CYBER SECURITY BREACHES SURVEY 2021

UK CHARITY 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 charities, which were first included in the 2018 survey.

1.

Despite COVID-19, cyber security remains a priority for charity boards. 68% of charities say that cyber security is a high priority for their trustees or senior managers (vs. 53% in 2018).

2.

Phishing is the most commonly identified cyber attack. Among the 26% identifying any breaches or attacks, 79% had phishing attacks, 23% were impersonated and 17% had malware (including ransomware).

3.

Unprepared staff risk being caught unaware. A total of 18% of charities train staff on cyber security and 14% have tested their staff response, for example with mock phishing exercises.

4.

COVID-19 has made cyber security harder. With resources stretched, fewer charities report having up-to-date malware protection (69%, vs. 78% in 2020) and network firewalls (57%, vs. 72% in 2020).

5.

There is room for improvement when it comes to suppliers and partners. In total, 8% of charities have reviewed cyber risks posed by their suppliers or partners (e.g. local organisations they work with).

Technical note: Ipsos MORI carried out a telephone survey of 487 UK registered charities from 12 October 2020 to 22 January 2021. This included 183 charities that identified a breach or attack in the last 12 months. Data are weighted to represent UK registered charities by income band and country.

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

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

This includes COVID-19 guidance covering:

- the tailored **Cyber Security Small Charity Guide**
- the **Cyber Essentials scheme** – independent certification for organisations that meet good-practice standards in cyber security
- cyber security under the COVID-19 pandemic, including guidance on **home working**, **video conferencing** and **moving your business online**.

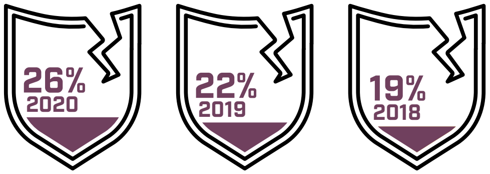
Department for
Digital, Culture,
Media & Sport

Ipsos MORI

UK CHARITY TRENDS

EXPERIENCE OF BREACHES OR ATTACKS

identified cyber security breaches or attacks in the last 12 months



AMONG THE 26% IN 2021:

26%
carried out staff training or comms after a breach

25%
lost staff time dealing with the breach

24%
needed new measures to stop future attacks

23%
were attacked at least once a week

DEALING WITH COVID-19

67%
have staff using personal devices for work

23%
cover use of personal devices for work in a cyber security policy

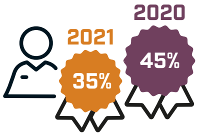
23%
cover home working in a cyber security policy

20%
have a VPN for remote working

27%
have a business continuity plan that covers cyber security

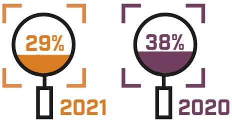
MANAGING RISKS

35%
have trustees or senior managers with a cyber security brief
(down from 2020)



32%
have done a cyber risk assessment

29%
monitor user activity
(down from 2020)



29%
have cyber insurance cover