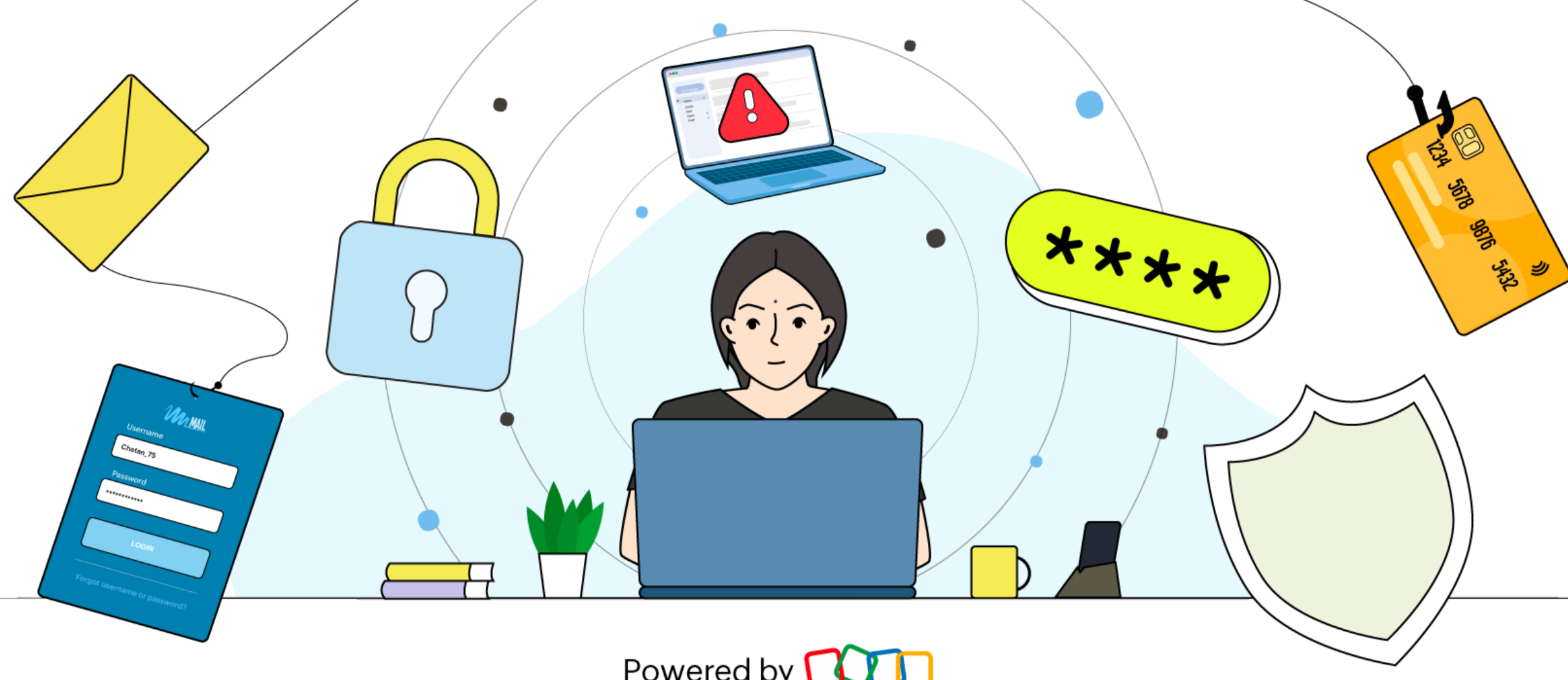



Workplace Security



Powered by 

26%

of employees admitted they would let someone into a secure area without verifying their identity.

25%

of employees say they leave their computer unlocked and unattended.

1 in 3

Android smart phones are not secured with a lockscreen passcode; the most basic level of protection.



30%

of internet users have experienced a data breach due to a weak password.

\$2.5M

Companies lose an average from the loss of memory sticks.

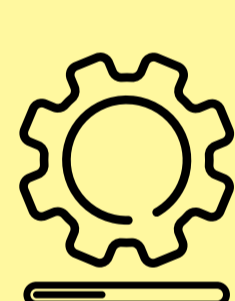
Good cyber hygiene in the workplace



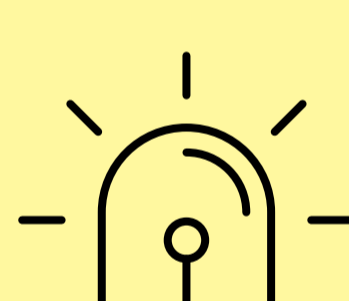
Always **lock your computer and phone** when stepping away.



Avoid public Wi-Fi for work-related tasks.



Install security patches and updates to prevent vulnerabilities.



Immediately **inform IT/system admin** if you notice suspicious activity.



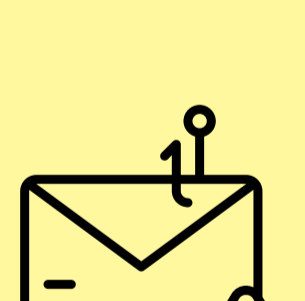
Keep sensitive documents locked away and **dispose** them properly.



Implement **complex, unique passwords** and enable **multi-factor authentication (MFA)**.

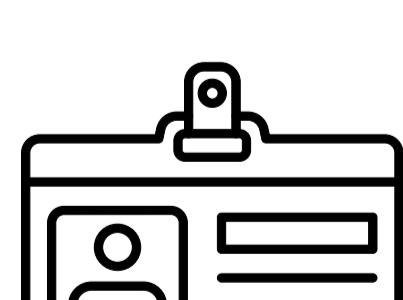


Verify links before clicking, and check attachments before downloading.



Verify emails and messages before sharing credentials or downloading files.

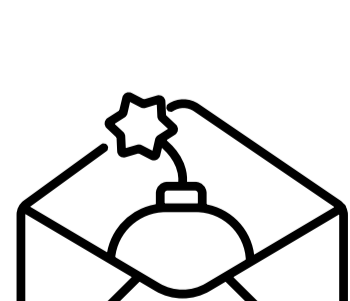
Workplace security mistakes to avoid



Don't share your ID card or allow tailgating.



Don't auto-forward emails to personal accounts.



Don't click on suspicious links or download unexpected attachments.



Don't use weak passwords—avoid short, predictable, or easily guessable ones.