



ENSURE PASSWORD HYGIENE

Passwords are the gatekeepers to your accounts and key to almost everything you do online.

Follow these simple ways to keep your passwords secure and hard to crack!

BEST PRACTICES



Keep long, complex, and unique passwords ideally with over eight characters in length, include both upper and lowercase letters, numbers, and symbols with the support of passphrases.

Use multifactor authentication by adding a second layer of security ideally using your phone number or email ID.



Avoid saving passwords in browsers and use password managers to manage multiple complex passwords.

Enable your phone's fingerprint or facial recognition feature for authenticating apps.



Make a habit to use different passwords for different accounts.

Never reveal your passwords! You probably wouldn't give your ATM card and PIN to a stranger. So, why would you give away your username and password?



MAINTAIN SOCIAL MEDIA HYGIENE



Social media has linked people and businesses worldwide.

To keep your personal identity and security of social accounts safe, follow these effective tips!

BEST PRACTICES



Avoid sharing sensitive personal details, financial details, DOB, house address and contact details on social media.



Review the privacy and security settings of your social accounts periodically.



Don't fall for fake news updates coming from unverified accounts. Rely on verified accounts only for news updates.



Think before you act! Avoid clicking on any enticing link received over chat, DM, posts, etc.



Block accounts posting objectionable content and report suspicious activity immediately.



Be careful of whom you meet online as you would in your in-person social life.



A NASSCOM® Initiative

CYBER SECURITY AWARENESS MONTH

SEE YOURSELF IN CYBER

TOGETHER
WE MAKE IT SAFER

CYBER SECURITY
BEST PRACTICES
A GUIDE TO STAY CYBER SAFE



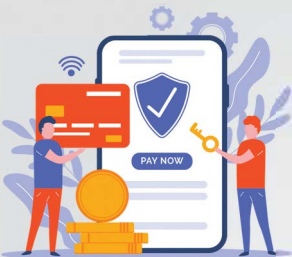
SUPPORTED BY



LastPass

Quick Heal

Securing Futures
A CSR initiative



DRIVE SAFE & SECURE DIGITAL PAYMENTS

Digital payments come with a lot of convenience and ease, but one has to stay extra alert and cautious while making online transactions through digital banking!

BEST PRACTICES



Never share any PIN/OTP password ever on call/email/SMS.

UPI PIN is only needed to SEND money. Never enter UPI PIN when expecting a payment.



Never entertain calls from people posing as bank representatives asking for your CVV/card/wallet bank account information.

Ensure online banking websites are HTTPS secured.



Don't use unsecure/open Wi-Fi networks to make online payments.

Download mobile banking/UPI based apps only from legitimate app stores.



RECOGNIZE & PREVENT PHISHING ATTACKS

Phishing attacks are constantly evolving. Be alert and practice smart measures to prevent falling victim to phishing attacks.



BEST PRACTICES



Do not open suspicious emails or attachments claiming to be from well-known organisations, if you aren't expecting it.



Check for red flags, such as strange email addresses grammatical mistakes or misspellings.



Legitimate emails usually don't demand immediate action. Be sceptical if they do!



Verify URLs by hovering the cursor over links. If the link doesn't match the text description or looks strange, it may be spoofed.



Never share personal or financial information to anyone over email.



Use stricter spam filtering for official and personal emails.



DEVICE SAFETY

Just like cars, your electronic devices need regular maintenance. With a little caution and latest updates, you can help prevent your devices from crashing!

BEST PRACTICES



Act promptly! If you see a software update notification, don't delay it. Better keep auto-updates ON.

Software updates are not limited to laptops or desktop computers. Keep your mobile devices in mind as well.



Install only licensed versions from official app stores/websites.

For portable media, perform full scan of hard drives, pen drives and SD cards with an updated antivirus before you open/use them.



Do not install freeware/antivirus/online games from online links.

Never leave your devices unattended, keep them locked when away from laptop screens.



1 /dsci.connect 2 /DSCI_Connect 3 /dsci.connect 4 /dscivideo 5 /data-security-council-of-india/
4th Floor, NASSCOM Campus, Plot No. 7-10, Sector 126, Noida, UP -201303
6 www.dsci.in

