CYBER SECURITY BREACHES SURVEY 2021

UK BUSINESS TRENDS

The Cyber Security Breaches Survey is an official statistic. Since 2016, it has measured how UK organisations approach cyber security, and the impact of breaches and attacks. This infographic shows the key findings for UK businesses.

1. **Despite COVID-19, cyber security remains a priority among management boards.** 77% of businesses say that cyber security is a high priority for their directors or senior managers (vs. 69% in 2016).

2. **Phishing is the most commonly identified cyber attack.** Among the 39% identifying any breaches or attacks, 83% had phishing attacks, 27% were impersonated and 13% had malware (including ransomware).

3. **Unprepared staff risk being caught unaware.** A total of 14% of businesses train staff on cyber security and 20% have tested their staff response, for example with mock phishing exercises.

4. **Businesses are adapting to new work patterns that affect cyber security.** Fewer now have firm rules preventing staff from using personal devices for work (64% vs. 69% in 2020).

5. **COVID-19 has made cyber security harder.** With resources stretched, fewer businesses report having up-to-date malware protection (83%, vs. 88% in 2020) and network firewalls (78%, vs. 83% in 2020).

6. **Businesses can better prepare for future uncertainties.** In total, 31% have business continuity plans that mention cyber security and 15% have done an audit of their cyber security vulnerabilities.

For the full results, visit www.gov.uk/government/statistics/cyber-security-breaches-survey-2021.

Technical note: Ipsos MORI carried out a telephone survey of 1,419 businesses (excluding sole traders, and agriculture, forestry and fishing businesses) from 12 October 2020 to 22 January 2021. This included 654 businesses that identified a breach or attack in the last 12 months. Data are weighted to represent UK businesses by size and sector.

For further cyber security guidance for your business, visit the National Cyber Security Centre website (www.ncsc.gov.uk).

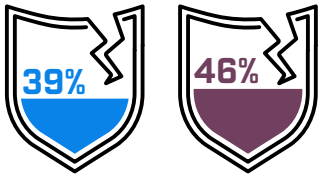
This includes COVID-19 guidance covering:
- **home working**
- **video conferencing**
- **moving your business online.**

Department for Digital, Culture, Media & Sport

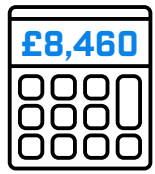
Ipsos MORI

UK BUSINESS TRENDS

EXPERIENCE OF BREACHES OR ATTACKS



of businesses identified cyber security breaches or attacks in the last 12 months **(down from 2020)**



is the average annual cost for businesses that lost data or assets after breaches

AMONG THE 39% IN 2021:

27%
were attacked at least once a week

23%
needed new measures to stop future attacks

DEALING WITH COVID-19

47%
have staff using personal devices for work

18%
cover use of personal devices for work in a cyber security policy

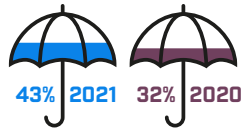
34%
have a VPN for remote working

23%
cover home working in a cyber security policy

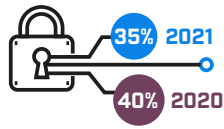
MANAGING RISKS

83%
have up-to-date malware protection **(down from 2020)**

43%
have cyber insurance cover **(up from 2020)**



35%
have used security monitoring tools **(down from 2020)**



34%
have done a cyber risk assessment

32%
monitor user activity **(down from 2020)**