



BUSINESS EMAIL COMPROMISE

Access control of an email account
which may lead to a data breach.





BUSINESS EMAIL COMPROMISE

Access control of an email account
which may lead to a data breach.





BUSINESS EMAIL COMPROMISE

Access control of an email account
which may lead to a data breach.





BUSINESS EMAIL COMPROMISE

Access control of an email account
which may lead to a data breach.





RANSOMWARE

Use malware to lock a device, encrypt files and demand a large ransom.





RANSOMWARE

Use malware to lock a device, encrypt files and demand a large ransom.





RANSOMWARE

Use malware to lock a device, encrypt files and demand a large ransom.





RANSOMWARE

Use malware to lock a device, encrypt files and demand a large ransom.





PHISHING

Send malicious links in a fraudulent email to gain sensitive personal information.





PHISHING

Send malicious links in a fraudulent email to gain sensitive personal information.





PHISHING

Send malicious links in a fraudulent email to gain sensitive personal information.





PHISHING

Send malicious links in a fraudulent email to gain sensitive personal information.





VIRUS

Deploy malicious code to spread through a company's system and corrupt files.





VIRUS

Deploy malicious code to spread through a company's system and corrupt files.





VIRUS

Deploy malicious code to spread through a company's system and corrupt files.

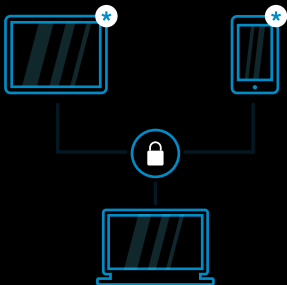




VIRUS

Deploy malicious code to spread through a company's system and corrupt files.

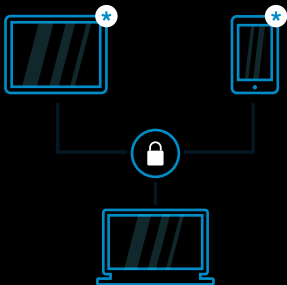




MULTI-FACTOR AUTHENTICATION

You have multi-factor authentication
activated on all administrator accounts.

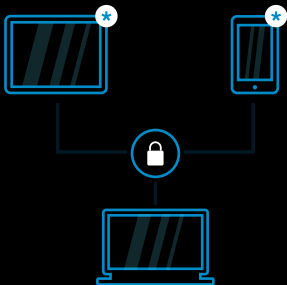




MULTI-FACTOR AUTHENTICATION

You have multi-factor authentication
activated on all administrator accounts.

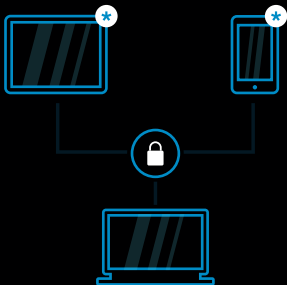




MULTI-FACTOR AUTHENTICATION

You have multi-factor authentication
activated on all administrator accounts.





MULTI-FACTOR AUTHENTICATION

You have multi-factor authentication
activated on all administrator accounts.





BACK-UPS

You back-up your data frequently online and offline and test your back-up plan.





BACK-UPS

You back-up your data frequently online and offline and test your back-up plan.





BACK-UPS

You back-up your data frequently online and offline and test your back-up plan.

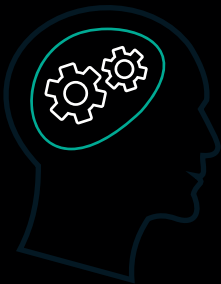




BACK-UPS

You back-up your data frequently online and offline and test your back-up plan.

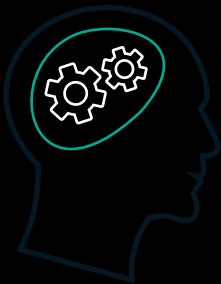




EMPLOYEE TRAINING

Your team's training means cyber crime
is identified before it causes harm.

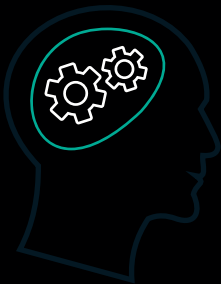




EMPLOYEE TRAINING

Your team's training means cyber crime
is identified before it causes harm.





EMPLOYEE TRAINING

Your team's training means cyber crime
is identified before it causes harm.





EMPLOYEE TRAINING

Your team's training means cyber crime
is identified before it causes harm.





ANTI-VIRUS

Your system detects malware and stops it from becoming a ransomware attack.





ANTI-VIRUS

Your system detects malware and stops it from becoming a ransomware attack.





ANTI-VIRUS

Your system detects malware and stops it from becoming a ransomware attack.





ANTI-VIRUS

Your system detects malware and stops it from becoming a ransomware attack.





SECRET WEAPON

Security star! Like other expert firms, you devoted 24% of your IT budgets to cyber.





SECRET WEAPON

Security star! Like other expert firms, you devoted 24% of your IT budgets to cyber.





SECRET WEAPON

Security star! Like other expert firms, you devoted 24% of your IT budgets to cyber.





SECRET WEAPON

Security star! Like other expert firms, you devoted 24% of your IT budgets to cyber.



RULES

Cards:

- 4 security + 4 attack in 4 colours
- 4 'Secret Weapons'

Rules:

- Deal: 4 players = 7 cards / 3 players = 9
- Place deck aside
- Player 1: plays attack card
- Player 2: plays matching colour security card OR Secret Weapon
- Next player: plays any coloured attack card
- Next player responds to last card
- Deck gone? Can't go? You're eliminated
- Winner = final player to play last card
OR last player standing