5 lessons to learn from 2020 security breaches

Capitalising on the disruption resulting from the move to remote working, cybercriminals ‘prospered’ in 2020, with:

20% rise in cyber security threats compared with 2019

80% surge in ransomware attacks in the third quarter.

Covid restrictions are still in place, and a move to a more flexible, hybrid working environment forecast post-pandemic - so greater security vigilance is essential.

5 lessons to learn from 2020:

1 Phishing is increasingly sophisticated

- spear-phishing
- vishing (voice phishing)
- smishing (SMS text phishing)
- angle phishing (targeting ‘bad experience’ customers via social media)

2 Simulate an attack - before it’s too late

- expose your vulnerabilities
- monitor your ability to detect a breach
- measure the response to a breach
- fix the weaknesses

3 Test the integrity of your software

- shake up your testing program
- don’t take the vendor’s word - test yourself
- use robust, manual review techniques
- test, test, and test again

4 Train your staff

- the most efficient way to limit risk
- develop an ongoing training program
- train, train, and train again

5 Don’t just check everything once!

- managing security is a continual process
- build it into your IT calendar
- make it a priority!

Talk to our team to find out more about how to stay secure.

Contact us