Investor awareness regarding Cybersecurity risks

Please be suspicious of emails from unknown senders. Don't click embedded hyperlinks or open email attachments from senders you don't know. Simply opening an attachment or clicking on an embedded hyperlink can download malicious code onto your computer. If that happens, your key strokes may be logged and your sensitive information may be sent to a remote server managed by cyber criminals. Visit websites responsibly and do not visit sites with suspicious content.

If you are not entirely sure an email is legitimate, don't reply to the email even if it seems to come from someone you know. Instead, you may want to contact the sender for validation through your own trusted means.

If you receive a suspicious email/message claiming to contain links to Citi websites or if you believe you've encountered a page designed to look like another page (phishing email/phishing site) in an attempt to steal users' personal information, you may report the same to your Citi representative.

Please refrain from engaging /responding to Call/ SMS from unknown numbers.

DO NOT share your login credentials with anyone, always keep it confidential. Citibank never requires customers to share their login credentials (such as password, OTP or PIN) with anyone. If someone acquires your password – through innocent or malicious intent – they could gain unauthorized access to your account, putting your information, data and assets at risk.

In case fraud has already happened, report the same to Cyber Crime helpline number 1930 or website www.cybercrime.gov.in

For more resources on cyber security risks and awareness, kindly refer to <u>Information Security</u> <u>Education and Awareness</u>; <u>Cybersecurity</u>





Always properly log out after completion of online transactions





Clear cookies and delete browsing history at the end of session and stay safe





Giving out your personal information online is not advisable





Keep software up to date





Only install apps and software from trusted sources



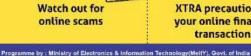
Scan any file downloaded from internet before opening/using/installing



Watch out for



online scams



& Cyber Safe





ABCs of Information Security Awareness





Do not carry your PIN number in wallets better to memorize your PIN





Help yourself to maintain a positive online presence



Lock your devices when not in use





Pay extra attention when using public Wi-Fi



Turn on Automatic Updates for your operating system





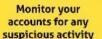
XTRA precaution for your online financial transactions

Enlighten yourself on Cyber Security measures









Ouarantine all unused apps



Use strong passwords with personal acronym



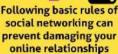
Your priority on cyber security makes you cyber aware citizen

Be careful

what you click

www

infoSec awareness.in







Join hands to stop spreading fake news



Never believe on forward messages, check source and URL





Respect the privacy of others





Verify with whom you are interacting online





Supported by : Ministry of Home Affairs (MHA), Govt. of India



















Information Security Education & Awareness

Department of Electronics & Information Technology, Ministry of Communications & Information Technology, Government of India.







Guidelines for passwords

- ✓ Use different passwords for different accounts
- ✓ Change your passwords regularly
- ✓ Your brain is the best place to store your passwords
- Never use your personal information for passwords
- ✓ Beware of shoulder surfing
- ✓ Avoid using dictionary words as password

Hard to remember PASSWORD P@\$\$wor9

Switch to a PASSPHRASE

My passphrase

Never judge a book by its cover

My password

nJ@66!C

never Judge @ 600k 6y !ts Cover What will your passphrase be?



For queries on Information Security Call us to Toll Free No.

1800 425 6235

between 10 AM to 6 PM or give us







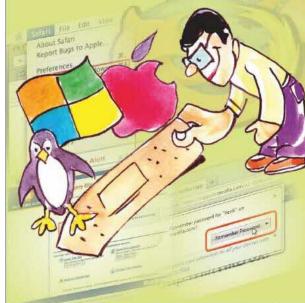
BROWSER SECURITY

Block pop-up windows in your browser

Disable the login and remembering password information

Have "Safe Search"ON in Search Engines





Use Privacy or Security settings which are inbuilt in the browser

Always update your Web-browser with latest patches



For queries on Information Security

1800 425 6235

between 10 AM to 6 PM or give us a missed call we will call you back in 24 hrs

