31 DAYS OF CYBERSECURITY TIPS

OCTOBER 2025 #WEEK1

Wednesday	Thursday	Friday	Saturday	Sunday
				
Know Your Assets	**Set Secure Defaults**	**Patch Quickly**	**Follow Alerts/ Advisories**	**Check for Weaknesses**
Make sure you have an up-to-date list of all your hardware, software, and important apps so that no system is left unprotected.	Make sure that servers, databases, and devices are set up securely from the scratch and turn off services or ports that aren't needed.	Install vendor patches and updates on time to fix known security weakness before hackers can use them.	To stay safe from the recent cyber threats, check CERT-In/NABARD Alerts and advisories on a regular basis and act basis the same.	Regularly conduct IS audits, cyber security audits, vulnerability scans, and penetration tests to find and fix security weakness.
Day 1	Day 2	Day 3	Day 4	Day 5

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

NABARD

2025 International Year of Cooperatives

/nabardonline

NATIONAL CYBERCRIME HELPLINE NUMBER 1930

31 DAYS OF CYBERSECURITY TIPS

OCTOBER 2025 #WEEK2

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
						
Protect Perimeter	**Secure Email**	**Separate Networks**	**No Shared Accounts**	**Use Strong Authentication**	**Review Access Regularly**	**Enforce Separation of Duties**
Use firewalls, an intrusion prevention system, and Web Application Firewalls to protect digital payment channels.	Use SPF, DKIM, and DMARC to stop phishing and fake emails from getting through.	Keep payment systems, CBS, and online banking servers separate from office endpoint networks.	Make sure that each user has their own login ID so that they are responsible and can't misuse it.	Make sure that CBS, admin users, and people who access the system from outside the office all use multi-factor authentication (MFA).	Perform regular reviews of user access and quickly disable access for staff who have left.	No one person should be able to do critical banking tasks without supervision.
Day 6	**Day 7**	**Day 8**	**Day 9**	**Day 10**	**Day 11**	**Day 12**

NATIONAL CYBERCRIME HELPLINE NUMBER 1930

31 DAYS OF CYBERSECURITY TIPS

OCTOBER 2025 #WEEK3

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
						
Secure Endpoints	**Disable Unauthorised Software**	**Safe Backups**	**Test Recovery**	**Have an Incident Plan**	**Report Breaches in 6 Hours**	**Third Parties Security**
To protect laptops, ATMs, and desktops, install anti-malware and turn off USB ports.	Allow only licensed and approved software.	Make regular backups that are encrypted and keep them offline or offsite for safety.	Regularly check that your backups and disaster recovery plans work so that your business can keep going.	Prepare plan and document how to respond to cyber-attacks quickly.	As per CERT-In direction it is advised to report cybersecurity incidents within six hours.	Vendors that handle banking data must meet the same security standards as the bank.
Day 13	**Day 14**	**Day 15**	**Day 16**	**Day 17**	**Day 18**	**Day 19**

NATIONAL CYBERCRIME HELPLINE NUMBER 1930

31 DAYS OF CYBERSECURITY TIPS

OCTOBER 2025 #WEEK4

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
						
Contractual Security	**Vendor Auditing**	**Train Employees**	**Appoint a Security Leader**	**Update Policies Regularly**	**Create a Security Culture**	**Use Zero Trust Principles**
Make sure that contracts for outsourcing include incident reporting, audits, and data protection.	Check the cybersecurity of your cloud, IT, and fintech partners on a regular basis.	Run programs to teach employees about cybersecurity to help stop phishing and social engineering.	Appoint a senior officer (CISO) to handle cyber security and liaise with CERT-In and the other government agencies.	As business, technology, and rules change, make sure to review and update your IT and cyber policies.	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.	Always check, never trust. Make sure that every user, device, and app on the network goes through strict access checks.
Day 20	**Day 21**	**Day 22**	**Day 23**	**Day 24**	**Day 25**	**Day 26**

NATIONAL CYBERCRIME HELPLINE NUMBER 1930

31 DAYS OF CYBERSECURITY TIPS

OCTOBER 2025 #WEEK5

Monday	Tuesday	Wednesday	Thursday	Friday
				
Secure Development Lifecycle	**Protect ATM Infrastructure**	**Monitor Privileged Users**	**Use Data Loss Prevention (DLP)**	**Use Network Access Control**
Include security checks like code review and SAST/ DAST tools in the development of banking apps.	Lock down ATM operating systems, set BIOS passwords, and use whitelisting to stop malware from getting in.	Use Privileged Access Management (PAM) mechanism to keep track of what admins and superusers do.	Set up DLP to stop people from moving sensitive customer or financial data without permission.	Use NAC to only let secure, compliant devices onto the banking network.
Day 27	**Day 28**	**Day 29**	**Day 30**	**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

2025 International Year of Cooperatives

/nabardonline

NATIONAL CYBERCRIME HELPLINE NUMBER 1930