

# CSIR CYBER SECURITY AWARENESS

## Beware and Stay Safe from **Cyber Attacks**

A cyberattack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Usually, the attacker seeks some type of benefit from disrupting the victim's network.

## User IT Equipment Security at Office

User IT equipment security refers to the practices and technologies used to protect individual user devices like laptops, desktops, and mobile phones from cyber threats.

### Do's



- ✔ Use Standard User accounts for regular work.
- ✔ Keep OS, Antivirus and BIOS updated with the latest patches.
- ✔ Always lock/log off desktops when not in use. And disable internet access to all devices.
- ✔ Configure printers to disable print history storage.
- ✔ Enable Desktop Firewall for data access.
- ✔ Use complex passwords with at least 8 characters, uppercase, lowercase, numbers, and special characters.
- ✔ Change passwords every 30 days, and enable Multi-Factor Authentication wherever possible.

### Don'ts



- ✘ Do not write sensitive info like passwords or IP addresses on unsecured material.
- ✘ Avoid using external mobile apps like Cam Scanner for government documents.
- ✘ Delete all pirated OS/software immediately
- ✘ Do not use unauthorized or non-approved software/applications.
- ✘ Do not reuse passwords across multiple services/websites/apps
- ✘ Avoid saving passwords in browsers or unprotected documents
- ✘ Never share system, printer, or Wi-Fi passwords with unauthorized persons.



# CSIR CYBER SECURITY AWARENESS

## Beware and Stay Safe from **Cyber Attacks**








### Internet Browsing and Email Security

Internet browsing security involves protecting online activities from cyber threats like phishing, malware, and unauthorized access. It includes using updated browsers, enabling security features, and avoiding suspicious websites and links.

Email security focuses on safeguarding email communications from threats such as phishing, malware, and unauthorized access. It involves using strong passwords, and being cautious about opening suspicious emails or attachments.








## Do's



-  Use Private/Incognito Mode for government, email, banking, or sensitive services.
-  Manually type the URL/domain name instead of clicking on links.
-  Use the latest version of browsers and keep them updated.
-  Configure Kavach Multi-Factor Authentication on NIC email accounts.
-  Download the Kavach app only from valid app stores.
-  Regularly review NIC email login history and report any discrepancies.
-  Use PGP or digital certificates to encrypt important emails.

## Don'ts



-  Avoid storing payment details in the browser.
-  Do not use 3rd-party anonymization services like VPNs, Tor, or proxies.
-  Never download unauthorized or pirated content from the internet. Do not open links or attachments from unknown senders.
-  Do not use official systems for installing or playing games.
-  Be cautious with shortened URLs, as they may lead to phishing or malware sites.
-  Do not share email passwords or Kavach OTPs with unauthorized persons.
-  Avoid using external/unauthorized email services for official communication.



# CSIR CYBER SECURITY AWARENESS

## Beware and Stay Safe from **Cyber Attacks**

### Social Media Security

Social media security focuses on protecting personal and organizational information shared on social platforms from threats like phishing, identity theft, and unauthorized access. It involves enabling strong authentication, being cautious with sharing sensitive data, avoiding suspicious links, and regularly reviewing account privacy settings to prevent misuse or cyberattacks.

### Do's



- ✔ Limit sharing of personal information on social media.
- ✔ Verify a contact's authenticity before accepting friend requests.
- ✔ Enable Multi-Factor Authentication for account security.
- ✔ Regularly review and update privacy settings to control who can view your content.
- ✔ Enable account activity alerts to monitor unauthorized access.
- ✔ Use secure, trusted apps for social media management.
- ✔ Log out from accounts when using shared or public devices.

### Don'ts



- ✘ Do not click on links or files from unknown contacts/users.
- ✘ Avoid sharing internal government documents on social media.
- ✘ Do not post unverified information on social platforms.
- ✘ Never share your @gov.in/@nic.in email address on social media.
- ✘ Avoid using third-party apps; prefer NIC's Sandes App for official communication.
- ✘ Avoid using public Wi-Fi when accessing social media accounts.
- ✘ Do not download apps or content from untrusted sources linked through social media.



# CSIR CYBER SECURITY AWARENESS

## Beware and Stay Safe from **Cyber Attacks**

### Mobile Security

Mobile security refers to safeguarding mobile devices and their data from unauthorized access, malware, phishing, and other cyber threats. It includes updating software, using strong authentication, avoiding malicious apps, and ensuring secure communication to protect sensitive information and maintain device integrity. Regularly backing up data and enabling remote wipe features are also essential for enhanced protection.

### Do's



- ✔ Keep the mobile OS and latest Antivirus updated with the latest patches.
- ✔ Download apps only from official app stores (Google Play/Apple Store).
- ✔ Check app popularity and user reviews before downloading.
- ✔ Note down the IMEI number and keep it offline for emergencies.
- ✔ Use auto-lock with passcode or security patterns. Enable Mobile Tracking for lost/stolen devices. Take regular offline backups of your data.
- ✔ Scan files with antivirus software before transferring to your mobile.

### Don'ts



- ✘ Do not root or jailbreak your mobile device. Avoid enabling Wi-Fi, GPS, Bluetooth, or NFC unless necessary.
- ✘ Do not accept unknown Bluetooth/file sharing requests.
- ✘ Avoid apps requesting unnecessary permissions (e.g., GPS for a calculator).
- ✘ Do not open suspicious links from SMS or social media. Disable automatic downloads on your phone.
- ✘ Avoid apps with bad reputations or low user bases.
- ✘ Do not store sensitive data without securing it on your phone.



# CSIR CYBER SECURITY AWARENESS

## Beware and Stay Safe from **SPEAR PHISHING ATTACKS**

Spear Phishing is a type of phishing attack, where the attacker targets a specific or a group of individuals or a Department, with customized phishing content tailor made to compromise the target.



## COMMON TRAITS OF SPEAR PHISHING MAILS TARGETED AT CSIR EMPLOYEES

**01** The Sender & Recipient of the Phishing Mail would be the same Email Address. You will be in Bcc

**02** Use of Shortened URLs for links (ex: <https://tinyurl.cc/alkm3>)

**03** Use of Subject like : Conference/Lecture Invite, Research Paper, Foreign Visit, DA Hike, Arrears, Pay Fixation, Tender, Bill Payment, Meeting Request, VPN, Email Migration...etc

**04** Mails with Password Protected Attachments, where password is shared in the Mail body

**05** Mails advising you to download an Application / Software hosted on external links (i.e., other than "\*.csir.res.in" or "\*.gov.in" or "\*.nic.in" sites) for accessing a CSIR or Govt Application / Service

## WHAT TO DO IF YOU RECEIVE A PHISHING/SUSPICIOUS MAIL

- Don't Click on the URLs /Links present in the Mail
- Don't open the attachments present in the Mail
- Don't respond to the Mail
- Don't Upload or share the contents of the Mail with any external/3<sup>rd</sup> party sites or Apps
- Report the mail to [incident@csir.res.in](mailto:incident@csir.res.in)

