IT SECURITY

EMAIL FRAUD - YOU & YOUR TEAM ARE BEING TARGETED

STREYM

EMAIL SECURITY IS YOUR NEW BUSINESS HEADACHE

We used to do all our business face to face or over the phone. Thanks to the internet we can now communicate with 100s of people every day from the comfort of our desks, just by pressing a few buttons.

We send over 205 billion emails every day, and it's predicted to rise to 246 billion by 2020. But that productivity comes at a risk. Emails can be hacked.

Cyber-crime is always in headlines and new threats pop up every day. In 2014, 60% of email traffic was spam, and that's a big problem for businesses.

You may think, "We've got anti-spam and anti-virus software, we don't need to worry, right?"

Wrong.

Anti-virus and anti-spam solutions are no longer sufficient. Criminal organisations are now preying on businesses of all sizes and will find their way in.

We've all seen the messages from a prince who has found themselves in hardship or emails with dodgy links, and we know they're important to avoid. But as well as phishing scams countless other email hacks will slip through the cracks and end up costing businesses millions.

Scammers are so clever that they can create impostor emails that look so much like the real thing that they can fool even the most savvy business person.

That's another important point. Scammers are business people. Today's hacker is looking for options that deliver high profits for minimum investments.

AN OPEN INVITATION - BUSINESS EMAIL COMMERCE

Also known as CEO Fraud, this is a relatively new type of scam that brings fast results and can be highly lucrative if your defenses are down.

Instead of wasting time sending phishing emails to random email addresses, cyber criminals are now doing their research to get to the goodies more quickly. They use social engineering tools to carefully select their next targets, impersonating key staff members or trusted partners to trick their victims into transferring funds online.

Hackers use tried and tested tricks that are highly successful. They look genuine and encouraging their victims to act quickly and without a thought for verification. Here are just some of them:

- Creating email addresses using domains that look very similar to the real thing
- Using urgent tones: "Needs to be done ASAP"
- Stating that the CEO is in a meeting and can't be disturbed
- Using a well-known line such as "sent from my iPhone", implying the sender is away
- Using legitimate looking account details, obtained from their social engineering tools

You may well be reading this thinking you'd never be so gullible as to fall for such a scam. But can you be sure your team would be so savvy?

How about when it's almost clocking off time, they're tired, and "The Boss" emails them asking to transfer a small amount of money into a "client" account?

What if there's nobody else around to ask and they don't want to let the boss down or annoy them, especially when the email clearly states that they mustn't be disturbed?

Hackers rely on "fear of management" psychology. They know that people want to be seen to be efficient and are unlikely to refuse to do something when specifically asked by their boss.

In terms of who they target, the most common victims are senior finance officers (because they're more likely to have instant access to bank accounts and the authority to use them), closely followed by HR.

Small and medium sized companies are particularly attractive to cyber criminals because they typically have fewer defence mechanisms in place. Hackers don't stick to just one type of business. Their victims come from all sorts of organisations, from small businesses, to large corporations.

If you've got 100 employees all sending 100 emails every day, that's already 10,000 messages full of data criminals would love to get hold of. With the new GDPR regulations just around the corner the implications of not properly looking after customer data are so major that it could be impossible to recover from.

Unwanted emails don't just affect productivity. You're now looking at huge financial losses, legal action, furious customers and irreparable brand damage.

To reduce email risk you'll need a bulletproof strategy that addresses the full spectrum of threats caused by both incoming and outgoing emails. There are multiple ways to keep your accounts secure.

BE VIGILANT

Unfortunately we now live in a world where complacency is dangerous. It's important to keep your wits about you. If anything looks even slightly suspicious, don't touch it.

Of course, there's only so much you can do yourself and there are only so many pairs of eyes in your staff team to keep peeled. 24/7 monitoring is the best way to stay safe from attack. Carefully developed software that looks out for unusual and unauthorised emails will be more effective than humans scanning for issues.

EDUCATE YOUR TEAM

It's essential that everyone is trained on email security and knows how to spot suspicious emails. Teach them to always question messages that ask them to act fast, especially if they mention anything to do with money.

Make it a requirement that employees use strong passwords and change them regularly. It's a pain but it's a lot better than being hacked. Also, never share passwords.

KEEP IT ON LOCKDOWN

Email encryption is one of the most reliable ways to protect your email content. It works by disguising the content of email messages to make them less attractive to unauthorised users.

If hackers gain unauthorised access through routes, other than email, they are also able to find their way into your systems and can hijack entire email accounts. Encryption means that if someone does gain access, they won't be able to read any of the content without the correct security.

UPDATE YOUR POLICIES

Having two-factor or multi-level authentication policies for wire transfers can stop Business Email Commerce attack, and it's wise to insist that any payments are confirmed verbally by you first. Strong BYOD (Bring Your Own Device) and data protection policies are also essential for reducing the risk of data breaches.

Recent news stories suggest that even some government officials took a somewhat lax approach to email security. Speaking in his defence, fellow MP Nadine Dorries took to Twitter to claim that it was entirely plausible for Damien Green's PC to have been hacked because she often shares her login details!!

Sensible employees should all take a zero tolerance approach to sharing passwords.

Likewise, never write them down and leave them on display. It's astonishing how many computers have notes displaying passwords stuck to their screens.

A password is there for a reason. And if it's there for all to see it's utterly pointless having one. Make sure your employees know exactly what's expected of them and you'll be less likely to end up with a data breach on your hands.

INVEST IN ROBUST EMAIL SECURITY PROTECTION

Protect your people, data and brand from common threats like phishing, impostor emails, malware, spam and bulk mail. The more layers of protection you have, the safer you'll be.

Robust email security software will analyse domain reputations, email content, headers and signatures and sender-recipient relationships to identify scams before they can reach your end users or do any damage.

Email filtering can help you control of all inbound and outbound communications. It quarantines spam, phishing emails and adult content, as well as helping you to prioritise the messages in your inbox.

Prevention is always better than cure, and with so many threats to your company's security appearing on an almost daily basis email security is something you simply can't afford not to take seriously.

Streym Ltd
18 Soho Square
London
W1D 3QL

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

STREYM