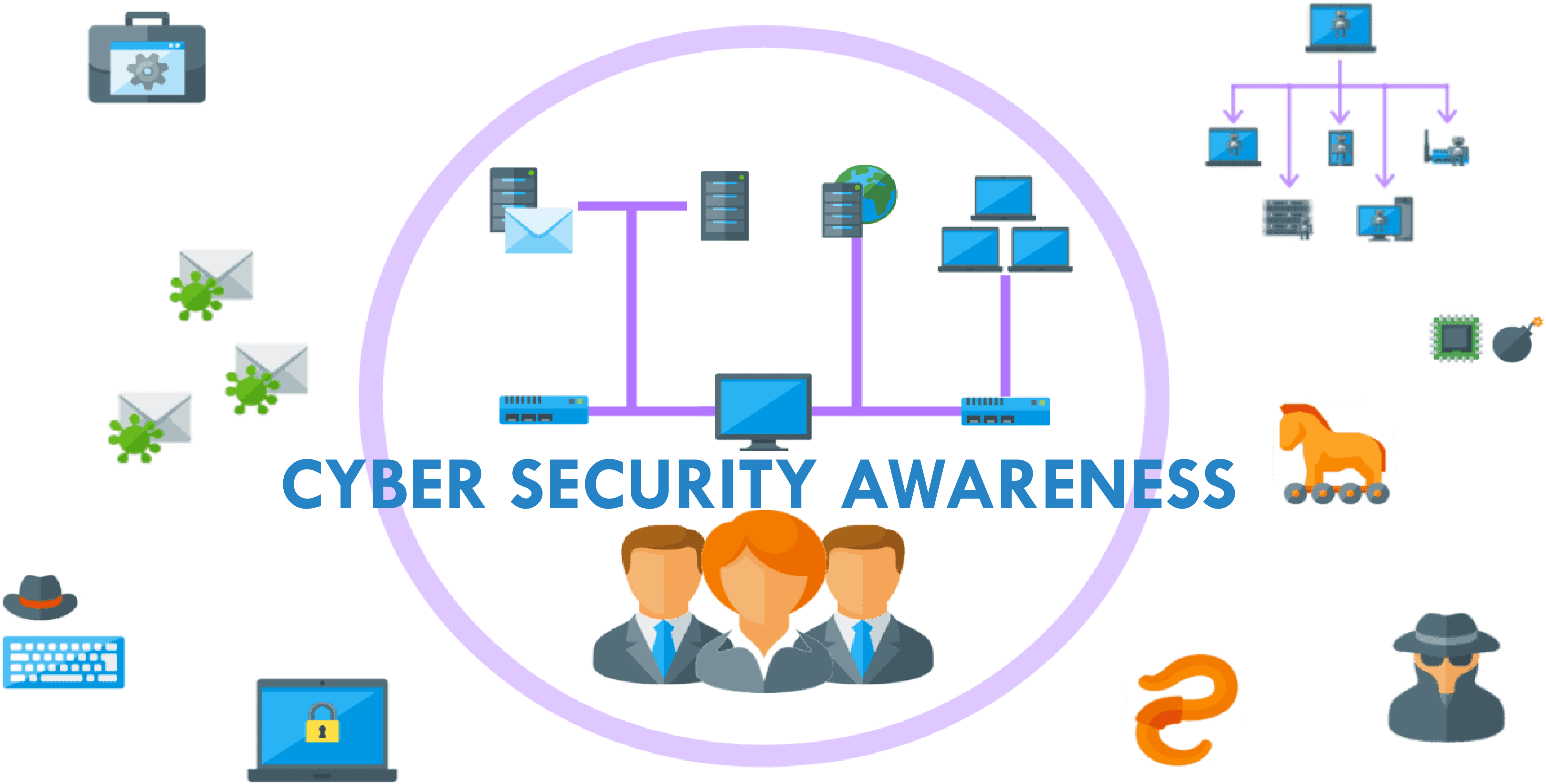
CYBER SECURITY AWARENESS



WHAT IS CYBER SECURITY?

Cybersecurity is the protection of internet-connected systems such as hardware, software and data from cyberthreats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems.

A strong cybersecurity strategy can provide a good security posture against malicious attacks designed to access, alter, delete, destroy or extort an organization's or user's systems and sensitive data. Cybersecurity is also instrumental in preventing attacks that aim to disable or disrupt a system's or device's operations.

IMPORTANCE OF CYBER SECURITY

With an increasing number of users, devices and programs in the modern enterprise, combined with the increased deluge of data -- much of which is sensitive or confidential -- the importance of cybersecurity continues to grow. The growing volume and sophistication of cyber attackers and attack techniques compound the problem even further.

CYBER SECURITY INCIDENTS

FEB. 2021

4.5 Million personal data of Air India passenger was exposed.

APRIL 2021

Upstox, the second largest stock broker in India, has suffered a massive data breach.

This breach has exposed user data like Aadhaar, PAN, bank account numbers and more**.**

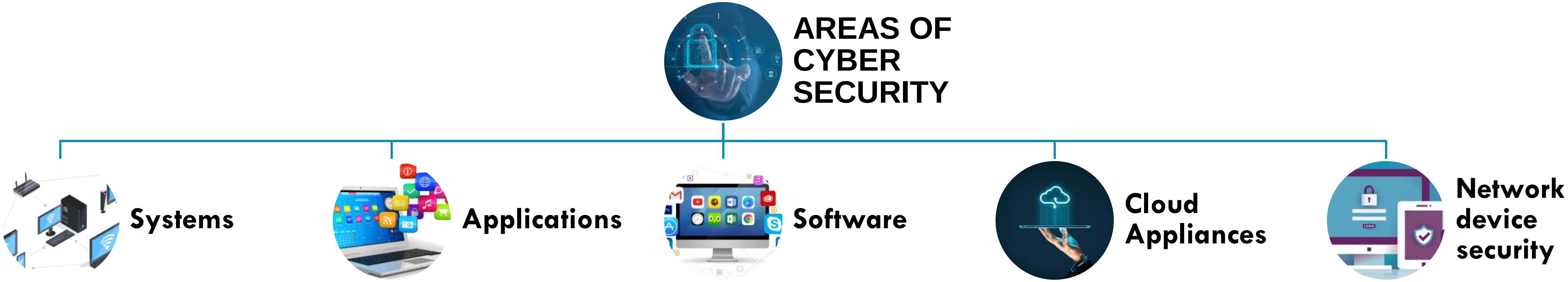
JULY 2022

SEBI faced cyber security incident involving its email systems.

TYPES OF CYBER THREATS

The threats countered by cyber-security are three-fold:

- **Cybercrime** includes single actors or groups targeting systems for financial gain or to cause disruption.
- **Cyber-attack** often involves politically motivated information gathering.
- **Cyberterrorism** is intended to undermine electronic systems to cause panic or fear.



AREAS OF CYBER SECURITY

Systems

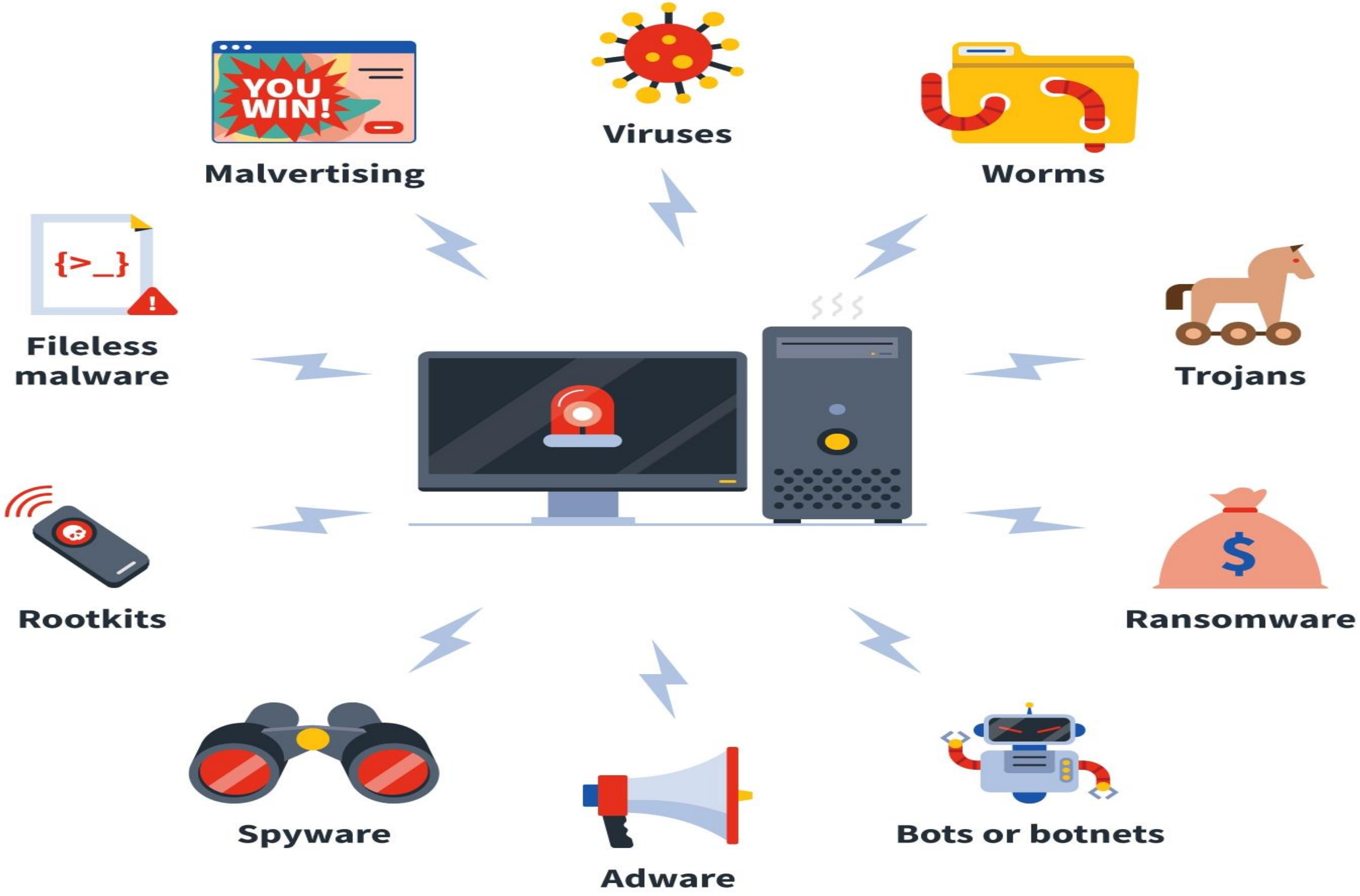
Applications

Software

Cloud Appliances

Network device security

TYPES OF CYBER SECURITY THREATS



BENEFITS OF CYBER SECURITY

- Protection against cyber attacks and data breaches.
- Protection for data and networks.
- Prevention of unauthorized user access.
- Improved recovery time after a breach.
- Protection for end users and endpoint devices.
- Regulatory compliance
- Business continuity

INFORMATION - CIA

- **Confidentiality** **–** restrict access to authorized individuals
- **Integrity** **–** data has not been altered in an unauthorized manner
- **Availability** **–** information can be accessed and modified by authorized individuals in an appropriate timeframe.

CONSEQUENCES OF DATA/INFORMATION LOSS

- Loss of Business
- Public Embarrassment
- Loss of Customer
- Loss of Employee Trust
- Penalties & Prosecution

MOBILE APPLICATION SECURITY

Mobile security refers to the techniques used to secure data on mobile devices such as smartphones and tablets and is another aspect of internet protection.

TIPS FOR KEEPING YOUR MOBILE PHONE SAFE AND SECURE

- Stay on native app store and stay away from third party app stores
- Never download apps without verifying their safety first
- Always update to the latest OS version as soon as possible
- Consider replacing your phone once it is unsupported by the OS
- Do not disable or bypass data protections from your employers
- Enable password protection on your OS, apps, and services when possible
- Turn on multifactor authentication
- When in doubt, always choose security over convenience

EMAIL SECURITY

Email security refers to the methods used to protect email accounts and correspondence against unauthorized access, loss, or compromise. Given that email is often used to spread malware, spam, and phishing attacks, email security is an important aspect of internet security.

HOW TO DEAL WITH EMAIL SPAM

- Mark spam emails as spam
- Never click on a link or open an attachment in a spam email.
- Be careful about where you disclose your email address
- Most email providers will offer privacy settings – review these and make sure they are set to a level you feel comfortable with.
- Look into third-party email spam filters.

FINANCIAL TRANSACTION SECURITY

It is critical to have good safeguards and practices for our financial transactions, as losses arising from financial fraud can considerably impact us. Rising cybercrime incidents, phishing attacks, and ATM hacks have made it even more critical.

TIPS FOR SECURE FINANCIAL TRANSACTIONS:

- Create strong passwords for online financial transactions
- Update software regularly for online financial transactions
- Buy from secure websites for online financial transactions
- Set a limit for your banking cards
- Don’t save payment information for online financial transactions.
- Use virtual keyboards
- Opt for SMS and email alerts
- Use OTP (One time passwords) for logging in

SOCIAL MEDIA & SOCIAL ENGINEERING

Social engineering is the art of manipulating people so they will part ways with their confidential information - with anything from passwords to banking details in their line of scope.

SOCIAL MEDIA SECURITY TIPS:

- Evaluate before posting anything on social media.
- Avoid sharing location while posting on social media.
- Don’t click on links, files, games or applications within the confines of social media
- Use multifactor authentication.
- Customize your privacy settings to be as restrictive as possible regarding who can read and see posts.

INTERNET SERVICES SECURITY

Internet security is a term that describes security for activities and transactions made over the internet. It’s a particular component of the larger ideas of cybersecurity and computer security, involving topics including browser security, online behavior and network security.

HOW TO PROTECT YOUR DATA ONLINE:

- Use firewall
- Choose your browser carefully
- Create strong password, and use a secure password manager
- Keep an up-to-date security program installed on your devices

REPORTING CYBERCRIME

According to the IT Act, a cybercrime comes under the purview of global jurisdiction which means that a cybercrime complaint can be registered with any of the cyber cells in India, irrespective of the place where it was originally committed or the place where the victim is currently residing/ staying.

cybercrime.gov.in

call on 1930

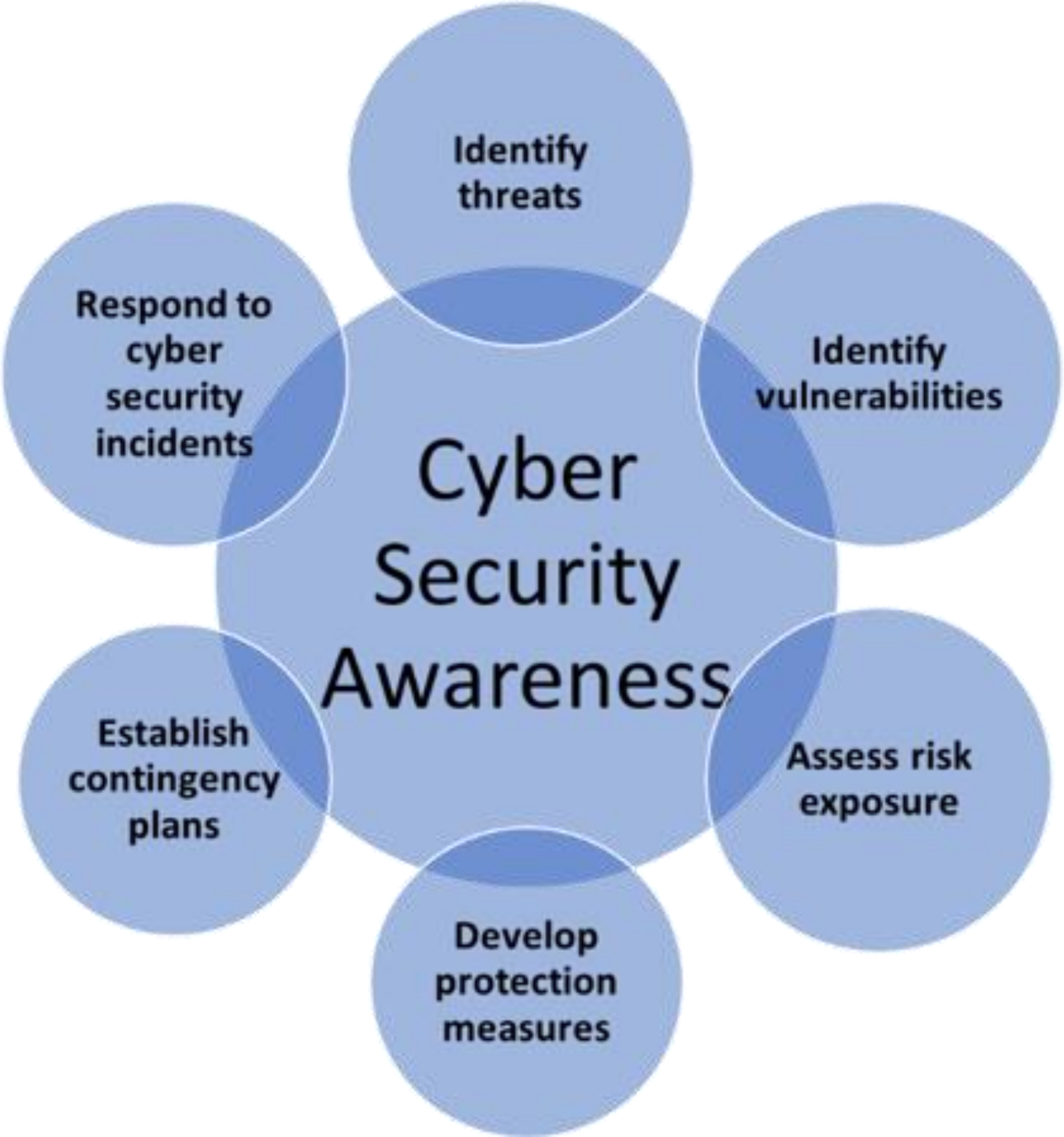
Report cybercrime complaints at
National Cyber Crime Reporting portal
(https://cybercrime.gov.in) of MHA

DATA SECURITY & PRIVACY

Data security is focused on protecting personal data from any unauthorized third-party access or malicious attacks and exploitation of data. It is set up to protect personal data using different methods and techniques to ensure data privacy.

Data privacy or Information privacy is concerned with proper handling, processing, storage and usage of personal information.

Data privacy is about proper usage, collection, retention, deletion, and storage of data. Data security is policies, methods, and means to secure personal data.



Cyber Security Awareness

Identify threats

Identify vulnerabilities

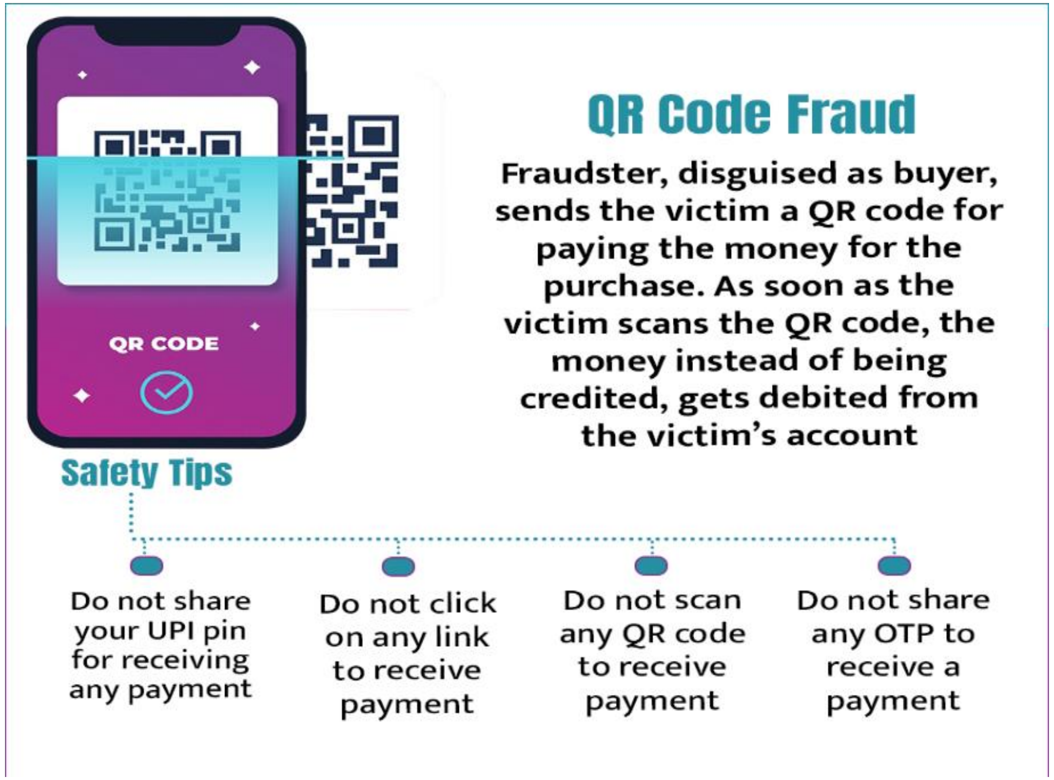
Assess risk exposure

Develop protection measures

Establish contingency plans

Respond to cyber security incidents

INTERNET SAFETY TIPS

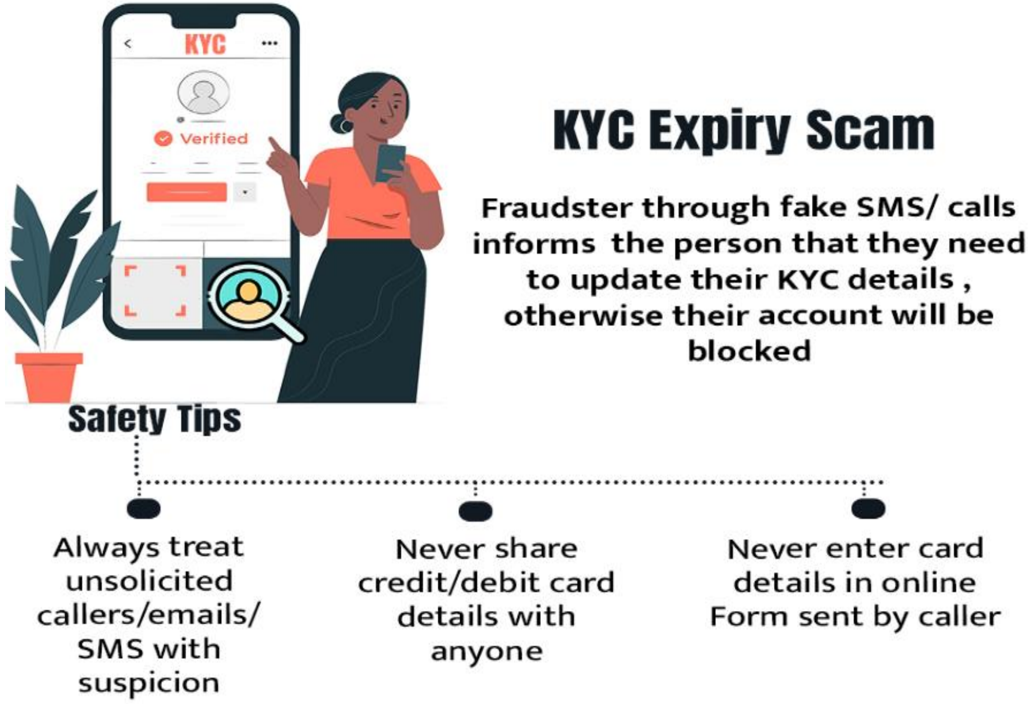


QR Code Fraud

Fraudster, disguised as buyer, sends the victim a QR code for paying the money for the purchase. As soon as the victim scans the QR code, the money instead of being credited, gets debited from the victim's account

Safety Tips

- Do not share your UPI pin for receiving any payment
- Do not click on any link to receive payment
- Do not scan any QR code to receive payment
- Do not share any OTP to receive a payment



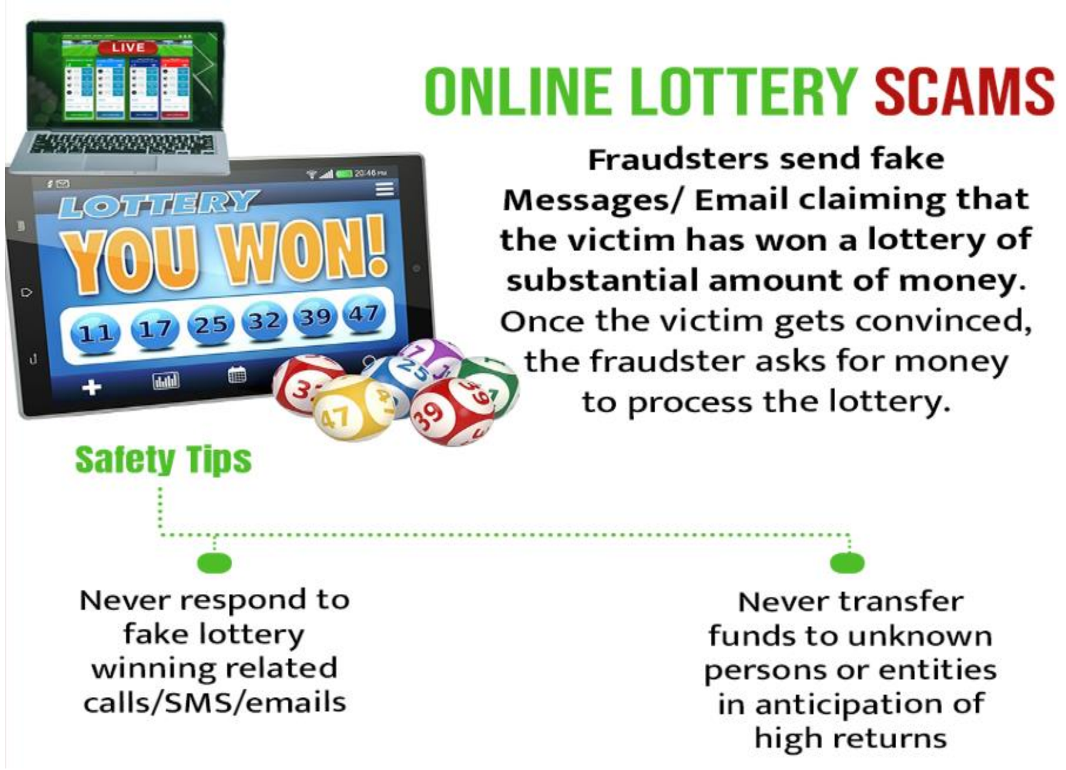
KYC Expiry Scam

Fraudster through fake SMS/ calls informs the person that they need to update their KYC details , otherwise their account will be blocked

Safety Tips

- Always treat unsolicited callers/emails/ SMS with suspicion
- Never share credit/debit card details with anyone
- Never enter card details in online Form sent by caller

INTERNET SAFETY TIPS

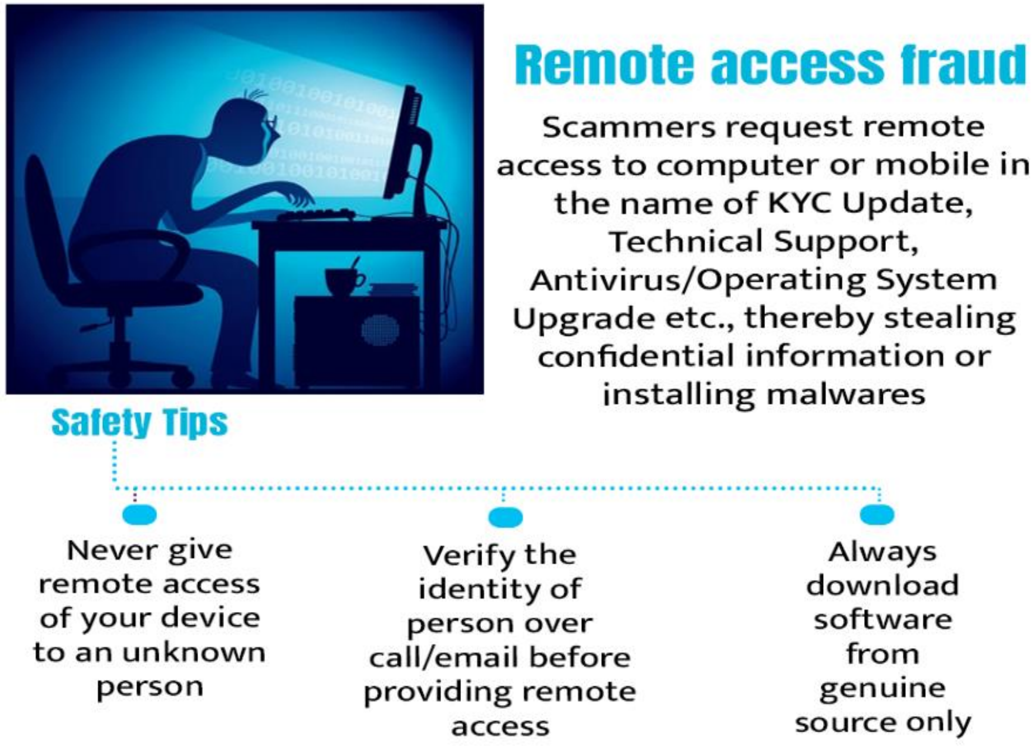


ONLINE LOTTERY SCAMS

Fraudsters send fake Messages/ Email claiming that the victim has won a lottery of substantial amount of money. Once the victim gets convinced, the fraudster asks for money to process the lottery.

Safety Tips

- Never respond to fake lottery winning related calls/SMS/emails
- Never transfer funds to unknown persons or entities in anticipation of high returns



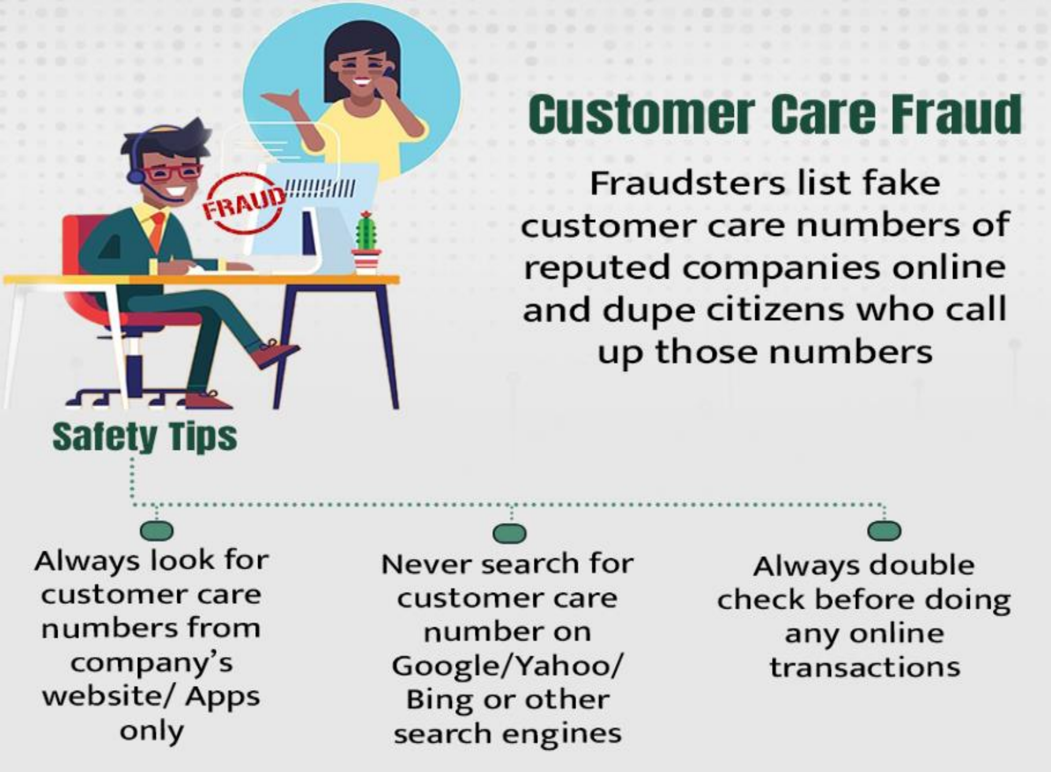
Remote access fraud

Scammers request remote access to computer or mobile in the name of KYC Update, Technical Support, Antivirus/Operating System Upgrade etc., thereby stealing confidential information or installing malwares

Safety Tips

- Never give remote access of your device to an unknown person
- Verify the identity of person over call/email before providing remote access
- Always download software from genuine source only

INTERNET SAFETY TIPS

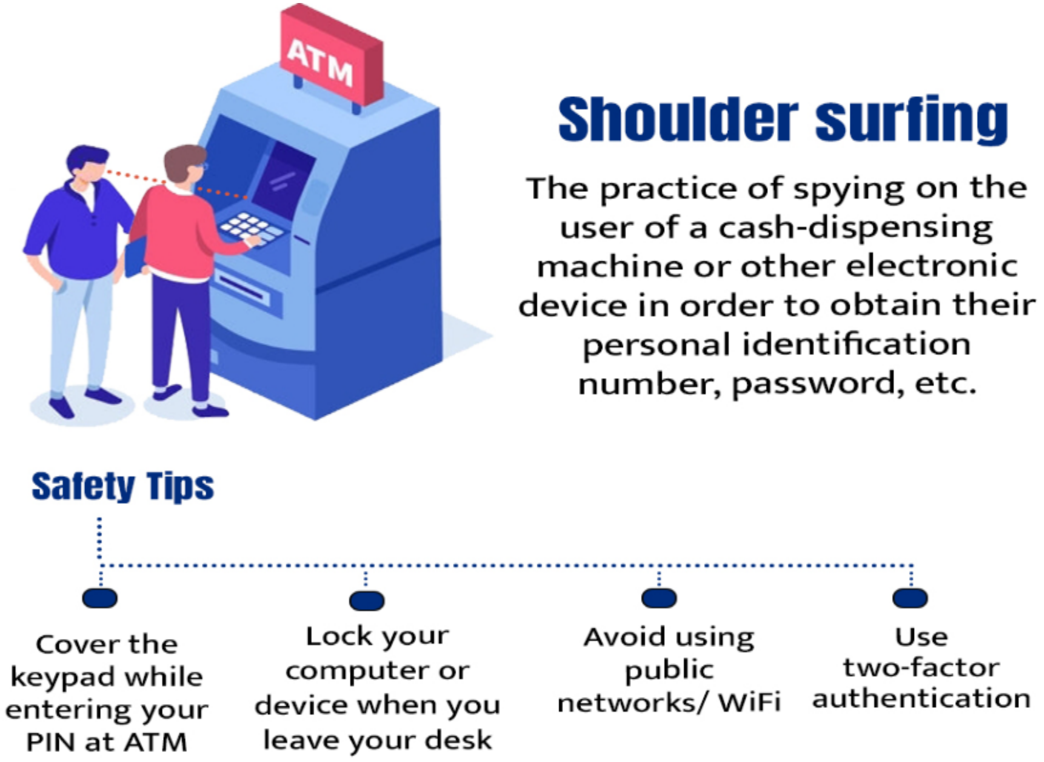


Customer Care Fraud

Fraudsters list fake customer care numbers of reputed companies online and dupe citizens who call up those numbers

Safety Tips

- Always look for customer care numbers from company's website/ Apps only
- Never search for customer care number on Google/Yahoo/ Bing or other search engines
- Always double check before doing any online transactions



Shoulder surfing

The practice of spying on the user of a cash-dispensing machine or other electronic device in order to obtain their personal identification number, password, etc.

Safety Tips

- Cover the keypad while entering your PIN at ATM
- Lock your computer or device when you leave your desk
- Avoid using public networks/ WiFi
- Use two-factor authentication

STAY CYBER SAFE

THANK YOU