

# 31 DAYS OF CYBERSECURITY TIPS

**OCTOBER 2025**  
**#WEEK1**

Wednesday



**Know Your Assets**

Make sure you have an up-to-date list of all your hardware, software, and important apps so that no system is left unprotected.

Day 1

Thursday



**Set Secure Defaults**

Make sure that servers, databases, and devices are set up securely from the scratch and turn off services or ports that aren't needed.

Day 2

Friday



**Patch Quickly**

Install vendor patches and updates on time to fix known security weakness before hackers can use them.

Day 3

Saturday



**Follow Alerts/Advisories**

To stay safe from the recent cyber threats, check CERT-In/NABARD Alerts and advisories on a regular basis and act basis the same.

Day 4

Sunday



**Check for Weaknesses**

Regularly conduct IS audits, cyber security audits, vulnerability scans, and penetration tests to find and fix security weakness.

Day 5

Join the 31-Day Cybersecurity Challenge — each day brings a new activity designed to boost the cybersecurity skills of SEs.



**NATIONAL CYBERCRIME HELPLINE NUMBER 1930**

# 31 DAYS OF CYBERSECURITY TIPS

**OCTOBER 2025**  
**#WEEK2**

Monday



**Protect Perimeter**

Use firewalls, an intrusion prevention system, and Web Application Firewalls to protect digital payment channels.

Day 6

Tuesday



**Secure Email**

Use SPF, DKIM, and DMARC to stop phishing and fake emails from getting through.

Day 7

Wednesday



**Separate Networks**

Keep payment systems, CBS, and online banking servers separate from office endpoint networks.

Day 8

Thursday



**No Shared Accounts**

Make sure that each user has their own login ID so that they are responsible and can't misuse it.

Day 9

Friday

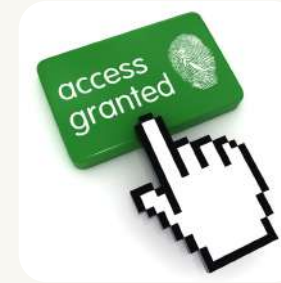


**Use Strong Authentication**

Make sure that CBS, admin users, and people who access the system from outside the office all use multi-factor authentication (MFA).

Day 10

Saturday



**Review Access Regularly**

Perform regular reviews of user access and quickly disable access for staff who have left.

Day 11

Sunday



**Enforce Separation of Duties**

No one person should be able to do critical banking tasks without supervision.

Day 12

**NATIONAL CYBERCRIME HELPLINE NUMBER 1930**

# 31 DAYS OF CYBERSECURITY TIPS

**OCTOBER 2025**  
**#WEEK3**

Monday



**Secure Endpoints**

To protect laptops, ATMs, and desktops, install anti-malware and turn off USB ports.

Day 13

Tuesday



**Disable Unauthorised Software**

Allow only licensed and approved software.

Day 14

Wednesday



**Safe Backups**

Make regular backups that are encrypted and keep them offline or offsite for safety.

Day 15

Thursday



**Test Recovery**

Regularly check that your backups and disaster recovery plans work so that your business can keep going.

Day 16

Friday



**Have an Incident Plan**

Prepare plan and document how to respond to cyber-attacks quickly.

Day 17

Saturday



**Report Breaches in 6 Hours**

As per CERT-In direction it is advised to report cybersecurity incidents within six hours.

Day 18

Sunday



**Third Parties Security**

Vendors that handle banking data must meet the same security standards as the bank.

Day 19

**NATIONAL CYBERCRIME HELPLINE NUMBER 1930**

# 31 DAYS OF CYBERSECURITY TIPS

**OCTOBER 2025**  
**#WEEK4**

Monday



**Contractual Security**

Make sure that contracts for outsourcing include incident reporting, audits, and data protection.

Day 20

Tuesday



**Vendor Auditing**

Check the cybersecurity of your cloud, IT, and fintech partners on a regular basis.

Day 21

Wednesday



**Train Employees**

Run programs to teach employees about cybersecurity to help stop phishing and social engineering.

Day 22

Thursday



**Appoint a Security Leader**

Appoint a senior officer (CISO) to handle cyber security and liaise with CERT-In and the other government agencies.

Day 23

Friday



**Update Policies Regularly**

As business, technology, and rules change, make sure to review and update your IT and cyber policies.

Day 24

Saturday



**Create a Security Culture**

Make security a part of your company's culture. Don't just see it as an IT problem; see it as a board-level issue to protect trust and reputation.

Day 25

Sunday



**Use Zero Trust Principles**

Always check, never trust. Make sure that every user, device, and app on the network goes through strict access checks.

Day 26

**NATIONAL CYBERCRIME HELPLINE NUMBER 1930**



# 31 DAYS OF CYBERSECURITY TIPS

**OCTOBER 2025**  
**#WEEK5**

Monday



Secure Development Lifecycle

Include security checks like code review and SAST/DAST tools in the development of banking apps.

Day 27

Tuesday



Protect ATM Infrastructure

Lock down ATM operating systems, set BIOS passwords, and use whitelisting to stop malware from getting in.

Day 28

Wednesday



Monitor Privileged Users

Use Privileged Access Management (PAM) mechanism to keep track of what admins and superusers do.

Day 29

Thursday



Use Data Loss Prevention (DLP)

Set up DLP to stop people from moving sensitive customer or financial data without permission.

Day 30

Friday



Use Network Access Control

Use NAC to only let secure, compliant devices onto the banking network.

Day 31

As this 31-Day Cybersecurity Challenge comes to a close, let this be the start of stronger digital habits — by staying vigilant, applying what has been learned, and sharing knowledge, every SE helps safeguard both themselves and their organization throughout the year.



**NABARD**



International Year  
of Cooperatives



**NATIONAL CYBERCRIME HELPLINE NUMBER 1930**