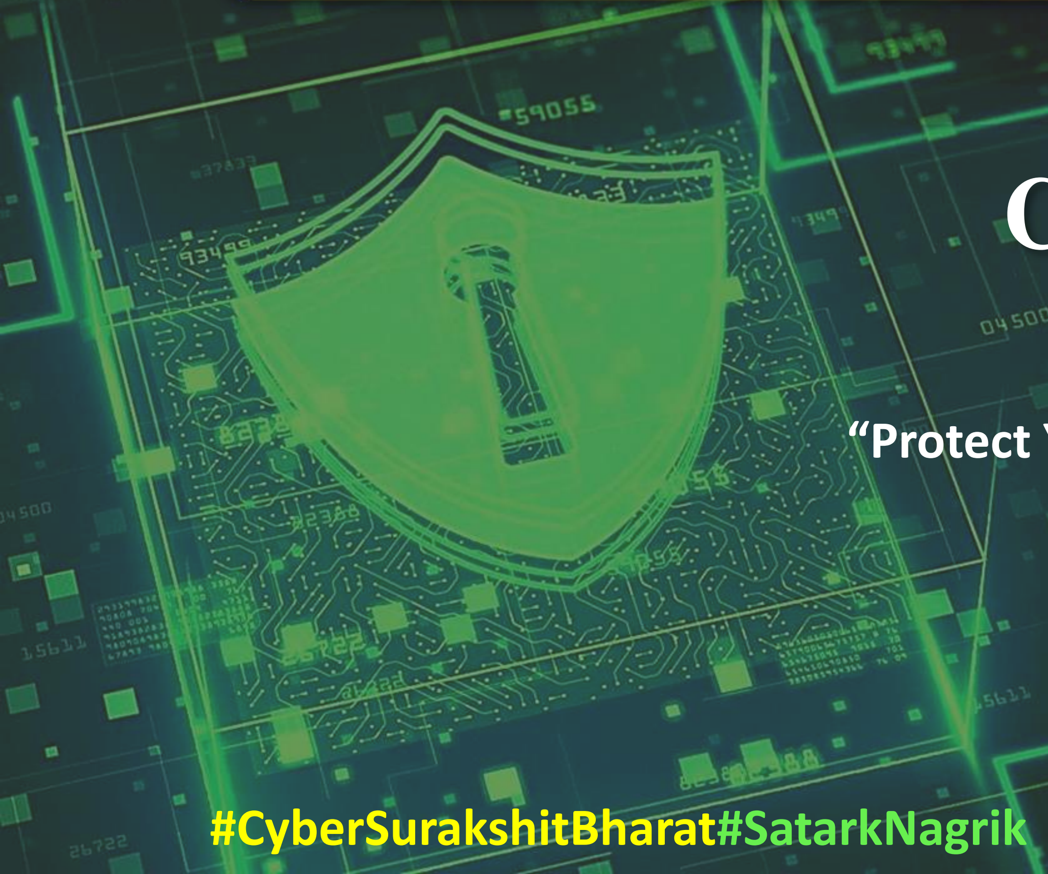
੧ਓ ਸ੍ਰੀ ਵਾਹਿਗੁਰੂ ਜੀ ਕੀ ਫ਼ਤਹਿ

पंजाब एण्ड सिंध बैंक
(भारत सरकार का उपक्रम)

Punjab & Sind Bank
(A Govt. of India Undertaking)

Where service is a way of life



Cyber Security Digest

"Protect Your Digital Life: Stay Smart, Stay Safe"

#CyberSurakshitBharat#SatarkNagrik

Prepared By-
HO CISO Cell

Dear Colleagues,

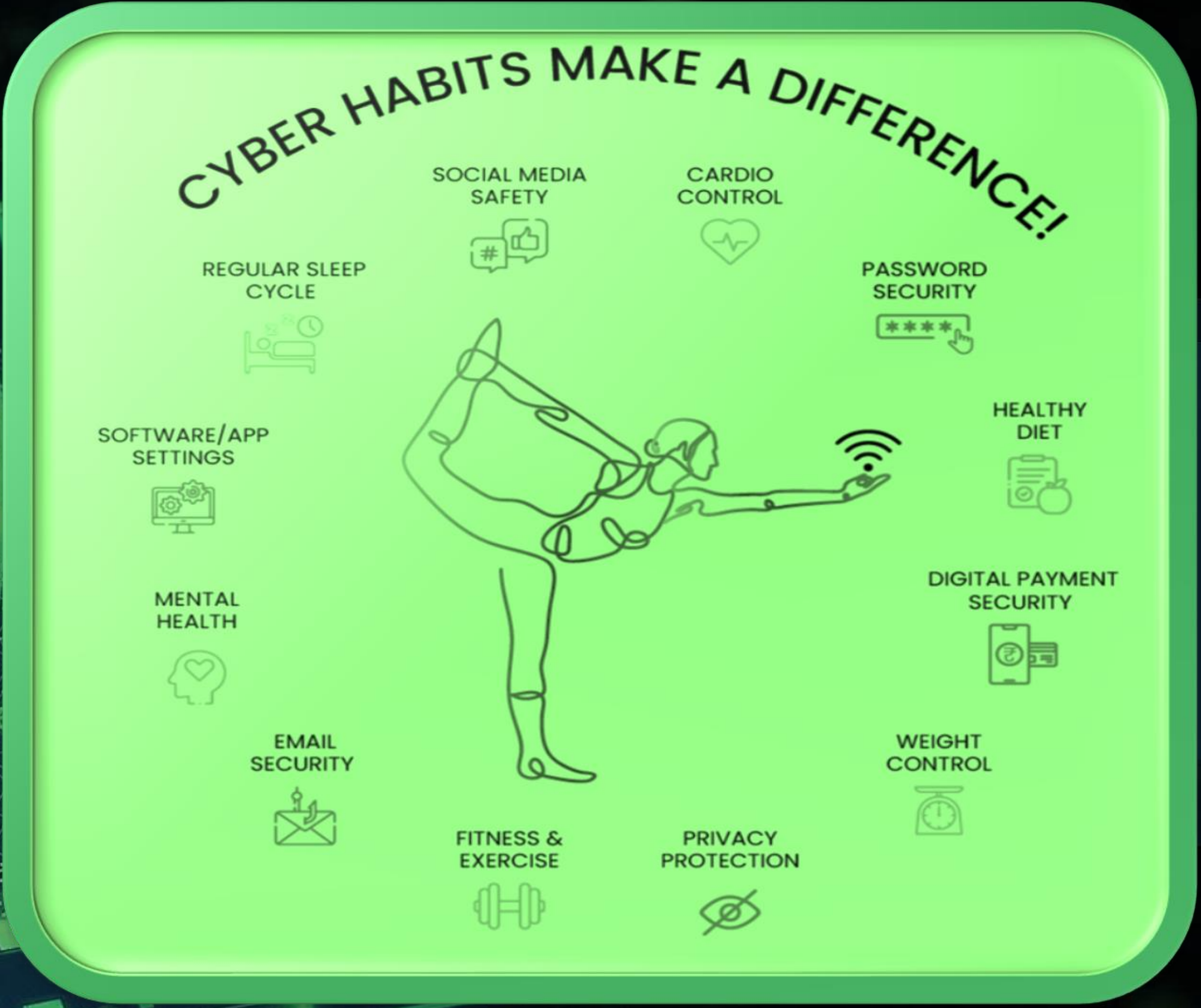
I would like to commend the efforts of our CISO Cell for their proactive initiative in creating the Cyber Security Digest. In today's rapidly evolving digital landscape, the importance of cybersecurity cannot be overstated. This booklet is an important resource that aims to educate and empower all of us in protecting the Bank's critical information and systems.

The Cyber Security Digest offers valuable knowledge on various types of cyber attacks, the importance of cyber hygiene, and practical cybersecurity practices. I encourage every staff member to not only read this document but to integrate the practices outlined into your daily operations. By doing so, you will play a vital role in strengthening our defense against potential cyber threats.

Let us all make optimum use of this resource and remain vigilant in our shared responsibility to safeguard the Bank's digital assets. Together, we can ensure a safer and more secure environment for our institution and our customers.

Best regards,

Rajeeva
Executive Director
Punjab & Sind Bank



CYBER HABITS MAKE A DIFFERENCE!

SOCIAL MEDIA SAFETY

CARDIO CONTROL

REGULAR SLEEP CYCLE

PASSWORD SECURITY

SOFTWARE/APP SETTINGS

HEALTHY DIET

MENTAL HEALTH

DIGITAL PAYMENT SECURITY

EMAIL SECURITY

WEIGHT CONTROL

FITNESS & EXERCISE

PRIVACY PROTECTION

#CyberSurakshitBharat#SatarkNagrik

IMPORTANCE OF CYBER SECURITY

- The internet allows an attacker to work from anywhere on the planet.

- Cyber Security is the safeguarding of computer systems and networks against data leakage, theft, or damage to their hardware, software, or electronic data, as well as disruption or misdirection of services.

- New and powerful cyber-attacks are striking the internet regularly. A minor lapse in managing our digital lives can open the door to cyber criminals. Cyber criminals can steal our money or damage our reputation.

- According to a study by a leading industry research organization, 90% of all cyberattacks are caused by human negligence. Therefore, cyber security awareness is important for everyone today.

#CyberSurakshitBharat#SatarkNagrik

Common Causes of Cyber attacks

- Use of Weak or stolen usernames and passwords
- Software Application vulnerabilities
- Absence of Antivirus and latest patches
- Use of Pirated Operating Systems
- System and Network Firewalls disabled
- Social engineering (tricking people into breaking security protocols)
- Poor access control (Unauthorized users have access)
- Insider threats (System Password has not set)
- Improper configuration of WIFI devices and Hotspots
- Unnecessary Ports opened on Network for Backdoor Entry

#CyberSurakshitBharat#SatarkNagrik

RANSOMWARE

Ransomware is a type of malware that restricts users from accessing the system and demands to pay ransom in order to regain access.

How Ransomware Infection Occurs ?

- Visiting Suspicious Websites / Opening Phishing Emails
- System Infected / Files Encrypted and Demand of Ransom

What To Do If Infected ?

- Disconnect the System from Internet
- Report the Incident To Concerned Authority
- Restore Data From Backup To Clean Device

- Keep Antivirus and Windows Updated
- Do not Open Suspicious Emails
- Do Not Click Suspicious Links on Websites
- Backup Data Regularly
- Enable Firewall Protection

#CyberSurakshitBharat

#SatarkNagrik

Keep Yourself Protected From Ransomware !!

VISHING/SOCIAL ENGINEERING

Cybercriminals use various tech tactics to trick users into revealing sensitive info, like vishing, pretexting, smishing, and impersonating support staff.

Modus Operandi

- Fraudsters investigate the background of their intended targets and launch campaigned attacks.
- Mostly happens on call asking you to click on links, donate money, update account details, etc.
- They psychologically manipulate the victim taking advantage of their natural reactions.

How To Stay Safe

- The golden rule is to avoid inbound customer service/technical service calls or email support requests.
- Never entertain calls from people posing as bank representatives. Banks never call and ask for CVV/PIN/OTP.
- In case a remote co-worker calls and asks for account credentials or official information, keep the IT Security team in loop and do as instructed.

#CyberSurakshitBharat

#SatarkNagrik

पी.एस.बी

SOCIAL MEDIA FRAUD

Cybercriminals exploit social media to trick users into sharing personal information or sending money by pretending to be a friend.

Modus Operandi

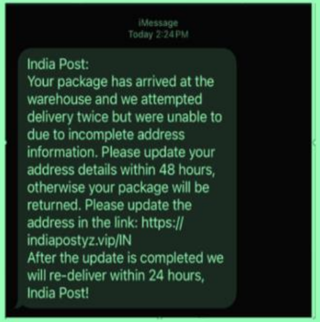
- Fraudsters populate/spread fake customer care numbers of banks and UPI platforms on social media platforms.
- Fake bank websites with similar design and fake UPI apps are uploaded.
- Users call on these numbers, fraudsters pose as official representatives.
- The fraudster extracts sensitive information and deducts money from the user's account.

How To Stay Safe

- Do not search for your app or bank's customer care numbers on search engines or social media.
- Always visit the official website, check URLs and contact genuine numbers.
- Do not share personal information containing location, frequently visited places, financial purchases, etc.

#CyberSurakshitBharat
#SatarkNagrik

Courier Scam


iMessage
Today 2:24 PM

India Post:
Your package has arrived at the warehouse and we attempted delivery twice but were unable to due to incomplete address information. Please update your address details within 48 hours, otherwise your package will be returned. Please update the address in the link: https://indiapostyz.vip/IN
After the update is completed we will re-deliver within 24 hours,
India Post!

Modus Operandi

- Scammers send fraudulent emails, SMS, or calls claiming a parcel needs payment or information for delivery.
- The message includes a link to a fake website that mimics a legitimate courier service, asking for personal or payment details.
- The scam often involves pressure, such as “urgent payment required” or “delivery will be canceled”.
- Victims are tricked into entering payment information or personal details, leading to financial theft or identity fraud.

How To Stay Safe

- Always confirm courier notifications through official channels or apps.
- Don’t click links in unsolicited messages. Inspect email addresses and phone numbers for unusual formats.
- Be cautious of messages with spelling errors.
- Only track parcels through the courier’s official website or app.

#CyberSurakshitBharat
#SatarkNagrik

Digital Arrest Scam

This scam involves fraudsters impersonate Law Enforcement officials and falsely claim to investigate crimes, using digital tools and fake setups to intimidate victims into transferring money to avoid fabricated legal troubles.

Modus Operandi

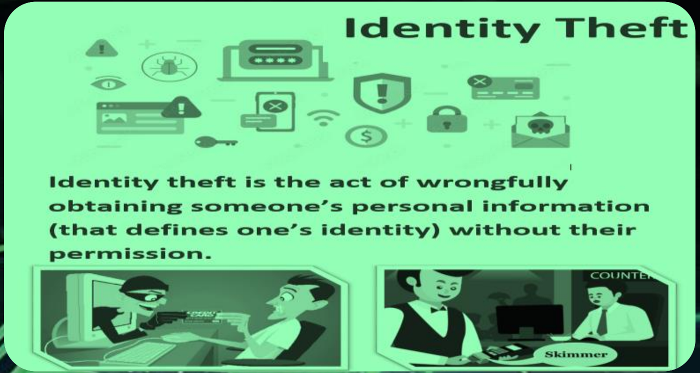
- Fraudsters impersonate law enforcement, claiming you are under investigation or have committed a crime.
- They demand payment(usually via wire transfer or cryptocurrency) to avoid arrest or legal trouble.
- These scams often involve threats, false urgency, and fake legal documents

How To Stay Safe

- Law enforcement will never demand money over the phone to avoid arrest.
- Verify any claims by contacting local authorities directly.
- Avoid making payments to unknown accounts or individuals under pressure

#CyberSurakshitBharat

#SatarkNagrik



Identity Theft

Identity theft is the act of wrongfully obtaining someone's personal information (that defines one's identity) without their permission.

Modus Operandi

- Cybercriminals steal personal information(e.g., name, email, mobile number, bank account details) to impersonate you.
- They can open new credit accounts, withdraw money, or apply for loans in your name.
- They assume your identity on social media.
- Identity theft can occur through data breaches, phishing or stealing physical documents.

How To Stay Safe

- Regularly monitor your financial accounts and credit reports.
- Use strong, unique passwords for online accounts.
- Avoid sharing personal information over unsecured communication channels

#CyberSurakshitBharat

#SatarkNagrik

DEEPFAKE SCAM

Modus Operandi

- The fraudster gathers sufficient data about the target individual, such as images, videos, social media posts, or audio recordings to create a realistic digital replica.
- The fraudster utilizes AI algorithms, particularly deep learning techniques, to train models that can generate highly convincing deepfake content using the victim’s data collected by fraudster.
- Fraudsters impersonate trusted figures through fake videos or audio mimicking to deceive.

How To Stay Safe

- Always cross-check video or audio requests through direct communication.
- Be Skeptical, don’t immediately trust content that looks or sound real deepfake can be deceptive.
- Only believe information from the trusted news outlets and official channels.
- Enable two factor authentication(2FA) on social media to prevent unauthorized access.

#CyberSurakshitBharat
#SatarkNagrik

SIM CLONING

Modus Operandi

- Fraudsters clone your SIM card, often through phishing or social engineering, to gain control of your phone number.
- The fraudster will then send an SMS to the victim with a request to restart the mobile on some pretext. Once the victim switches off his mobile, the fraudster starts the phone with a duplicate SIM in his control, before the victim restarts his mobile. This act will successfully initiate/activate the mobile with cloned SIM card.
- Once the cloned SIM is successfully initiated the attacker will take over the victim's mobile number, SIM, and his account.

How To Stay Safe

- Avoid sharing sensitive personal information, such as your mobile number, on public platforms or with unknown individuals.
- Keep your SIM card in a secure location and avoid sharing it with others. Report any lost or stolen SIM cards to your service provider immediately.
- Enable Personal Identification Number (PIN) and Personal Unblocking Key (PUK) code on your SIM card to add an extra layer of protection.
- Implement 2FA using methods other than SMS-based verification, such as email authentication app-based authenticators, or hardware tokens.

#CyberSurakshitBharat
#SatarkNagrik

TAILGATING

Modus Operandi

- Sneaking into line along with valid card holder.
- The user enters with a valid ID card and seeks access/entry at Software-based electronic gates .
- The gate opens to provide access to the valid ID card holder. Meanwhile the fraudster grabs the opportunity to gain an unauthorized entry by sneeking in at the same time.
- The fraudster may also steal the ID card if an authorized employee to gain access or entry into the restricted space

How To Stay Safe

- Management to install biometric scanners and turnstiles to prevent a tailgater from just walking in the building.
- Biometric scanners and electric access gates prevent the tailgater from walking with user inside the building.
- When an unidentified person is noticed inside an office, check if he has a visitor badge.

#CyberSurakshitBharat
#SatarkNagrik

QR CODE PAYMENTS

Modus Operandi

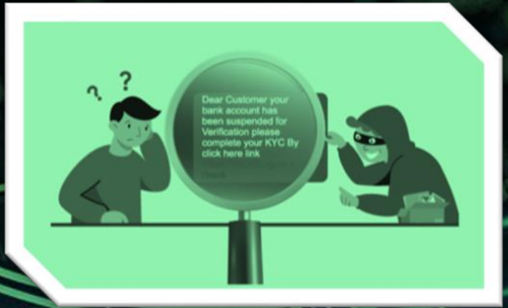
- Merchants create unique QR codes linked to their payment systems.
- Codes are shown at the point of sale or sent digitally.
- Customers scan the code with their smartphone payment app.
- Customers confirm the amount and authorize the payment.
- Transaction is processed and both parties receive confirmation.

How To Stay Safe

- Only scan codes from reputable payment apps.
- Confirm QR codes are from legitimate business.
- Use secure networks for transactions.
- Check for signs of tampering.

#CyberSurakshitBharat
#SatarkNagrik

KYC FRAUDS


Dear Customer your bank account has been suspended for Verification please complete your KYC By click here link

Modus Operandi

- Fraudsters make a fake call to the victim pretending to be representative from a bank requesting them to update the KYC immediately and warning them of account block/suspension.
- The caller says that the validation/KYC can be done online to keep the account active, and asks the customer to download an APP on the digital device being used.
- Once the app is downloaded, the fraudsters will ask you to share code and grant certain permissions, which will enable them to gain access to your digital device.
- The fraudster makes use of these details to gain unauthorized access to the victim's bank account to commit fraud.

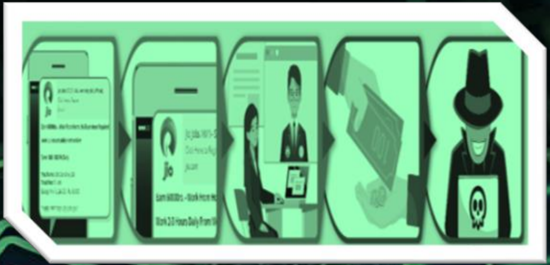
How To Stay Safe

- Never click on unknown links or links received from unverified sources.
- Always remember that a banks other authorized institutions, never does KYC on calls or send any links to its customers, for updating KYC.
- Never share your mobile number, account number, password, OTP, PIN or any other confidential details with anyone. Bank never asks its customers to share any confidential information.
- Do not give your access to your device for anyone by installing remote access type of applications (AnyDesk , Quicksupport ,Team Viewer etc.)

#CyberSurakshitBharat
#SatarkNagrik

EMPLOYMENT SCAMS

Modus Operandi



- The user receives messages/emails/calls regarding attractive Job Listings created by Scammers claiming to offer high-paying positions, flexible work hours, and promising benefits to attract job seekers.
- The scammers impersonate legitimate companies, using familiar names, logos to appear authentic and gain the trust of potential victims.
- Once any users contact them the scammers may proceed to conduct fake interviews over phone calls, or messaging apps.
- The scammers request upfront payments or fees for various reasons which are often non-refundable. Once they make the payment the fraudster either stops responding or on some pretext or other evades their calls/messages/emails or may disappear totally.

How To Stay Safe

- Before applying for a job or providing any personal information, thoroughly research the company or employer.
- Stick to reputable and well-known job portals when searching for job opportunities.
- Be cautious when sharing personal information. Legitimate employers typically don't ask for sensitive details.
- When communicating with potential employers, use secure channels

#CyberSurakshitBharat

#SatarkNagrik

पी.एस.बी

CYBER SECURITY

DO’s & DONT’s

#CyberSurakshitBharat #SatarkNagrik

PASSWORD SECURITY TIPS

- Always use different passwords for different accounts. Ensure password is strong.
- Strong passwords should contain combination of upper case, lower case, numbers, "Special" characters (e.g., @#$%^&*()_+|~--=\'{}[]: ";<>/,etc.)
- Immediately, change any password which might have been shared or revealed by mistake.
- Do not use Birth dates, names, ID proofs and other personal information such as addresses and phone numbers while setting passwords .

#CyberSurakshitBharat#SatarkNagrik

INTERNET SAFETY PRECAUTIONS

- While opening any website look for secured connection by checking if the website starts with "HTTPS" or not.

- Be vigilant while clicking/ downloading from suspicious links/ URLs

- Make it a habit of clearing browser history after confidential activities/ transactions.

- Verify the Authenticity and Identity of social media profiles before getting involved in any correspondence.

- Do not use any public computer or Wi-Fi for carrying out financial transactions like online shopping, internet banking, UPI transaction, etc.

#CyberSurakshitBharat#SatarkNagrik

UPI AND ATM TRANSACTIONS PRECAUTIONS

- Do not share confidential information with any one like:-Card Number, Expiry & CVV number etc
- Remember ,UPI PIN is not needed while receiving payments.
- Verify the name of “Payee” or QR code before proceeding with the payment

- Manage your card limit using mobile banking apps for additional safety
- Do not use Public WiFi/Network while doing any transaction / payment.

#CyberSurakshitBharat#SatarkNagrik

MOBILE SAFETY PRECAUTIONS

- Before downloading any App, same should be checked for its reputation/ authenticity.
- Protect your device with a strong PIN/Password or Biometrics and enable auto lock setting in mobile phone.
- Do not reply or click on link sent through SMS, e-mails or chat messenger by strangers.

- Review the default privacy settings of the smartphone, mobile applications and social media accounts . Personal photos posted on social media with public visibility may be misused
- Do not store any classified/ sensitive data (text /video /photograph) in the mobile device.

#CyberSurakshitBharat#SatarkNagrik

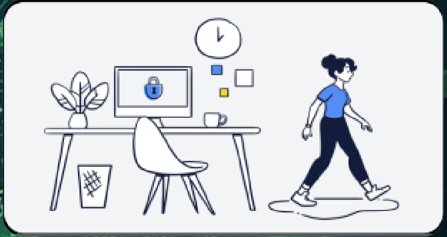
PHISHING EMAILS

- Check for improper spelling or grammar in email content.
- Check for email content that creates urgency of entering data or clicking on link to do payment or update KYC details etc.
- Check for suspicious attachments in email.
- Hover mouse over links mentioned in suspicious email to know the correct address of the URLs
- Avoid sharing financial or Personal information over emails that are not from known sender

#CyberSurakshitBharat#SatarkNagrik

CLEAR DESK & CLEAR SCREEN POLICY

- Computer/ workstations must be locked when workspace is unoccupied.
- Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
- Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.



- Computer/ workstations must be shut down at the end of the work day.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

#CyberSurakshitBharat#SatarkNagrik