Transaction Analysts (India) Pvt. Ltd.
#4, Sathyam Arcade, 1st Floor, 1st Phase, BTM Layout 2nd Stage, Bangalore - 560076
info@transactionanalysts.com + 91 80 26784479

General TIPs for Cyber Security

- Always keep your systems/devices (desktop, laptop, mobile) updated with latest patches.
- Protect systems/devices through security software such as anti-virus with the latest version.
- Always download software or applications from known trusted sources only. Never use pirated software on your systems/devices.
- Ensure all devices/accounts are protected by a strong PIN or passcode. Never share your PIN or password with anyone.
- Do not share your net-banking password, One Time Password (OTP), ATM or phone banking PIN, CVV number etc. with any person even if he/she claims to be an employee or a representative of the bank and report such instances to your bank.
- Always change the default admin password on your Wi-Fi router to a strong password known only to you. In addition, always configure your wireless network to use the latest encryption (contact your network service provider, in case of any doubt).
- Be cautions while browsing through a public Wi-Fi and avoid logging in to personal & professional accounts such as e-mail or banking on these networks.
- Always use virtual keyboard to access net-banking facility from public computers; and logout from banking portal/website after completion of online transaction. Also ensure to delete browsing history from web browser (Internet Explorer, Chrome, Firefox etc.) after completion of online banking activity.
- Do scan all e-mail attachments for viruses before opening them. Avoid downloading e-mail attachments received in e-mails from unknown or un-trusted sources.
- Be careful while sharing identity proof documents especially if you cannot verify the authenticity of the company/person with whom you are sharing information.
- Note the IMEI code of your cell phone and keep it in a safe place. The operator can blacklist/ block/trace a phone using the IMEI code, in case the cell phone is stolen.
- Observe your surroundings for skimmers or people observing your PIN before using an ATM.
- Discuss safe internet practices and netiquettes with your friends and family regularly! Motivate them to learn more about cybercrimes and safe cyber practices.
- Do not save your card or bank account details in your e-wallet as it increases the risk of theft or fraudulent transactions in case of a security breach.
- If you think you are compromised, inform authorities immediately.

Transaction Analysts (India) Pvt. Ltd.
#4, Sathyam Arcade, 1st Floor, 1st Phase, BTM Layout 2nd Stage, Bangalore - 560076
info@transactionanalysts.com + 91 80 26784479

Specific TIPs for Cyber Security

TIPs for Safe Internet Browsing ·

- Beware of various fraudulent lucrative advertisements regarding discount coupons, cashback and festival coupons offering payments through UPI apps popping up while browsing.
- Some URL links on the internet are advertising to provide fake apps. Do not download such fake apps on your mobile, as these apps may steal your personal or biometric data from your mobile phone
- Avoid using third-party extensions, plug-ins or add-ons for your web browser as it may track your activity and steal your personal details.
- Always browse/visit the original website for purchasing.
- Always type the information in online forms and not use the auto-fill option on web-browser to fill online forms as these forms may store your personal information such as card number, CVV number, bank account number etc.
- Be careful about the name of a website. A malicious website may look identical to a legitimate one, but the name may use variation in spelling or a different domain (e.g.,[dot]com, [dot]net etc.)
- In general, all the government websites have [dot]gov[dot]in or [dot]nic[dot]in ending.
- Avoid clicking 'Keep me logged in' or 'Remember me' options on websites, especially on public computers.
- Beware of fraudulent charity activities or non-existent charitable organizations having names identical to government charity funds, requesting money for victims, products or research. Always check the credentials of charity organizations before donation.
- Never allow the browser to store your username/password, especially if you use a shared computer device. Also make it a habit of clearing history from the browser after each use session to protect your privacy.
- Be cautious with tiny or shortened URLs (it appears like http://tiny.cc/ba1j5y). Don't click on it as it may take you to a malware infected website.
- Prior to registering on a job search portal, check the privacy policy of the website to know the type of information collected from the user and how it will be processed by the website.
- Many social networking sites prompt to download a third-party application that lets you access more pages. Do not download unverified third-party applications without ascertaining its safety.
  · Beware of e-commerce websites and advertisements selling items at highly discounted prices.

TIPs for safe Internet Banking

- Always use virtual keyboard for accessing net banking facility and log off from banking portal/website after completion of online transaction. Also ensure deletion of browsing history from web browser (internet explorer, chrome etc.) after completion of online banking activity.
- Use multiple factor authentications for login into your bank accounts.
- Avoid writing down or storing in mobile phones the information used to access digital wallets/bank accounts.
- One should not use the same password for internet banking of all accounts.
- One should not keep the same mobile number registered for all bank accounts.
- Always enable getting notification of transactions from the banks via both SMS & e-mail.
- Login and view your bank account activity regularly to make sure that there are no unapproved transactions. Report discrepancies, if any, to your bank immediately.
- It is preferable to have two separate e-mail accounts, one for communicating with people and another for your financial transactions

TIPs for E-wallet Security

- Enable password/PIN on your mobile phones, tablets & other devices that you use.
- While doing transactions using your e-wallet, you should never save the details of your debit or credit cards.
- Use multiple factor authentication for logging into your e-wallets.
- Avoid writing down information used to access the digital wallets in mobile phones.
- Install e-wallet accounts from sources you trust. Do not install e-wallet apps via links shared over email, SMS or social media. Always verify and install authentic e-wallet apps directly from the app store (Google/ iOS store) on your smart phone. Please check if the app is having the “Play Protect” shield.

TIPs for E-mail Account Security

- Never keep the same password for all your e-mail accounts.
- Use secure network connections.
- Avoid the use of public Wi-Fi networks. More secure Wi-Fi connections require passwords & are easily identified as “WPA or WPA2”. Highly insecure Wi-Fi is open for anyone to connect to & may be labelled as a “WEP” (Wired Equivalent Privacy).
- Don't click on the links provided in suspicious e-mails even if they look genuine as this may lead you to malicious websites and this may be an attempt to defraud your hard-earned money.

TIPs for Identity Proof’s Security

- Never leave the discarded photo copy of your identity proof at shops.
- Never allow the shopkeeper to keep a copy of your identity proof in their computer.
- Never share your identity proof to unknown persons on social media platforms including WhatsApp.
- Never share your property papers or other personal information on social media platforms.

TIPs for Password Security

- Keep a strong password of at least 8 characters with alphanumeric, special character, upper case & lower-case combination.
- Keep two factor authentication for all your accounts.
- If you suspect that any of your account has been hacked, immediately change the password and contact the nearest Police Station.

-----ooOOoo----