

ONLINE SAFETY BASICS

A simple guide covering various Online Safety aspects for our Digital well-being.

MAKE **CYBER
SAFETY** A HABIT



#StayCyberSafe

<https://www.dsci.in/content/stay-cyber-safe>



BASIC CYBER SAFETY PRACTICES

Online safety begins with passwords. They are the gatekeepers to your data/accounts. Choose a good one!



- Make passwords long, complex & unique. Use 'passphrases- a series of random words' and enable two-factor authentication wherever applicable.
- Use password managers to manage multiple complex passwords.
- Install antivirus and keep operating systems updated with the latest version.
- Install only licensed software versions from official websites and apps from reputed stores.
- Change the default router name and password of your Wi-Fi network.
- Set regular data backups locally and/or on cloud for disaster recovery.
- Erase all data and set to factory defaults before selling devices.

PRIVACY PRACTICES

- Be mindful of what you share online and what is being collected through apps & websites.
- Don't give unnecessary permissions to apps. Be mindful of the purpose before you allow.
- Consciously check and configure privacy settings of Social Media platforms and apps.
- Do not share sensitive information online especially on social networking sites.
- Limit cookies and allow only for trusted websites. Avoid third-party cookies.

DIGITAL PAYMENT SAFETY



- UPI PIN is NOT needed to RECEIVE money. Never share when expecting a payment.
- Bank or any customer care will never ask for your details such as Card CVV, PIN, UPI M-PIN or OTP. Keep it confidential and NEVER SHARE.
- Double-check the beneficiary account and/or mobile number before transferring money.
- Ensure online banking as well as websites where you make online payments are **https** secure or display the  icon.
- Do not use unsecure/open Wi-Fi networks/hotspots for online payments.

Beware of fake bank apps and check payment website URLs closely.



INTERNET SAFETY PRACTICES

- Avoid saving passwords in browsers and check browser security settings.
- Do not fall prey to Adware. Ads displaying offers too good to be true are just baits laid by cybercriminals.
- Visit only trusted sites and always check for **https** or the  sign while browsing.
- Check the integrity of URLs before surfing. They may look identical to a legitimate site, but the URL will have a variation in spelling or a different domain (e.g., .com vs. .org).
- Stay away from Phishing emails. To stay safe, always check the sender's address, URLs within the email, spelling & layout, attachments, etc. to identify the authenticity of an email.
- Keep an eye on automatic content download. These can be trojans, viruses, ransomwares.

ONLINE SAFETY OF KIDS

- Make kids comfortable to be able to walk up to parents for any help.
- Teach kids about Digital Footprint, Netiquette and Cyber Bullying.
- Educate kids to respects others and be polite online just as in real life.
- Limit screen time and exposure to video games.
- Educate them about the dangers of online games like Blue Whale, Fire Fairy, etc. Counsel them to share if someone approaches for playing games online.
- Create a separate user account for kids with limited permissions for online services.
- Monitor online activities of kids depending on their age and discuss issues.

Digital Burnout is on the rise. Make kids understand the importance of real interactions.



BE DIGITALLY EDUCATED

Do not just adopt a Digital Lifestyle; strive for Digital Transformation. Spend time to learn about the safety aspects of the services you like to use.

BE WISE, MONEYWISE

By never sharing OTP & PIN, you can safeguard yourself from payment frauds to a huge extent. They are meant to be entered personally, not shared publicly.

BE PRIVACY CONSCIOUS

Never share more than necessary and be aware of the purpose of the data being collected. Be extra cautious with personal data.

#StayCyberSafe