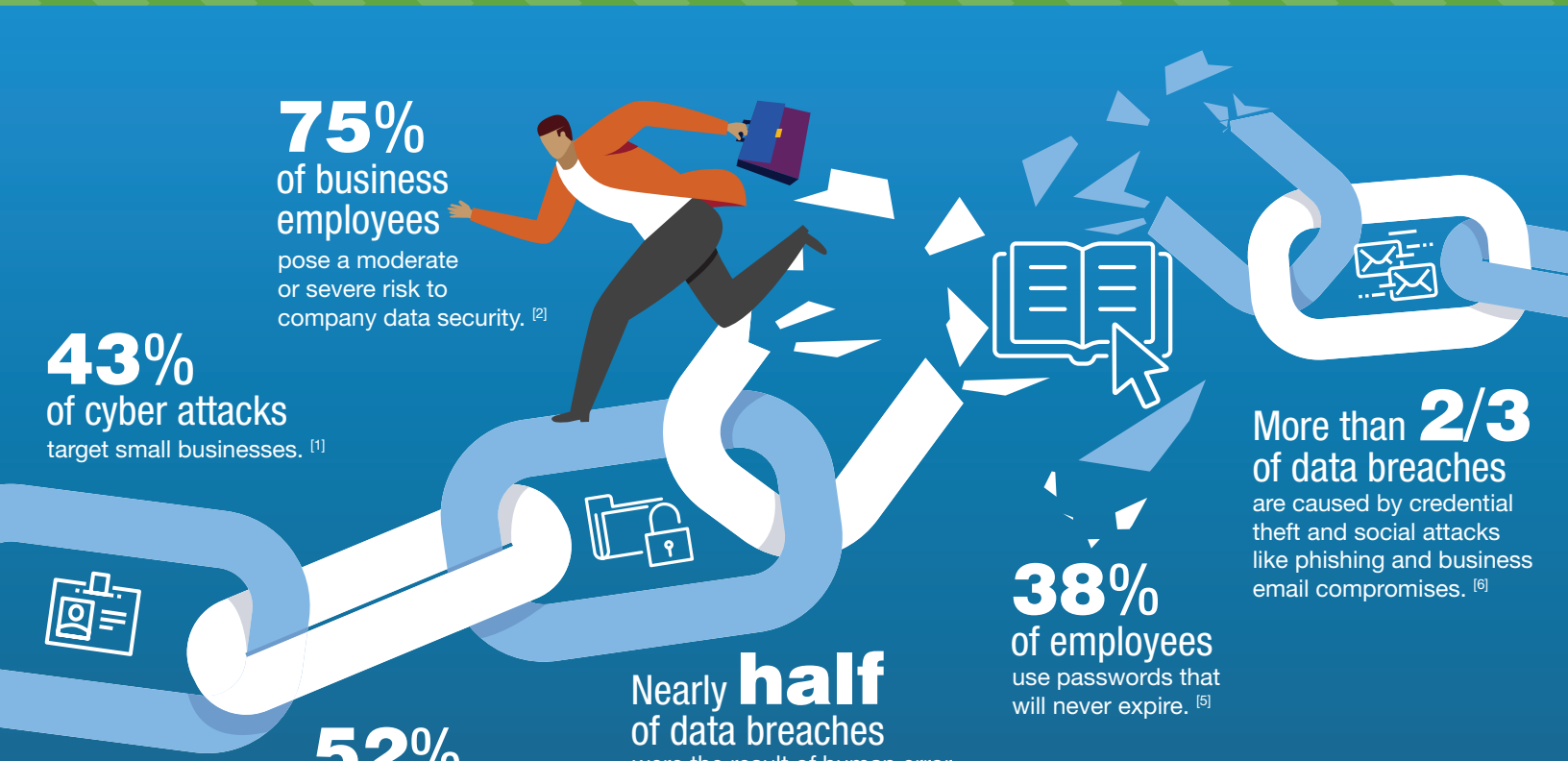
Cybersecurity Opportunity:
Teach employees to avoid cybersecurity incidents.

Every employee in your organization plays an important role in helping protect sensitive business data and systems from cyberattack.

Investing in employee training can greatly strengthen corporate cybersecurity.

Here's why you'll find your greatest opportunity in proper employee education:



75% of business employees pose a moderate or severe risk to company data security. [2]

43% of cyber attacks target small businesses. [1]

52% of business leaders don't know how to respond to a cybersecurity incident. [3]

Nearly **half** of data breaches were the result of human error and system glitches. [4]

38% of employees use passwords that will never expire. [5]

More than **2/3** of data breaches are caused by credential theft and social attacks like phishing and business email compromises. [6]

ONLY **31%** of employees said they receive annual company-wide cyber security training or updates. [7]

[1] Verizon, 2019 Verizon Data Breach Investigations Report
[2] MediaPRO, 2018 State of Privacy and Security Awareness Report
[3] CyberArk, 2018 Global Advanced Landscape Report: Focus on Devops
[4] Ponemon Institute and IBM Security, 2019 Cost of a Data Breach Report
[5] Varonis, 2019 Global Data Risk Report
[6] Verizon, Verizon Business 2020 Data Breach Investigations Report
[7] Chubb, Third Annual Cyber Report, July 2019

CYBERSCOUT®

Five Ways to Bolster Your IT Security Strategy with Employee Training

Employee cybersecurity education is an opportunity to strengthen your company's cyber defenses where you're most likely to be attacked—at a human level.

Take proactive steps now to protect your organization from a data breach. First, ensure your IT security strategy prevents malicious content from reaching your employees. Then, toughen your defenses by continually educating your workforce about security best practices and common scams.

1. **Train *everyone*.**
   Share information about policies and best practices with everyone in your organization—not just IT staff or business leaders. Implement a regular schedule of engaging training sessions to keep employees up to date about new risks and vulnerabilities.
2. **Promote good password hygiene.**
   Since 2 in 3 users reuse passwords to access different accounts [1], chances are that your employees may be using the same credentials for both personal and business accounts. Teach employees how to create a strong password and the importance of unique passwords. Be sure to require regular password updates and limit the number of unsuccessful log-in attempts to minimize credential attacks.
3. **Teach how to avoid common phishing scams and spot email spoofing.**
   Educate employees about common phishing scams and show them how computers get infected from malicious email and other links. Share tips for spotting, avoiding, and protecting against business email compromises, spoofing, ransomware, and downloading infected files.
4. **Experiment with simulated attacks and conduct practice drills.**
   Build a knowledgeable and more secure workforce through mock attacks and simulated phishing drills. Train employees through experience to avoid scams and gain insight into the risks across your organization. Tailor your security awareness and education plan accordingly.
5. **Create a data breach response plan.**
   The FTC [2] recommends for all businesses to be prepared with a plan to save data, run the business, and notify customers if a breach is experienced. Provide employees with actionable steps to limit the damage if a mistake has been made and data was compromised

[1] "Google Survey Finds Two in Three Users Reuse Passwords," Info Security Magazine, February 2019

[2] FTC. "FTC's Data Breach Response: A Guide for Business," ftc.gov/DataBreach