NABARD

DoS - CSITE Cell

Celebrate Cybersecurity Awareness Month

October 2024

31 Days of Cybersecurity Safeguards

Day 1	Day 2	Day 3	Day 4	Day 5
Create alphanumeric passwords (at least 12 characters, including letters, numbers, and symbols) and avoid using personal information	Activate two-factor authentication (2FA) on all accounts to add an extra layer of security.	Be aware of unsolicited requests for sensitive information, whether via phone or email.	Use a Virtual Private Network (VPN) when accessing sensitive information on public Wi-Fi.	Update your operating systems, applications, and antivirus software updated to protect against vulnerabilities.
Day 6	**Day 7**	**Day 8**	**Day 9**	**Day 10**
Change PIN of Debit/ Credit Card and UPI account regularly.	Check for any passwords/ PIN written on paper and discard them.	Host an open forum for employees to ask cybersecurity-related questions.	Ensure you're accessing the website via HTTPS, especially when entering sensitive information	Be cautious about sharing personal or financial information online or over the phone.
Day 11	**Day 12**	**Day 13**	**Day 14**	**Day 15**
Configure Ad-blocker in your PC.	Educate Yourself on Phishing	Regularly back up critical data to a secure location, either in the cloud or an external hard drive.	Delete your browsing history and cache at the end of each day to protect sensitive information.	Review and update your privacy settings on social media and online services.
Day 16	**Day 17**	**Day 18**	**Day 19**	**Day 20**
Enable account alerts for transactions, logins, and changes to account settings.	Turn off auto-fill features in browsers for sensitive information like passwords and personal details.	Review apps permission in your mobile and limit.	Learn about Browser Privacy settings (Incognito- InPrivate Mode in web browsers)	Use biometric security features (like fingerprint or face recognition) on your mobile devices.
Day 21	**Day 22**	**Day 23**	**Day 24**	**Day 25**
Share cybersecurity tips with family members, especially if they access your devices.	Ensure that you do not use personal email or social media accounts for any work-related communication.	Learn how and where to report Cyber Crime.	Subscribe to cybersecurity newsletters or alerts to keep up with new threats and trends.	Track your subscriptions and services, ensuring you're only using trusted and necessary ones.
Day 26	**Day 27**	**Day 28**	**Day 29**	**Day 30**
Review your email and delete spam or junk emails immediately and unsubscribe from unnecessary mailing lists.	Familiarize yourself with your organization's incident response plan and know your role.	Disable international transactions on payment channels, if not needed.	Set your computer to activate a screen saver with a password after a few minutes of inactivity.	Review and manage your browser extensions, removing any that are unnecessary or untrusted.
Day 31				
Ensure that your devices have security settings enabled, such as firewalls and encryption.				