a cybersecurity risk associated with compromised public USB charging stations. Hackers can exploit USB ports that charge and transfer data, using them to install malware or steal sensitive information. While no confirmed cases exist, staying vigilant is essential.

Dos

- **Carry Your Charger:** Use your own charger and cable to avoid potentially tampered public ports.
- **Verify Prompts:** Be cautious of "trust this device" prompts and accept only from trusted sources.
- **Opt for AC Outlets:** Choose standard electrical outlets whenever possible.

Don'ts

- **Avoid Public Ports:** Do not use unknown or public USB ports or cables.

AI Generated Imagery

The AI-generated imagery trend, particularly styles inspired by Ghibli, involves using AI to create stunning images-often based on real people or concepts. While it seems artistic and harmless, this technology poses a serious cyber security threat. Hackers can exploit publicly shared photos to generate images for identity spoofing, social engineering or deepfake scams. These can manipulate emotions and spread misinformation.

Dos

- **Limit Personal Image Sharing:** The less facial data available, harder it is for attackers to generate realistic fakes.
- **Check Privacy Controls:** Review privacy controls to understand data handling, storing and sharing.
- **Stay Updated**: Stay updated and current on the latest deepfake detecton.

Don'ts

- **Unknown Platforms:** Do not use unknown or untrusted AI platforms.
- **Facial Data:** Do not share photos with close-up of face.
- **Unusual Links/Photos:** Do not click on messages/ links/ photos that seem unusual even if they are sent from trusted contacts.

Best Practices for Mobile Handling

Securing mobile devices is more important than ever as our phones hold personal and financial information. To stay safe, your mobile must be safe. With just a few smart habits, you can keep your phone and your information safe from cybercriminals.

1. Use strong passcode or biometric lock (fingerprints/ face recognition).
2. Install apps only from trusted sources (Google Play Store/ Apple App Store).
3. Use two-factor authentication (2FA) for accounts.
4. Keep your OS and apps updated to patch security vulnerabilities.
5. Install antivirus software.
6. Turn off Bluetooth, Wi-Fi, Air Drop, NFC and location when not in use to avoid tracking or unauthorised access.
7. Clear cache/contacts/data/unused apps periodically.
8. Back up data regularly using cloud or encrypted storage.
9. Avoid syncing financial payment methods with Whatsapp (similar apps).
10. Avoid using public Wi-Fis/ Hotspots while making financial transactions.