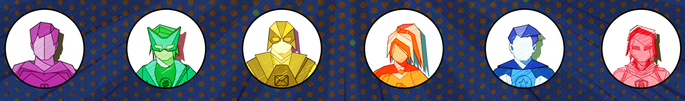
SECURE OUR WORLD

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

CYBER SAFETY ESSENTIALS FOR SENIOR CITIZENS



CYBER SCAMS TO BE AWARE OF

(While anyone can be affected by these scams, senior citizens may be particularly vulnerable to falling prey)

INSURANCE POLICY FRAUD

The senior citizens are targeted and tricked of insurance schemes where fraudsters posing as financial advisors or insurance agents convince seniors to buy fake policies or invest in fraudulent schemes, stealing their savings with the objective to steal their lifelong savings.

Safety Tips

- Research the insurance company or scheme independently through official websites or trusted sources.
- Always verify the insurance agent's credentials with the official insurance company before purchasing any policy.
- Go through the insurance policy documents carefully and ask for written confirmation before the final purchase.

SOCIAL MEDIA SCAMS

Hackers create fake accounts to connect to older adults as a friend or grandchildren, to later convince them for sending money, gifts or other personal favors.

Safety Tips

- Always confirm with a trusted family member before sending money to someone who claims to be a relative or friend on social media platforms.
- Verify if the person sending a friend request is truly who they claim to be, especially if they say they are a relative or grandchild.
- Avoid sharing your most personal information on social media, as scammers can use it to manipulate you anytime.

BANKING & FINANCIAL FRAUDS

Fraudsters trick seniors into sharing personal details like card numbers, OTPs, or passwords, often by offering fake gifts, free trials, or help with KYC/card renewal.

Safety Tips

- Banks will never ask for your PIN, OTP, or passwords. Be cautious of anyone requesting this information.
- Hang up if someone calls claiming to be from your bank and asks for sensitive information. Always call your bank using official numbers.
- Set up SMS or email alerts for every transaction to stay informed about any activity on your bank account.

ONLINE SHOPPING SCAMS

Scammers create fake websites that look real, selling non-existent products, often at very low prices. They might never deliver the product, or deliver poor-quality items, especially during high-demand periods like festivals.

Safety Tips

- Only purchase from reputable and well-known e-commerce websites. Double-check the website URLs in the address bar to ensure whether it is legitimate.
- If a deal seems too good to be true, it probably is. Think before making any final purchases online.
- Read customer reviews and ratings on shopping apps and websites to ensure the seller is reliable.

TECH SUPPORT SCAMS

Pop-ups or fake ads may trick seniors into believing their devices are infected. They might be fooled into downloading malicious software or giving control of their device to scammers who demand payment for fake repairs or upgrades.

Safety Tips

- If a pop-up or unsolicited message claims your computer is infected, ignore it. Legitimate companies don't offer tech support this way.
- If someone calls claiming to be from tech support, hang up and contact the official company directly to verify.
- Don't provide credit card information or make payments to anyone who claims to fix a random tech problem.

YOUR CYBER SAFETY CHECKLIST

- [ ] Learn the basics of computer, mobile, and internet security settings and features. If needed, ask for help from a trusted person.
- [ ] If your children are abroad, do not trust calls from unknown numbers claiming to be from them for any unusual request or threatening harm to them in any form. Always verify their safety by contacting them directly first.
- [ ] Never indulge in calls asking for sensitive information, even if they claim to be from trusted services like banks or Aadhaar department.
- [ ] For online shopping involving transactions, only trust or shop from well-known and reputable websites. If you need assistance, consider asking your grandkids or kids for help.
- [ ] Do not open attachments or click on links in emails from unknown or unverified sources.
- [ ] Be suspicious of offers that seem too good to be true, like lotteries or free gifts. Think before clicking on such links.
- [ ] Avoid sharing personal details like your phone number, address, or date of birth publicly on social media platforms.
- [ ] Enable multi-factor authentication for your online accounts to add an extra layer of security. Use a PIN, password, fingerprint, or facial recognition to lock your mobile devices.
- [ ] Avoid making charitable contributions over the phone unless you're absolutely sure it's legitimate.
- [ ] If you live alone or are unsure about online activities, have a trusted person assist you with your online tasks.

*Do you know that the **Chakshu Portal** is an innovative initiative by the Department of Telecommunication (DoT), GoI which is designed to curb cyber frauds across India. The portal facilitates citizens to report the suspected numbers/spam calls with the intention of defrauding telecom service users for cyber-crime, financial frauds, non-bonafide purpose like impersonation or any other misuse through Call, SMS or WhatsApp.* ***Source : Sanchar Saathi Portal of DoT***

Senior citizens can also reach out to **'Elder Line- 14567,' a National Helpline Number** *by the Ministry of Social Justice and Empowerment, for guidance, emotional support, and assistance in times of distress or unsafe situations, including intervention for abuse and rescue.*

ACT NOW TO PROTECT YOURSELF ONLINE

Stay Smart & Alert

Trust your instincts. If something feels off, avoid responding, sharing and believing anything online or on a call.

Talk to Others

Seek advice from a trusted family member, friend, or neighbor to safely navigate the online world.

Report Scams

In case you are a cyber crime victim Call 1930 or visit https://cybercrime.gov.in to register your complaint.