Cyber Security Awareness: DOs and DON'Ts Guidelines

General Computer Usage	
DOs	**DON'Ts**
Always download applications and software from trusted and authorized sources	Do not install pirated, cracked, or unauthorized software. These may contain malware
Keep operating systems, applications, and security software up to date	Do not ignore software or security updates
Lock screens and keep desk clean when unattended	Do not leave documents, notes, or screens visible to unauthorized persons
Backup important data regularly as per organizational requirements	Do not store sensitive information in unauthorized locations
Report suspicious system behaviour or security concerns promptly	Do not bypass or disable security controls
Scan all USB drives and external media before use	Do not connect unknown or unapproved USB devices to company systems

Incident Reporting & Fraud Prevention	
DOs	**DON'Ts**
Report phishing attempts, malware alerts, and suspicious activities immediately	Do not ignore security alerts or suspicious events
Report lost or stolen devices without delay	Do not delay reporting security incidents
Verify payment instructions and financial requests through approved channels.	Do not process transactions solely based on email instructions.
Report suspected fraud, unauthorized access, or data leakage promptly.	Do not conceal security incidents or policy violations.
Report cyber security incidents immediately to: IT / Information Security Team: infosec@namfin.in Mobile: 9588842700 IT Ticketing Portal: https://itconnect.namfin.in/ Immediate Reporting Line: Your Reporting Manager	

Data Protection & Privacy	
DOs	**DON'Ts**
Protect customer, employee, and business information	Do not share confidential information with unauthorized persons
Access information only when required for authorized purposes	Do not access information beyond your authorized role
Ensure sensitive information is protected from unauthorized viewing	Do not leave confidential documents or screens exposed
Follow applicable data privacy and information security requirements	Do not store sensitive data on personal devices or unapproved platforms
Verify recipients before sharing sensitive information	Do not discuss confidential information in public places
Use only approved organizational storage systems for business data	Do not store or transfer company data to personal email, cloud storage, or unauthorized applications

Password & Authentication Security Management	
DOs	**DON'Ts**
Use strong and unique passwords for each account	Do not use weak or easily guessable passwords such as Password@123, 123456, name, DOB, or mobile number
Enable Multi-Factor Authentication (MFA) wherever available	Do not share passwords, OTPs, or authentication codes
Use different passwords for different accounts and services so that if one password is compromised, other accounts remain secure	Do not reuse passwords across multiple accounts
Change passwords immediately if compromise is suspected	Do not write passwords down or leave them visible
Protect your login credentials at all times	Do not save passwords in unsecured files or locations which is easily visible

Internet, Remote Working Security & Device Security	
DOs	**DON'Ts**
Use secure and trusted internet connections	Do not use unsecured public Wi-Fi when accessing sensitive information
Keep Wi-Fi and Bluetooth disabled when not required.	Do not leave active sessions unattended.
Be cautious if you are asked for personal information	Don't use illegal software and programs
Use organization-approved devices for official work whenever possible	Do not access sensitive systems from public or shared computers
Ensure confidential information cannot be viewed by unauthorized persons	Do not discuss sensitive information in public areas
Install applications only from trusted and approved sources	Do not install unverified or unauthorized mobile or desktop applications

Email & Phishing Security	
DOs	**DON'Ts**
Verify the sender before opening emails, links, or attachments	Don't open email attachments from unknown sources or suspicious sources
Report suspicious emails, messages, or links immediately	Do not click on suspicious links or pop-up messages
Carefully check email addresses for authenticity	Do not respond to phishing, spam, or fraudulent communications
Verify requests for payments, account changes, or sensitive data through approved channels	Do not act on urgent requests received via email, SMS, or phone without verification
Use digital signatures where applicable to ensure email authenticity	Don't respond or reply to spam in any way
Confirm unusual instructions even if they appear to come from senior management	Do not trust messages based only on authority or urgency

Customer Security Awareness	
DOs	**DON'Ts**
Verify website URLs before entering credentials or personal information	Do not share OTPs, passwords, PINs, or authentication codes with anyone
Use strong and unique passwords for online accounts and services	Do not click on links received from unknown or unverified sources
Contact official support channels only through details published on the company's website	Do not disclose personal or financial information in response to unsolicited calls, emails, SMS, or social media messages
Verify payment requests directly with the concerned party before making transfers.	Do not scan QR codes or approve payment requests received from unknown persons.
Ensure you are on a secure website indicated by "https://" and the correct domain name.	Do not enter credentials on websites reached through pop-ups or suspicious advertisements.
Keep registered mobile number and email address updated for receiving security alerts.	Do not share screenshots containing account details, OTPs, or sensitive information.
Be cautious of messages creating urgency, fear, or pressure to act immediately.	Do not respond to threats of account suspension or KYC expiry without verifying through official channels.

Cyber Security is Everyone's Responsibility:

Stay vigilant, protect sensitive information, and promptly report suspicious activities. At Namdev Finvest Limited, we are committed to fostering a secure digital environment through the shared responsibility of our employees, customers, and business partners.