

Tightening Digital Perimeters with Multi-Factor Authentication (MFA)

100

Is the average # of passwords people juggle today when it comes to their digital encounters.

81%

Of security breaches are due to stolen or weak passwords.

61%

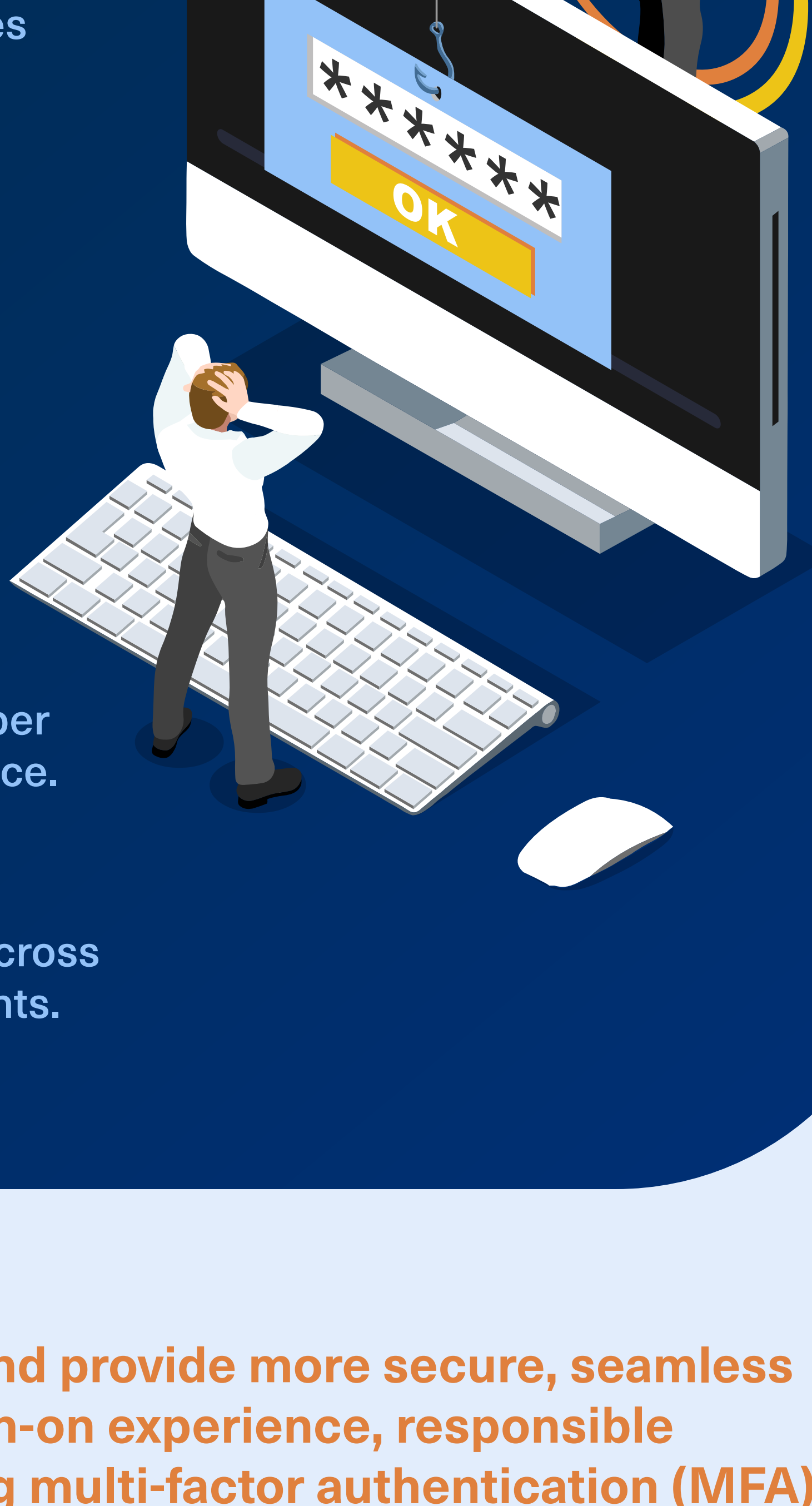
Of people reuse passwords across multiple accounts.

51%

Of individuals struggle to remember their log-in details while at the office.

44%

Of employees reuse passwords across personal and work-related accounts.



To bypass bad habits and provide more secure, seamless and satisfying sign-on experience, responsible organizations are adding multi-factor authentication (MFA) to their security playbook.

What Is MFA and How Does It Work?



MFA is a digital authentication method that grants users access to a website, system or data only after they present two or more factors (AKA pieces of evidence) to prove they are who they say they are.

MFA systems use a combination of a:

- Password
- Physical token (mobile device, smartcard, one-time password/OTP, etc.)
- Biometric (finger or face)
- Or location factor

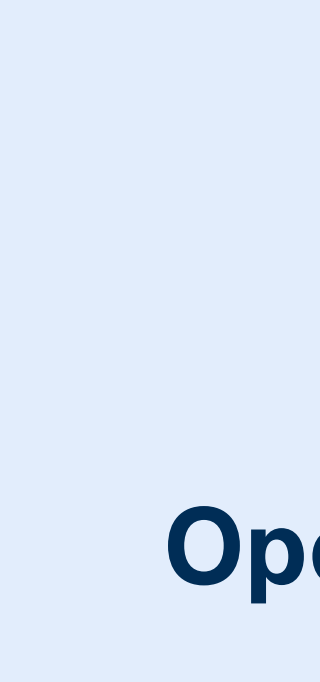
MFA provides an added layer of security!

- Used on top of standard usernames and passwords
- Ensures applications are accessed by the right person, every time.
- Balances protection, encryption and ease-of-use, while ensuring the sign-on experience is efficient and seamless for all.

Advantages of Multi-Factor Authentication



Stronger Authentication



Enhanced Security



Better User Experience



Increased Productivity



Reduced Operational Costs

MFA's Triple Threat

RFID Readers & Modules

Credentials

Application Software



Protection Across Industries

Banking/financial:

- Simple and convenient authentication
- Real-time access security and fraud prevention
- Enhanced protection of transactions
- Compliance with data protection and privacy regulations

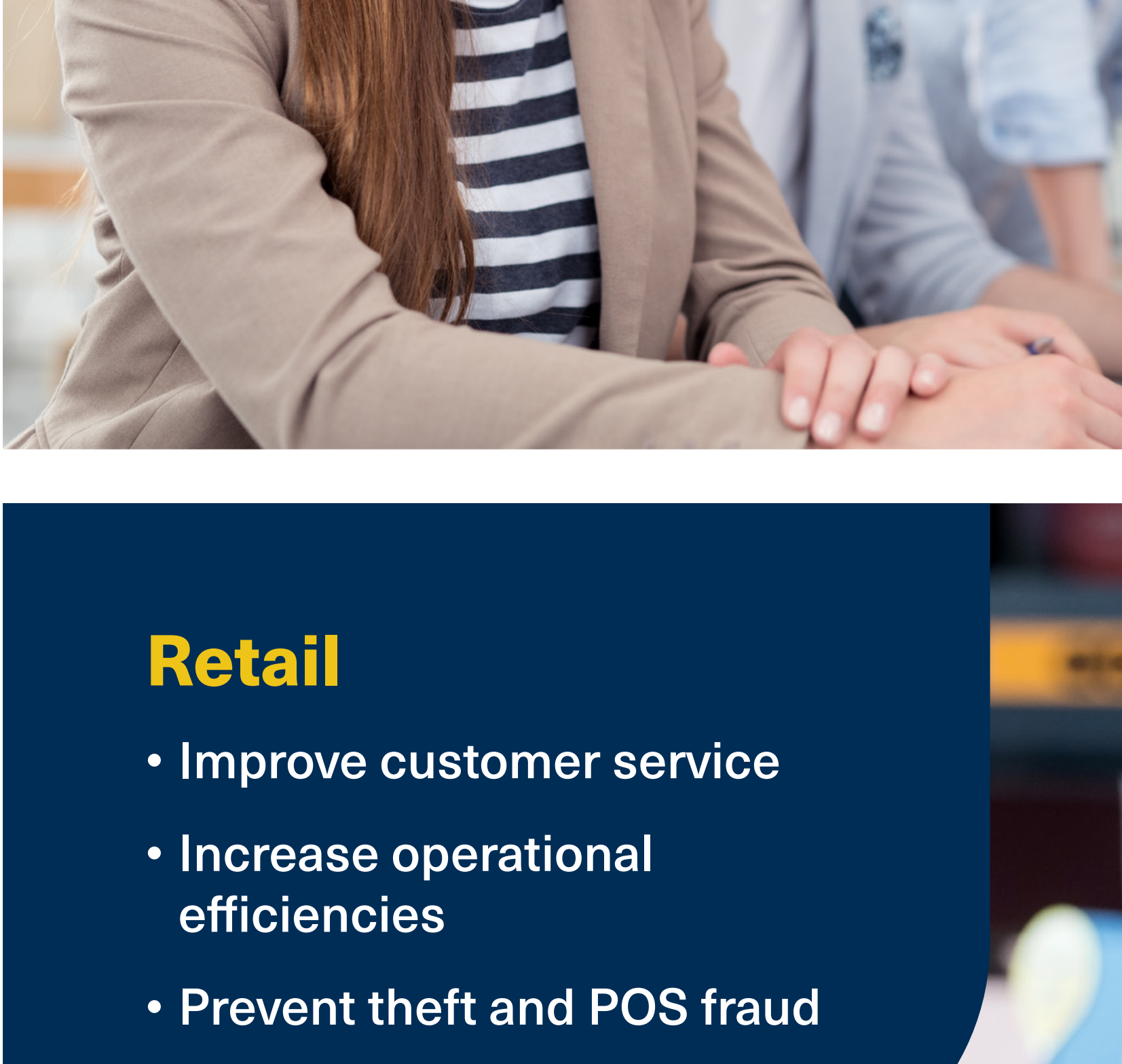


Government:

- Secure access to government services and critical applications
- Frictionless identity verification
- Protect sensitive government data
- Compliance to standards and Regulations

Healthcare

- Quickly verify patients, doctors and staff for confidential information
- Protect patient records and data
- Secure authentication to shared workstations
- Improve efficiency and save time
- Touchless, hygienic transactions
- Compliance (HIPAA/EPCS)

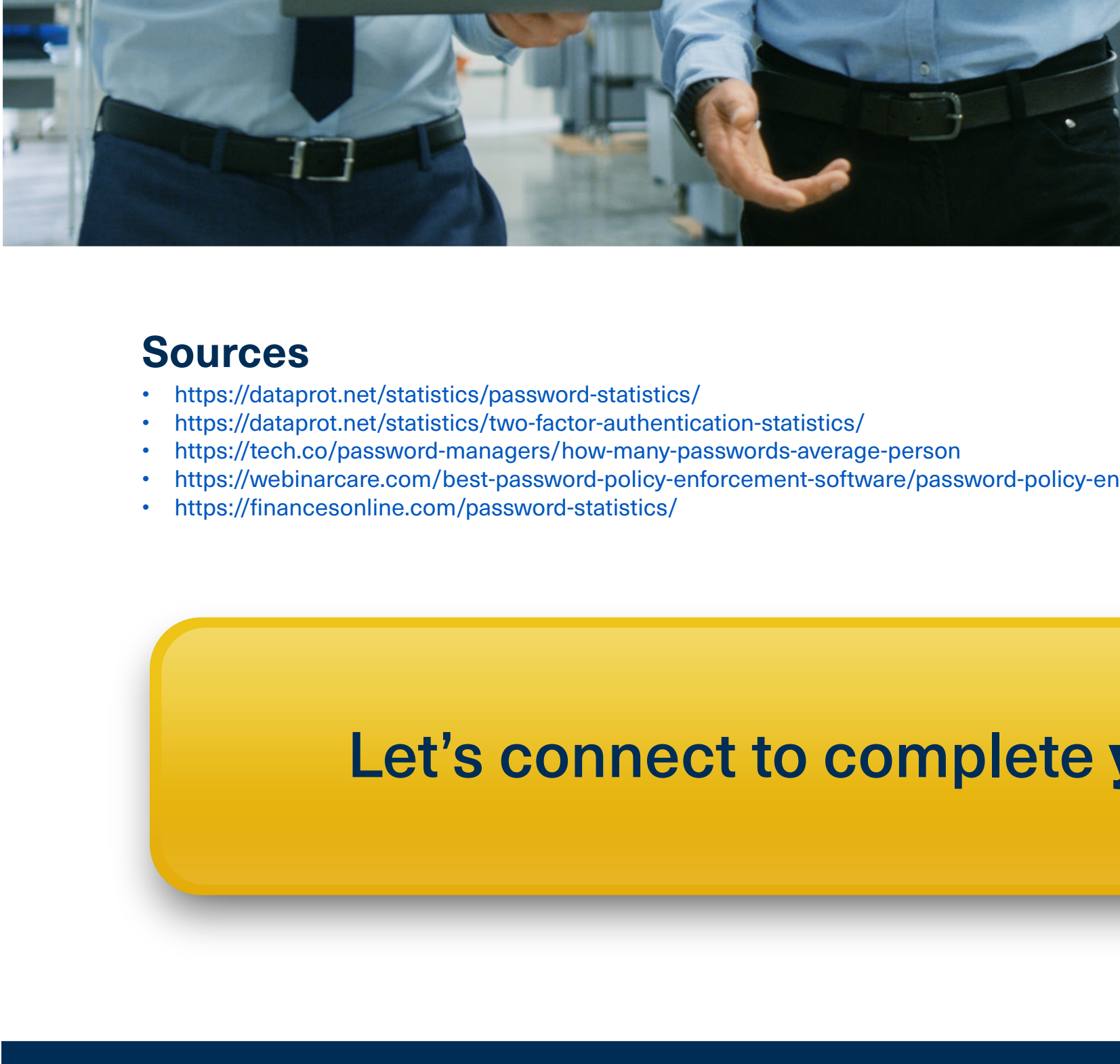


Enterprise/Workplace

- Secure, seamless authentication
- Simple security for hybrid workplaces mixing in-office and remote work
- Works with many third-party applications leveraging single-sign on (SSO)

Retail

- Improve customer service
- Increase operational efficiencies
- Prevent theft and POS fraud



Manufacturing/Warehouses

- User verification effectiveness
- Secure access to machines
- Inventory with confidence

Sources

- <https://dataprot.net/statistics/password-statistics/>
- <https://dataprot.net/statistics/two-factor-authentication-statistics/>
- <https://tech.co/password-managers/how-many-passwords-average-person>
- <https://webinarcare.com/best-password-policy-enforcement-software/password-policy-enforcement-statistics/#7>
- <https://financesonline.com/password-statistics/>

Let's connect to complete your security picture!