IT SECURITY

WOULD YOU PASS OR FAIL OUR 57 MINUTE SECURITY CHALLENGE?

STREYM

DON'T MAKE IT EASY FOR HACKERS TO GET IN

It's easy to believe that cyber criminals are not interested in your business, because you're small not a big household name, or have a small team of staff.

Sadly, this isn't true. Cyber criminals don't go after specific targets, they release malware into the wild, seeking out easy targets.

HERE'S HOW EASY IT IS TO BE AFFECTED

It only takes one computer on your network to be a little out of date, to allow bad software to get in

It only takes one member of staff clicking a dodgy link in a spammy email

It only takes one USB stick with Malware to be placed into one of your laptops

Most businesses are a lot more hackable than they realise. And the consequences are huge...

If you are hit with something like Cryptolocker, you can get locked out of your devices and data for days. It takes a lot of time, effort and often cash to get back to business as normal.

HERE'S THE CHALLENGE FOR YOU AND YOUR BUSINESS

We're confident that if we were to visit your business today, we'd find a weakness in your IT system within just 57 minutes

We call this our 57 minute Data Security Challenge. We bet that we can uncover a way to get into your system, or an unsafe working practice.

All we have to do is ask you some questions and have a quick look at your computers, and the systems your staff are using.

You see, cyber criminals are always looking for ways into computer systems, and countless business owners make it really easy for them. Just having anti-virus software in place, even if it's really good, simply isn't enough in 2018.

There are a lot of great anti-virus products out there, but never assume they will protect you from all threats. If cyber attackers really want to find a way in, there are plenty of other options available to them.

It's all about perception. One of the biggest security problems I see every day is the attitude that it's only the bigger companies that are at risk. The fact is, companies of all sizes face exactly the same threats. And cyber attackers particularly love the ones that take a blasé approach to security.

MISCONCEPTIONS OF CYBER SECUTIRY

"Cyber threats are always external."
False! Many data breaches are internal. Some are deliberate and others are unintentional. Most businesses employ staff and give full access to all internal systems, it's easy for data to end up in the wrong hands.

There are also employees who click on infected links or email attachments that put entire networks at risk. Your biggest threat isn't always a lurking, it's the person you work with who makes a mistake, maybe without even realising it.

"Nobody could ever guess my password."
False. Passwords are super easy to figure out. We all know the difficulty of having complicated upper and lower cases and symboled passwords, so this is where a lot of people are lazy. Many pick passwords that mean something to them, like a name or date, and then use them everywhere for everything.

"I'm safe from viruses because I only open emails from people I know."
False. Cyber attackers are clever. They replicate emails and email addresses that are almost identical to the real thing and that can fool even the most eagle-eyed administrator into opening a dodgy attachment.

"It's easy to spot an infected computer."
Not necessarily. Sure, if your screen is full of pop ups and takes half an hour to download a photo, it's probably a good sign that it's sickly. But a lot of viruses and malware can now run completely undetected, sneakily stealing all your critical data without any outward signs of infection.

"Cyber security is an expense I can't afford."
When you're running a business you want to keep costs down. But the fact is, you stand to lose a lot more money if you take chances with your cyber security than if you get the cover your business needs.

When you consider the fact that non-compliance with the new GDPR can mean multi-million pound fines (and carries a thorough risk to your business's reputation), spending a bit of money on protecting your data is actually the smart thing to do. IT security is an investment, not an unnecessary expense.

LET'S LOOK AT SOME STATS

1. In 2017 4/10 of UK businesses had at least 1 hack

2. Over half of small businesses have been targeted

3. 81% of attacks are due to employee negligence or poor password choices

5. The average no. of records taken per attack has risen by 87% from just over 5,000 to 9,350

6. The average cost of a breach is over £1.2m

If these figures are scary enough, here's another one:
Around 87% of small businesses still think they won't be targeted at all

Yup. 87%. You might even be reading this now thinking, "Yeah, but it still won't happen to me. I'll take my chances."

Please don't.

Smaller businesses are different to huge multi-national corporations. But that certainly doesn't make them less attractive to cyber attackers. Quite the opposite.

It makes them positively irresistible.

One of the most important differences is that the big boys usually survive attacks, because they have sufficient resources to fall back on. Small businesses, on the other hand, usually don't.

About half of all small businesses that experience cyber-attacks go bust within the next six months. And the bad guys love that. Bullies pick on weaknesses, after all. If they see you've got minimal security measures in place they'll see it as the perfect opportunity to pick on you.

Perhaps one of the reasons that the average business owner takes the "it won't happen to us" approach is that we usually only hear about the high profile cases in the news. The headlines are full of stories about cyber-attacks, but when the only names we hear are big ones like Facebook, Talk Talk, Netflix, Carphone Warehouse and the NHS it's easy to switch off.

HERE'S A LOOK AT CASES THAT ARE CLOSER TO HOME

These cases were featured in the Daily Telegraph a year ago.

Marcos Steverlynck runs an e-commerce marketplace called Rise Art. The site was subjected to several attacks last year, including a distributed denial of service (DDoS) which deliberately restricted the London based company's access to the internet. For an e-commerce site that's pretty bad news.

Nottingham based plant nutrition firm Micromix was hit by a ransomware attack in May 2016. They're very open about the fact that they took a relaxed approach to cyber security prior to the event, believing they would be of little interest to hackers. Operations manager Charlotte Halls told the Daily Telegraph:

> "We felt it wouldn't happen to us. We're now far more security conscious as we know it's not just the TalkTalks and Tescos of the world that hackers have in their sights."

Auto components manufacturer Talbros fell prey to the Wannacry virus that swept through the NHS in May 2017. The company had security systems in place, but they weren't robust enough to prevent the virus infiltrating their network and accessing their critical data. Head of IT, Rakesh Budhiraja, told the Daily Telegraph:

> "When we tried accessing our data, money was demanded in the form of bitcoins."

To read the full Daily Telegraph story from last year, go to:

www.telegraph.co.uk/connect/small-business/cyber-security/lessons-learnt-smes-cyber-attack-stories/

COMMON WAYS HACKERS GET IN

1 Socially engineered malware

This is the no.1 method of attack at the time of writing. It involves tricking end users into running "Trojan Horse" programs that come from trusted sites.

The website is temporarily compromised, delivering malware that tells the user to install a new piece of software in order to keep using the website. They'll keep being given prompts to click past security warnings and disable defences. Might sound like something you wouldn't get caught out by, but they're surprisingly believable and responsible for millions of hacks yearly.

2 Phishing

Around 70% of all email is spam, and a huge proportion of that spam is phishing attacks created to trick users into handing over important information. The attacker masquerades as a reputable person or organisation, distributing links and attachments that when opened steal login credentials and account details.

3 Out of date software

If your software is past its sell by date and missing out on the latest patches and updates, you're gambling with your IT security. Technology has a way of becoming damaged in ways that aren't obvious. Cyber criminals, however, can easily spot flaws in software and use them as a way into your network.

4 Social media

Social media is brilliant. It connects us with people from all over the world, opening up whole new commercial opportunities that would have never been possible even 20 years ago. But it's not without its problems. Corporate hackers are always on the lookout for new ways to hack into your Facebook, Twitter or LinkedIn accounts and steal your contacts. Or identity.

5 Mobile apps

A lot of people think that if an app is available through Google Play store or Apple it's got to be safe. Sadly, that's not always the case and many apps contain malicious codes that can steal your data and compromise users' privacy. If your staff are using their own devices for work, there's potential for a data disaster.

Seems a bit more real now, doesn't it?

BACK TO THE BEGINNING...

So, back to my original question: Would your business pass my 57 minute Data Security Challenge? Let's find out!

When it comes to cyber security, you simply cannot afford to take risks and short cuts. A proactive, pre-emptive approach is what's needed, and it doesn't have to cost a fortune.

Streym Ltd
18 Soho Square
London
W1D 3QL

+44 (0) 845 2301 420
info@streym.com
www.streym.com

STREYM