KnowBe4
Human error. Conquered.

CYBER
Solutions

# USE STRONG PASSWORDS

## AND A PASSWORD MANAGER

Creating a robust password is essential for online security, as it acts as the primary defense against unauthorised access to personal and sensitive information. With cyber-attacks becoming more advanced, using easily guessable or weak passwords poses a significant risk to individuals and organizations. Creating and regularly updating strong passwords is an essential habit to protect against hacking attempts, identity theft, and data breaches.

### USE A COMPANY APPROVED PASSWORD MANAGER

Use a company-approved password manager to securely store and manage your passwords, ensuring only authorized individuals can access them. This method creates unique passwords for each account, reducing the risk of security breaches. Adhere to your organization's password management guidelines for optimal security.

### SET A UNIQUE PASSWORD FOR EACH ACCOUNT

Avoid reusing the same password across multiple accounts to prevent hackers from accessing all your accounts. If one account is compromised, hackers could potentially gain access to all your accounts using the same credentials. Use unique passwords for each account and use a password manager for secure tracking.

### FOLLOW YOUR COMPANY PASSWORD POLICY

Following your organization's current password policies is one of your top responsibilities. Failure to do so could lead to security incidents that provide unauthorized access to attackers.

### UPDATE YOUR PASSWORD REGULARLY

It's important to regularly update your passwords, especially for important accounts such as emails, banking, or company systems. Changing passwords frequently helps reduce the chance of unauthorized access, especially after potential data breaches. If you think any account may have been compromised, change the password right away to prevent additional harm.

www.c1-s.com