7 key cyber security threats for businesses – and how to tackle them

Feature
20 Oct 2020

In partnership with the UK Domain, we round up seven of the most common cyber security threats to businesses and what you can do about them

-
-
-
-
- COMMENT

Cyber security threats cost businesses thousands of pounds a year

Anna Jordan

-

Cyber security breaches are threats to businesses of any size, but more developed businesses risk losing a greater proportion of the growth they've worked so hard to build.

Government statistics from 2020 show that 46 per cent of firms have reported cyber security breaches in the past 12 months. A sizeable 32 per cent said they were experiencing attacks once a week vs 22 per cent in 2017. Worryingly, the attacks are becoming more sophisticated too – 86 per cent of businesses experienced phishing attacks, 26 per cent were impersonated (purporting to be from someone that the victim trusts) and 19 per cent had malware infections.

Businesses lose an average of £3,230 from missing data or assets after breaches and 20 per cent of firms report lost staff time in dealing with the breaches.

From 2010 to 2020, roughly four billion business records were stolen in the UK, according to figures from bulletproof.co.uk.

The good news is that measures can be put in place to prevent disaster for your company. We delve into seven cyber security threats and what you can do to combat them.

1. Malware infections

You may be familiar with malware already. It's short for malicious software and can include ransomware, spyware, viruses and trojans. In a more general sense, malware is classed as an unwanted action to the victim which will benefit the criminal.

Antivirus technology and a reliable firewall are key in fighting these menaces. Spend the time to research trusted antivirus programmes and firewalls and make sure they are kept up to date. Allowing automatic updates is best as bugs can be fixed in the background while you and your staff work.

2. Phishing attacks

Phishing attacks leave staff vulnerable to sensitive data being stolen, often through email. It's one of the most common ways malware is brought into a business.

Spear phishing is when a targeted email comes through which looks like it's from someone that you know.

Emails can contain links which, once clicked, release ransomware into your computer and into the broader network. The idea is that you get your data back by paying a ransom, regularly costing thousands of pounds.

To combat this, businesses should be backing up their data. You can back up data on an external hard drive. Alternatively, some computers have auto back-up features – these will back up your data little and often, which is the best approach to take.

Sarah Lyons, at the National Cyber Security Centre (NCSC), says that companies should be encouraging lines of communication to support staff welfare. So, when employees report phishing emails, they should be able to admit that they clicked on a phishing link without receiving blame for doing so.

"A clear process for reporting suspected phishing emails internally should be carried over from the office into a remote working setting," says Sarah Lyons, deputy director for economy and society engagement at the National Cyber Security Centre (NCSC).

"Staff should be encouraged to forward anything that doesn't look right to the Suspicious Email Reporting Service (SERS) via report@phishing.gov.uk."

3. An inadequate or non-existent BYOD (bring your own device) policy

Unsecured devices could be carrying any number of viruses. That's why it's crucial to have a solid BYOD policy in place. A BYOD policy is a set of rules about how employees' own devices can be used for work – this could be smartphones, tablets, laptops or other devices. It should also outline what responsibilities lie with the employee and what responsibilities lie with the employer, such as repairs.

Coming to the nitty gritty, your policy must ask staff to agree to terms and conditions and state the right for you as the employer to revoke these rights. Remember to include what counts as acceptable use, what the company will and will not pay for in relation to the device, security protocols like passwords and the risks and disclaimers of using your own device.

Having a solid BYOD policy reduces the vulnerabilities associated with staff using their own devices such as data loss. It also sets out what should happen if data security is compromised.

As a quick addendum to this point, we should mention virtual private networks (VPNs). If staff are often working in remote locations like a co-working space or an airport, ensure a virtual private network is used. Without one, hackers could be watching the transfer of sensitive data. If your employees have a VPN, traffic will be transformed into cryptic characters, keeping data safe from criminals.

4. Website weaknesses

Website weaknesses can leave you vulnerable to attacks, like Structure Query Language (SQL) injections.

"A SQL injection is where an attacker adds a Structured Query Language (SQL) code to make changes to a database and gain access to unauthorised resources or make changes to data," says Sarah Lyons.

"Businesses should ensure that they're using the most up-to-date versions of software to protect themselves from this. Previously discovered vulnerabilities may not be patched in older versions of software."

The NCSC recommends looking at its Vulnerability Disclosure Toolkit and its Vulnerability Management guidance.

Additionally, those who haven't changed over to a secure URL yet should really do so. Secure Sockets Layer (SSL) encrypts your web connection and performs similar types of actions to the virtual private network mentioned above. Website visitors will be able to see a keypad on the browser bar, but be warned that these have been replicated by scammers in the past to make a fake site look trustworthy.

If you haven't already, you can get an SSL certificate from your web host. Alternatively, you can get one from Google if you use certain Google or partner products.

5. Insider threats

There's a chance that ex-employees might, knowingly or not, compromise your cyber security, especially if they have access to your networks. Reduce the chances of this happening by having specific accounts for people with privileges and ensuring that you remove employees from your network when they leave the company.

Sarah Lyons advises combatting this by understanding where your data goes and what needs to be protected. This will allow your business to develop ways to detect these behaviours.

"A good insider threat program is built on trust and two-way dialogue between employees and their organisation – and being aware of how attackers could target staff. They may offer them incentives for useful information, approach those facing career uncertainty to carry out specific actions or try to solicit information that would help identity IT security vulnerabilities," she says.

Managers seeking to assist staff can refer to the Centre for the Protection of National Infrastructure's line managers campaign, the 'It's ok to say programme', accompanied by the 'don't take the bait' campaign.

6. General lack of cyber security knowledge and awareness among staff

Education will help safeguard your cyber security strategy. By staying on top of your employee training and keeping updated with technological changes and emerging criminal trends, your business is more likely to be able to detect and recognise potential cyber attacks and threats.

The NCSC has a Top Tips for Staff e-learning package, which can be completed online or built into an existing training platform. It's free, easy to use and takes less than 30 minutes to complete.

"Exercising is one of the most effective ways an organisation can test how it responds to cyber incidents. By practising defence and response mechanisms, organisations can understand how effective they really are and where there are areas for improvement," says Sarah Lyons.

For this, the NCSC recommends its free Exercise in a Box toolkit which provides exercises based around the main cyber threats.

7. Distributed Denial of Service (DDOS) attacks

One area you should know about are Distributed Denial of Service (DDOS) attacks. Hackers will try to make a machine or network inaccessible to its primary users. DDOS attacks result in heavy web traffic which slows down the site and can force services offline. Attacks can last for up to 24 hours. Those whose business offering is predominantly based online are the most vulnerable.

"While the risk of a DDoS attack can never be eliminated, businesses can potentially reduce the severity of an attack by being well prepared," says Sarah Lyons. "Working with service providers to help deal with surges in traffic is important in any response to a DDoS attack."

"Quickly responding to a DDoS attack is key and hinges on having a solid, well understood response plan in place. This should lay out everything from confirming that an attack is happening to monitoring and recovery."

The NCSC provides a basic DDoS attack response plan online for all businesses to use.

Which is the biggest cyber security threat to my business?

Any of these cyber security attacks could be detrimental to your business. And just because they're listed as seven separate attacks, there is plenty of opportunity for overlap. For example, the link contained within a spear phishing email could contain malware.

But there are a number of things you can do to protect your company's cyber security – and you needn't do them all at once.

Whatever measures you decide to take, make sure your staff – be they based at work or remotely – are aware of, and properly trained to deal with, cyber security risks.

You can find more advice at the UK Domain's cyber security section.

This article was brought to you in partnership with the UK Domain.

Read more

5 ways your business can reinforce homeworking cybersecurity

-
-
-
-

Related Topics

- Cybersecurity

Comments (0)

Previous Post Next Post

- **Helping you grow your business is our number one priority, if you would like to take your business to the next step just sign up!**

SIGN UP NOW

-
-

. Recent Articles

Deals of the Week July 26–30 – a GrowthBusiness roundup

30 Jul 2021

Build Back Better #4 – how do I go about selling a business?
28 Jul 2021

Companies raise 121% more in H1 2021 than the same period last year
27 Jul 2021

How to sidestep your bank and find the best exchange rate for bank transfers
26 Jul 2021

Deals of the week July 19 to July 23 – a GrowthBusiness roundup
23 Jul 2021

The Bonhill Network

- Bonhill Group plc
- Information Age
- InvestmentNews
- What Investment
- Small Business
- Growth Business
- Tax Guide
- DiversityQ

Further Information

- Terms & Conditions
- Privacy Policy
- Cookies Policy
- About GrowthBusiness
- About Bonhill Group plc
- Contact us

Bonhill Group plc, 29 Clerkenwell Road, London EC1M 5RN T. 0207 250 7010

Further Information [+]