ONLINE BANKING SAFETY



- For mobile banking, download only the verified official app of your bank.
- Do not click on links embedded in emails claiming to be from your bank. Instead, type your bank's web address directly in the browser and navigate from there.
- Use a strong password for online banking and change passwords periodically.
- Always use the virtual keyboard for logging into your net-banking account.
- Do not use public Wi-Fi/cyber café/ public computers for online banking.
- Never share your net-banking credentials, passwords, Credit/Debit card numbers, PINS, CVV with anyone.
- Use a different phone number for your banking apps than for other Apps.



National Cyber Security Awareness Month

October 2026 Day 25

National Helpline 1930 | Cyber Crime Reporting Portal: cybercrime.gov.in

Artwork by Janhabee | Image by Meta

Online Payment Security



- You never need to enter your UPI PIN to receive money. If someone asks you to enter your PIN to "receive" a payment, it's a scam.
- Scanning a QR code is only for paying. You never need to scan a QR code to get money.
- At shops, before you pay, check that the name shown on your screen matches the shop name.
- Check the receiver's name before confirming a payment. When sending money to someone new, send a small amount first.
- Be suspicious of a stranger claiming a "wrong transfer, please return." Don't send it back yourself – ask them to raise it through their bank or UPI App.
- Read every "collect request" carefully before approving it. Scammers send requests labelled as "refund," "prize," or "cashback."



National Cyber Security Awareness Month **October 2026 Day 27**

National Helpline 1930 | Cyber Crime Reporting Portal: cybercrime.gov.in

Security Tips by Anurag | Artwork by Janhabee | Image by Meta

Protect Your SMART PHONE



- Keep mobile data and location turned OFF when not needed.
- Change your smartphone settings so it does not automatically connect to nearby Wi-Fi networks.
- Turn OFF NFC (Near Field Communication) when not in use. NFC is a short-range wireless technology that allows data exchange between devices.
- Always use a strong Password, PIN, or Pattern Lock on your mobile device. Configure screen timeout lock to trigger within few seconds of inactivity.
- If someone approaches you saying their phone is lost or out of battery and asks to use your phone to make an emergency call, don't hand over your phone.
- Don't let anybody dial anything from your phone.

National Cyber Security Awareness Month

October 2026 Day 20



National Helpline 1930 | Cyber Crime Reporting Portal: cybercrime.gov.in

Artwork by Janhabee | Image by Meta

Be SOCIAL in Social Media

Various undesirable incidents of "public outrage" and "mob lynching" happen due to viral propagation of **FAKE NEWS** through social media platforms.



- Do not accept any image, video, or news received on social media as true unless its authenticity is verified from other reliable sources.
- Do not post or forward any controversial image, video, or news that claims to report an incident or event, unless it is corroborated by a trusted source.
- If you find fake or hateful content, report it on the platform. Don't argue in the comments and make it more viral.
- Never spread rumours. Use social media for good, and let there be peace in the world.



National Cyber Security Awareness Month

October 2026 Day 17

National Helpline 1930 | Cyber Crime Reporting Portal: cybercrime.gov.in

Artwork by Janhabee | Image by Meta

Password Security

Your password is your first line of defence against hackers and unauthorized access to your accounts.



- Always use Strong and Unique Password. Don't use the same password for multiple accounts, especially for the most sensitive ones, such as bank accounts, credit cards, tax records etc.
- If one password gets hacked, your all other accounts with the same password will be compromised.
- Never click on "Remember Password" option.
- Never share password with anyone. If you suspect that it has been compromised, change your password immediately.
- Use a password manager to store multiple unique passwords of various accounts.



National Cyber Security Awareness Month

October 2026 Day 19

National Helpline 1930 | Cyber Crime Reporting Portal: cybercrime.gov.in

Artwork by Janhabee | Image by Meta

SCAREWARE

is a scam that uses fake virus warnings to create shock and fear, tricking you into downloading dangerous software, like fake antivirus, or calling a fake support number.



- Don't click the "Scan Now" / "Fix" / "Download" button in the pop-up. That's the trap.
- Don't tap or click anywhere inside the pop-up, not even the "X" inside the alert box.
- Never call the phone number shown in the pop-up. That's the tech-support scam.
- Close the browser instead: Alt + F4 on Windows, Cmd + W on Mac, or swipe the tab away on your phone.
- Use a reputable antivirus from its official website only, never from a pop-up or Ad. Windows Defender, already on your PC, is a solid free option.
- Keep your browser, OS and antivirus updated.
- Run virus scans ONLY with your real, installed antivirus, on a regular basis.
- Enable the pop-up blocker in your browser.
- If you already clicked: disconnect from the internet, run a full scan with your real antivirus, and change your important passwords.

Golden Rule: If it creates URGENCY + FEAR, it's almost certainly scareware.
Stop! Breathe!! Close!!!



National Cyber Security Awareness Month
October 2026 Day 14

Security Tips by Anurag | Artwork by Janhabee | Image by Meta

Safety Tips for WhatsApp



- Turn on the two-step verification.
- Never click on unverified links received on WhatsApp.
- Block and report suspicious accounts.
- Change privacy settings to control who sees your details.
- Take advantage of Disappearing Messages.
- Enhance privacy with 'View Once' for shared content.
- Regularly check devices linked to your WhatsApp account.



National Cyber Security Awareness Month

October 2026 Day 13

National Helpline 1930 | Cyber Crime Reporting Portal: cybercrime.gov.in

Artwork by Janhabee | Image by Meta

Beware of

Fake Social Media Profiles

Not every profile is real, and not all information shared online is true.



- Be cautious when accepting friend requests from strangers.
- Avoid connecting with people you don't know or cannot verify from other reliable sources.
- Verify profiles before trusting — check for verified badges, mutual friends, and genuine posts.
- Adjust your privacy settings to ensure only your friends can view your activities and join your conversations.



National Cyber Security Awareness Month **October 2026 Day 15**

National Helpline 1930 | Cyber Crime Reporting Portal: cybercrime.gov.in

Artwork by Janhabee | Image by Meta

Safe Use of Mobile Apps

- Do not download Apps from untrusted sources / link.
- Always use licensed anti-virus software for your smartphone and scan your device at a regular interval.
- Do not give unnecessary permissions to Apps that you install on your smart phones.
- Do not keep any App or software in your device which you do not use regularly.
- Regularly install latest updates for all the app/software you are using in your smart phone.
- Turn on automatic updates.



Remember, if your device is compromised, criminals may have access to all your data through your cloud storage such as iCloud or Google Drive. So keep only minimum necessary information in your mobile devices.



National Cyber Security Awareness Month **October 2026 Day 11**

National Helpline 1930 | Cyber Crime Reporting Portal: cybercrime.gov.in

Artwork by Janhabee | Image by Meta

Go for Genuine

Always use Licensed Operating System, Antivirus, Firewall and Software.



- Don't download and install pirated software or anything else from random sites off the internet. Many of them are malware ridden.
- As and when companies find bugs in their software and OS, they also fix them by releasing security patches. Run software and App updates as soon as they are available. These updates fix software vulnerabilities and security problems.
- Turn on automatic updates.



National Cyber Security Awareness Month

October 2026 Day 10

Artwork by Janhabee | Image by Meta

Beware of Installing
REMOTE ACCESS APPS



- Never grant remote access to anyone who contacts you unexpectedly, even if they claim to be from a legitimate company.
- Never download and install remote access apps like TeamViewer or AnyDesk if advised by any unknown caller.
- When you realise that criminals have gained control over your phone through some remote access app, immediately disconnect the internet. The criminal will lose control over your phone.
- Uninstall the Remote Access App from your phone.

Visit the Bot Clearing Portal
https://www.csk.gov.in/security-tools.html
Download the botnet removal tool and run it on your device.

National Cyber Security Awareness Month **October 2026 Day 12**



National Helpline 1930 | Cyber Crime Reporting Portal: cybercrime.gov.in

Artwork by Janhabee | Image by Meta

The Online Shopping Scam

Criminals often exploit specific festival times of the year or ongoing big events in their scams.

Beware of clicking on phishing URLs to grab special offers like big discounts, winning prizes, rewards, cash-back offers or filling up customer review forms for lucky draw.



- Check that the online shopping site starts with https://
- Do not purchase from spam or phishing emails.
- Beware if prices are ridiculously low.
- While shopping online you need to provide only payment related information and delivery address. Don't give more private information.
- Go for Cash on Delivery (COD).



National Cyber Security Awareness Month

October 2026 Day 08

National Helpline 1930 | Cyber Crime Reporting Portal: cybercrime.gov.in

Artwork by Janhabee | Image by Meta

OTP Security

Banks and official services never ask your OTP.
Keep it secret! Keep it safe!



- Never share OTP or any validation code with anyone.
- Always verify the transaction details before entering an OTP.
- Never enter an OTP on a website or app you do not recognize.
- OTP messages always come with a text where purpose of OTP is mentioned very clearly. Read it carefully.



National Cyber Security Awareness Month **October 2026 Day 23**

National Helpline 1930 | Cyber Crime Reporting Portal: cybercrime.gov.in

Artwork by Janhabee | Image by Meta

Beware of FAKE Customer Care Numbers

Criminals make their Fake Websites containing Fake Customer Care Numbers appear at the top by using Search Engine Optimisation technic.



- Do not search helpline numbers on search engines / social media sites.
- Check the purchase invoice for the official contact number of the company.
- Check the official website of the organisation for their service centre number.



National Cyber Security Awareness Month

October 2026 Day 09

Artwork by Janhabee | Image by Meta

Protect Your Device



- Never leave your computer unattended with sensitive information visible on the screen.
- Always lock your screen when stepping away — use "Windows + L"
- Secure all your devices — PCs, laptops, tablets, and smartphones — with Strong Passwords to prevent unauthorized access.
- A very good idea is to enable a Screensaver with a timeout of no more than 2 minutes.
- Do not plug in unknown USB drives or external devices. Always Scan all removable devices with anti-virus before using them.



National Cyber Security Awareness Month

October 2026 Day 24

National Helpline 1930 | Cyber Crime Reporting Portal: cybercrime.gov.in

Artwork by Janhabee | Image by Meta

DIGITAL ARREST SCAM

Real police or courts never question or arrest people via video calls.



If you receive A PHONE CALL

- Claiming from some legal authority
- Saying a parcel containing illegal drugs/passport/other items has been seized
- It was sent using your details and you are involved in this
- Threatening for legal proceedings against you
- Demanding for money to "settle" fake charges or warrants

Don't panic Don't respond
It's a SCAM

- ✓ Do not attend online interrogation by fake police officer.
- ✓ Do not send money or share personal details.
- ✓ Disconnect the call right away.

Report the phone number with CHAKSU at
https://sancharsaathi.gov.in/



National Cyber Security Awareness Month

October 2026 Day 22

National Helpline 1930 | Cyber Crime Reporting Portal: cybercrime.gov.in

Artwork by Janhabee | Image by Meta

Bluetooth Protection



- Turn Off When Not Needed.
- Set Bluetooth to "Non-discoverable" mode. Don't allow your device to be found by all.
- Don't Pair new devices in crowded places. Attackers can intercept pairing code.
- Reject Unknown Pairing Requests. If you get a random pairing request – DECLINE immediately. That's Bluejacking / Bluesnarfing attack.
- Use Strong Pairing Authentication such as PINs or passkeys.
- Devices should be set to require manual approval before pairing.
- Enable "File Transfer Alert".
- Regularly update device firmware to ensure that latest security patches are applied.
- Remove Old Paired Devices. Delete old phones, speakers, shop's devices you no longer use. They can auto-connect.
- For PC/Laptop turn OFF Bluetooth file transfer if not needed.
- Before giving phone/laptop for repair/exchange – unpair ALL Bluetooth devices.
- For smart gadgets, use Apps that support encrypted Bluetooth (BLE Secure Connections).

National Cyber Security Awareness Month **October 2026** **Day 28**



National Helpline 1930 | Cyber Crime Reporting Portal: cybercrime.gov.in

Artwork by Janhabee | Image by Meta