Cybersecurity at Work Stats and Facts

FACTS

1. **Phishing Attacks:** Employees clicking on fraudulent emails or links can give hackers access to sensitive company data and systems.
2. **Weak Password Practices:** Using simple, repeated, or shared passwords increases the risk of unauthorized access to work accounts and systems.
3. **Unsecured Devices:** Laptops, smartphones, or USBs without proper encryption or antivirus expose the network to malware and data theft.
4. **Outdated Software:** Failure to update or patch systems leaves known vulnerabilities that can be exploited by cybercriminals.
5. **Lack of Training:** Employees unaware of digital hygiene or scam recognition are more likely to fall victim to cyber threats.
6. **Remote Work Vulnerabilities:** Home networks and personal devices often lack the same protections as on-site systems, increasing exposure.
7. **Insider Threats:** Disgruntled or negligent employees may intentionally or accidentally compromise security systems or leak confidential data.

STATS

- In Canada, 44% of organizations reported experiencing a cyber attack (attempted or successful) in the last 12 months as of 2024.
- In the US, there were 2,741 publicly disclosed data breaches between November 2023 and April 2024, compromising over 6.8 billion records.
- Business email compromise (BEC) incidents in Canada surged from 15% of total cyber incidents in 2023 to 32% in 2024.
- The industry-wide Phish-prone Percentage stands at 33.1%, meaning one-third of employees are susceptible to phishing and social engineering attacks (2025 benchmark).
- 44% of survey participants in a 2025 study admitted to interacting with a phishing message in the last year.
- Only 34% of small and medium-sized business employees in Canada report receiving mandatory cybersecurity awareness training.
- Statistics Canada reported that cybersecurity incidents affected 18% of Canadian businesses in 2021, with over half experiencing downtime or recovery costs.