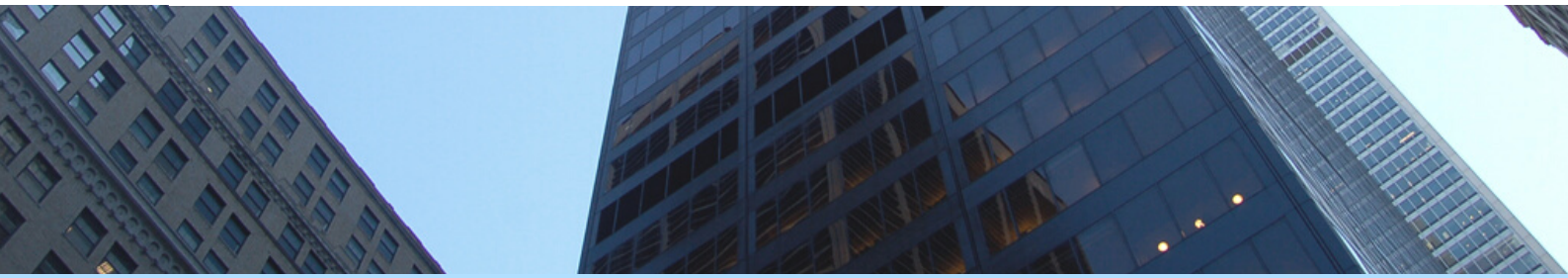
Securze

Be Secured, Be Assured.



CYBERSECURITY: THE DO's AND DON'Ts FOR EVERY EMPLOYEE

www.securze.com

info@securze.com

+91 84510 73938

securze

securze_com

Securze

Cybersecurity is essential in any workplace, and employees play a crucial role in maintaining a secure environment.

DOs:

Use Strong Passwords: Create complex passwords and update them regularly. Use a mix of letters, numbers, and special characters.

Enable Two-Factor Authentication (2FA): Whenever possible, enable 2FA to add an extra layer of security to your accounts.

Lock Devices: Lock your computer and mobile devices whenever you leave your desk to prevent unauthorized access.

Update Software: Keep operating systems, applications, and antivirus programs up-to-date to protect against known vulnerabilities.

Be Cautious with Emails: Avoid opening emails or attachments from unknown sources. Be vigilant about phishing attempts.

Use Encrypted Connections: Ensure websites you visit use HTTPS, especially when dealing with sensitive information.

Secure Wi-Fi Connections: When using Wi-Fi, connect to secure, password-protected networks rather than public, unsecured ones.

Report Suspicious Activities: If you notice anything unusual, such as strange pop-ups or unexpected requests for information, report it to your IT department.

Encrypt Sensitive Data: If you handle sensitive information, use encryption tools to secure the data both in transit and at rest.

Backup Data: Regularly back up important files and data to prevent data loss in case of a cybersecurity incident.

Use Company Resources Responsibly: Use company-provided devices and resources for work-related tasks only, avoiding personal or unauthorized software installations.

Be Aware of Social Engineering: Be cautious about sharing personal or company information over the phone or in person, even if the requester seems legitimate.

DON'Ts:

Share Passwords: Never share your login credentials or passwords with anyone, including colleagues.

Clean Desk and Desktop: Keep your desk and desktop clean. Don't write sensitive data such as customer details, password and stick them on/near your desk. Anyone unknown passing by can steal this data.

Click on Suspicious Links: Avoid clicking on links in emails or messages from unknown sources. Hover over links to see the actual URL before clicking.

Download Unauthorized Software: Do not download or install software or apps without approval from the IT department. Unauthorized software can contain malware.

Leave Devices Unattended: Do not leave your computer, tablet, or smartphone unattended, especially in public places.

Ignore Security Updates: Regularly update your software and applications. Ignoring updates can leave your system vulnerable to attacks.

Connect to Public Wi-Fi Unprotected: Avoid connecting to public Wi-Fi networks without a VPN (Virtual Private Network) to encrypt your connection.

Store Sensitive Information Insecurely: Do not store sensitive information on easily accessible locations such as sticky notes, physical documents, or unencrypted files.

Engage in Risky Online Behavior: Avoid visiting suspicious websites, downloading files from untrustworthy sources, or engaging in online activities that might compromise security.

How Securze can help?

At Securze, we offer comprehensive Cyber Security Awareness Training to elevate your employees' security practices to a best-in-class level for your business. A single oversight from an employee can lead to significant consequences due to inadequate training on common cyber attack vectors. We specialize in training your employees, equipping them with effective cyber attack defense strategies, and ensuring they stay consistently updated on the latest cyber trends. For more info, reach out to us at info@securze.com

A TEAM OF PROFESSIONALS WHO HAVE TRAINED -

ICICI Lombard GENERAL INSURANCE

AXIS BANK

IDBI BANK

ICICI Bank

HDFC BANK

IDFC FIRST Bank

आर सी एफ

and many more...

Securze
Be Secured, Be Assured.

For business inquiries, **contact us.**

www.securze.com

info@securze.com

+91 84510 73938

securze

securze_com

Securze