E.HO.DOS/27/02

NABARD

CYBER SECURITY AWARENESS MONTH 2026

Arunachal Pradesh Rural Bank
(Scheduled Bank Owned by Government)

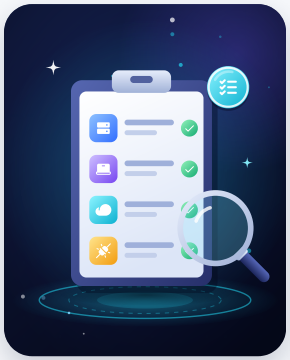
31 DAYS OF CYBERSECURITY TIPS

OCTOBER 2026

#WEEK1

Get the Basics Right

Thursday



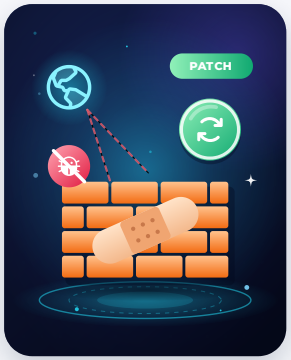
Know Your Assets

Keep an up-to-date list of all hardware, software, APIs and cloud services, including test and old servers. You cannot protect what you do not know.

QUICK CHECK
Is every system, including test servers, in your asset register?

DAY 1

Friday



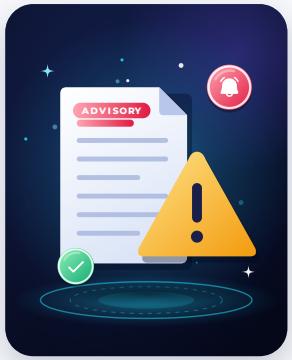
Patch the Edge First

Patch internet-facing systems such as VPNs, firewalls and websites first. Attackers begin exploiting newly announced flaws within days.

QUICK CHECK
Are VPN and firewall patches applied within set timelines?

DAY 2

Saturday



Act on Advisories

Read every CERT-In and NABARD advisory, check whether it applies to your systems, and complete the action within the given timeline.

QUICK CHECK
Is every advisory tracked to closure with a named owner?

DAY 3

Sunday

Use Your .bank.in Domain

Run your website and official emails on the RBI-mandated '.bank.in' domain, and tell customers that genuine bank websites end with .bank.in.

QUICK CHECK
Do your website and official email IDs use .bank.in?

DAY 4

Join the **31-Day Cybersecurity Challenge** - one practical tip every day of October to help SEs stay ahead of today's cyber threats and frauds.

READ today's tip

CHECK it in your bank

ACT and share it

THIS MONTH'S THEMES

WEEK 1	Get the Basics Right	1 - 4 Oct
WEEK 2	Stop Today's Frauds	5 - 11 Oct
WEEK 3	Lock Down Access	12 - 18 Oct
WEEK 4	Detect, Respond, Recover	19 - 25 Oct
WEEK 5	Strengthen Governance	26 - 31 Oct

/nabardonline

NATIONAL CYBERCRIME HELPLINE NUMBER 1930 | Report online: **cybercrime.gov.in**

NABARD

CYBER SECURITY AWARENESS MONTH 2026

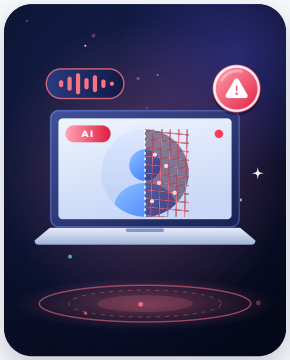
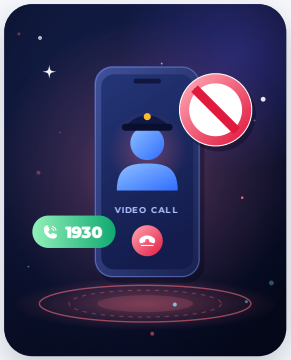
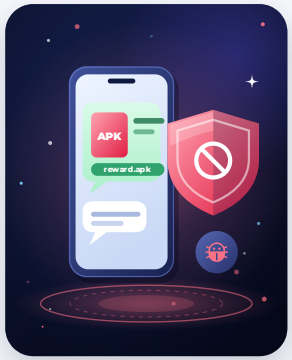
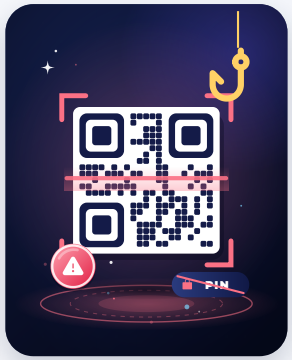
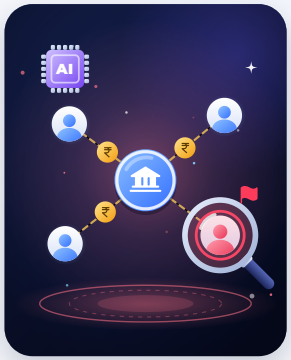
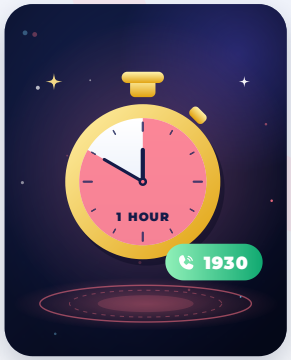
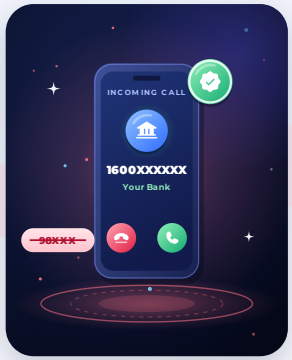
Arunachal Pradesh Rural Bank
(Scheduled Bank Owned by Government)

OCTOBER 2026

31 DAYS OF CYBERSECURITY TIPS

#WEEK2

Stop Today's Frauds

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
						
Spot Deepfakes	**No Digital Arrest**	**Block Fake APK Files**	**Stop QR Code Scams**	**Hunt Mule Accounts**	**Report in the Golden Hour**	**Call from 1600 Numbers**
A video or voice call from a 'senior officer' asking for an urgent transfer or password may be AI-generated. Always verify on a known number first.	There is no 'digital arrest' in law. Police, CBI, ED or RBI officials never arrest anyone or demand money over a video call. Disconnect and call 1930.	Never install '.apk' files received on WhatsApp or SMS, such as fake challan, KYC or reward apps. Download apps only from official app stores.	You never need to scan a QR code or enter your UPI PIN to receive money. Always check the payee name before you pay.	Watch for accounts with sudden large credits and quick withdrawals. Use tools like MuleHunter.AI and act fast on requests from I4C and police.	Report cyber fraud on 1930 or cybercrime.gov.in within the first hour. Quick reporting gives the best chance to freeze the money.	Make all service and transaction calls to customers only from '1600xx' numbers, so customers can tell a genuine bank call from a fraud call.
☑ QUICK CHECK Do staff call back on a known number before acting?	☑ QUICK CHECK Are customers alerted about 'digital arrest' scams via SMS and branches?	☑ QUICK CHECK Are unknown-source app installs blocked on office phones?	☑ QUICK CHECK Do branch staff warn customers about QR 'receive money' scams?	☑ QUICK CHECK Are mule-account alerts reviewed and acted on daily?	☑ QUICK CHECK Is 1930 displayed in every branch and on your website?	☑ QUICK CHECK Have all service and transaction calls moved to 1600 numbers?
DAY 5	DAY 6	DAY 7	DAY 8	DAY 9	DAY 10	DAY 11

NATIONAL CYBERCRIME HELPLINE NUMBER 1930 | Report online: **cybercrime.gov.in**

E.HO.DOS/27/02

NABARD

CYBER SECURITY AWARENESS MONTH 2026

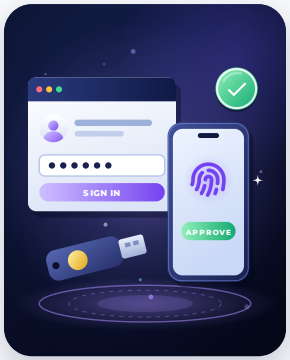
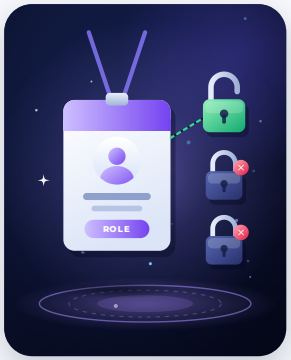
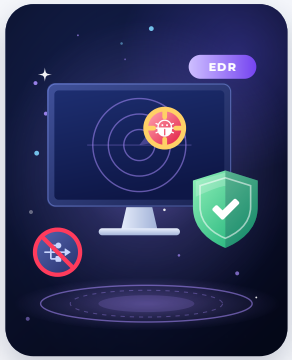
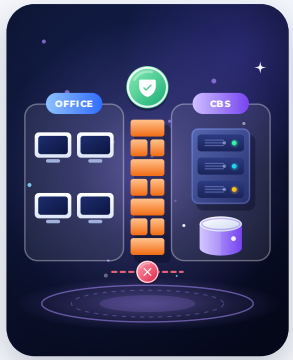
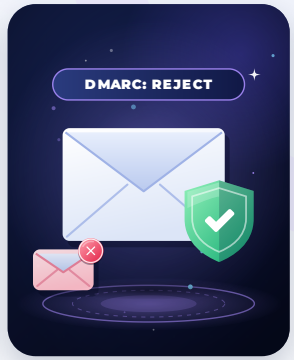
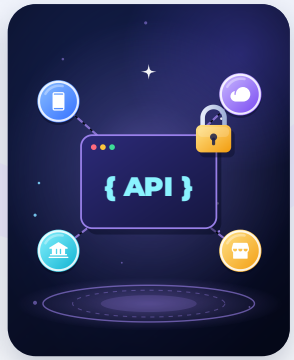
Arunachal Pradesh Rural Bank
(Scheduled Bank Owned by Government)

OCTOBER 2026

31 DAYS OF CYBERSECURITY TIPS

#WEEK3

Lock Down Access

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
						
Use Stronger MFA	**Give Least Privilege**	**Control Admin Access**	**Go Beyond Antivirus**	**Separate Your Networks**	**Harden Your Email**	**Secure Your APIs**
Enable MFA for CBS, email, admin and remote access. Prefer authenticator apps or hardware keys over SMS OTP, which can be stolen through SIM swap.	Give each user only the access their role needs, with no shared IDs. Remove access the same day a staff member leaves or is transferred.	Route all admin and vendor logins to CBS, servers and databases through PAM. Record the sessions and review them regularly.	Use EDR on all servers and desktops to spot ransomware behaviour early, and block USB storage devices by default.	Keep CBS, ATM, payment and DR networks apart from office PCs and internet-facing systems, so one infected PC cannot reach critical systems.	Set DMARC to 'reject' with SPF and DKIM, and tag emails coming from outside the bank. This blocks fake emails sent in your bank's name.	List every API linked to UPI, mobile banking and fintech partners. Protect each one with strong authentication, rate limits and monitoring.
☑ QUICK CHECK **Does every admin and remote login require MFA?**	☑ QUICK CHECK **Were IDs of exited or transferred staff disabled the same day?**	☑ QUICK CHECK **Can anyone reach CBS or database servers without PAM?**	☑ QUICK CHECK **Are all servers and desktops reporting to the EDR console?**	☑ QUICK CHECK **Can an office PC directly reach CBS or the ATM switch?**	☑ QUICK CHECK **Is your domain's DMARC policy set to 'reject'?**	☑ QUICK CHECK **Is there an up-to-date API inventory with named owners?**
DAY 12	DAY 13	DAY 14	DAY 15	DAY 16	DAY 17	DAY 18

E.HO.DOS/27/02

NABARD

CYBER SECURITY AWARENESS MONTH 2026

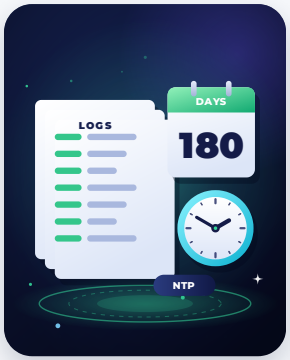
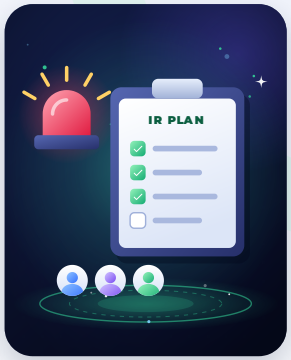
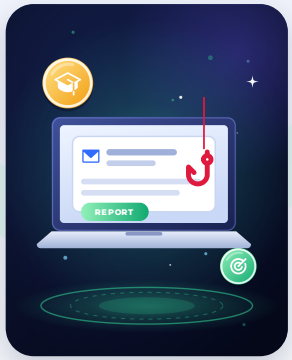
Arunachal Pradesh Rural Bank
(Scheduled Bank Owned by Government)

31 DAYS OF CYBERSECURITY TIPS

OCTOBER 2026

#WEEK4

Detect, Respond, Recover

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
						
Keep Logs for 180 Days	**Watch 24x7**	**Report within 6 Hours**	**Ransomware-Proof Backups**	**Test Your Recovery**	**Rehearse the Response**	**Train with Real Drills**
As per CERT-In directions, keep logs of all ICT systems for 180 days within India and sync system clocks with NIC or NPL time servers.	Have a Security Operations Centre (own or shared) monitor alerts from CBS, firewalls, servers and endpoints round the clock, and act on them fast.	Report cyber incidents to CERT-In within 6 hours of noticing them, and inform NABARD/RBI as per extant instructions.	Follow the 3-2-1 rule: 3 copies of data, on 2 different media, with 1 copy offline or immutable, so ransomware cannot reach it.	Run DR drills and restore data from backups regularly. A backup that has never been restored is only a hope, not a plan.	Keep your incident response and crisis communication plan updated, and test it with tabletop exercises that include top management.	Run phishing simulations and short monthly sessions so every employee can spot and report suspicious emails, calls and links.
☑ QUICK CHECK Can you pull a log entry from 170 days ago?	☑ QUICK CHECK Who acts on a critical alert at 2 AM on a Sunday?	☑ QUICK CHECK Are the CERT-In reporting format and contacts ready?	☑ QUICK CHECK Is at least one backup copy offline or immutable?	☑ QUICK CHECK When did you last restore data and run from DR?	☑ QUICK CHECK Has top management joined a tabletop exercise this year?	☑ QUICK CHECK What was the click rate in your last phishing drill?
DAY 19	DAY 20	DAY 21	DAY 22	DAY 23	DAY 24	DAY 25

NATIONAL CYBERCRIME HELPLINE NUMBER 1930 | Report online: cybercrime.gov.in

E.HO.DOS/27/02

NABARD

CYBER SECURITY AWARENESS MONTH 2026

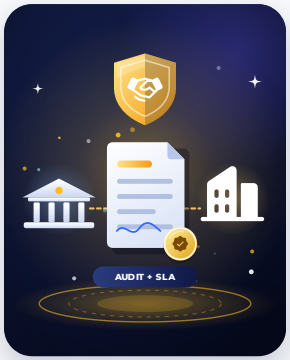
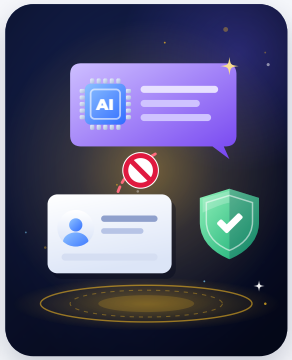
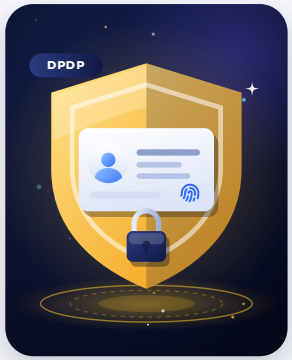
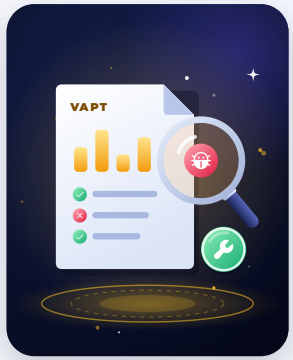
Arunachal Pradesh Rural Bank
(Scheduled Bank Owned by Government)

OCTOBER 2026

31 DAYS OF CYBERSECURITY TIPS

#WEEK5

Strengthen Governance

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
					
Vendor Risk is Your Risk	**Secure the Cloud**	**Use AI Safely**	**Protect Personal Data**	**Close Audit Gaps**	**Lead from the Board**
Your CBS, ASP and IT vendors must meet your security standards. Ask for audit reports and VAPT closure, and add incident-reporting clauses to contracts.	Check cloud settings regularly: no public storage, MFA on admin consoles, encryption switched on, and payment data stored only in India.	Never paste customer or bank data into public AI chatbots. Use only approved AI tools and check AI answers before relying on them.	Prepare for the DPDP Act, 2023: collect only the customer data you need, keep it secure, and be ready to report breaches under the DPDP Rules, 2025.	Get VAPT and IS audits done by CERT-In empanelled auditors, close critical findings quickly and re-test. An open finding is an open door.	Make cyber risk a regular Board agenda item: review incidents, audit findings and security spending. Security is everyone's job, led from the top.
☑ QUICK CHECK **Do vendor contracts include audit rights and incident timelines?**	☑ QUICK CHECK **Is any cloud storage or admin console open to the internet?**	☑ QUICK CHECK **Does your bank have an approved AI usage policy?**	☑ QUICK CHECK **Do you know where all customer personal data is stored?**	☑ QUICK CHECK **Are critical VAPT findings closed and re-tested?**	☑ QUICK CHECK **Did the Board review cyber risk at its last meeting?**
DAY 26	DAY 27	DAY 28	DAY 29	DAY 30	DAY 31

STAY ALERT. STAY SAFE.

As this 31-Day Challenge ends, let it be the start of stronger digital habits. Stay alert, apply what you have learned and share it - every SE helps keep banking safe all year.

31/31 COMPLETED

/nabardonline

NATIONAL CYBERCRIME HELPLINE NUMBER 1930 | Report online: **cybercrime.gov.in**