5 steps
to better email security

Do you realise you and your team are being targeted by email fraudsters?

Email security is your business's new headache. They are targeting MDs, CEOs and other senior staff.

Watch our video **here**

How they do it and how you can minimise the risks

Cyber-crime is rarely out of the headlines now and new threats are popping up every day. In 2014, two thirds of all email traffic was spam, and that's a big problem for small and medium sized businesses. "No big deal", you might think, "We've got anti-spam and anti-virus software so we don't have to worry, right?"
Wrong.

The threat landscape has changed so much over the past couple of years that it's no longer sufficient just to invest in anti-virus and anti-spam solutions to keep your network safe. Criminal organisations are now preying on businesses of all sizes and will use all sorts of methods to find their way in.

Scammers are so clever now that they can create impostor emails that look so much like the real thing that they can fool even the savviest business person into handing over important information without even realising it.

Business Email Commerce (BEC) gives them exactly that. Also known as CEO Fraud, this is a relatively new type of scam that brings fast results and can be highly lucrative if your defences are down.

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 every single member of your team would be so savvy?

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. 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?

If you've got 100 employees all sending 100 emails every day, that's already 10,000 messages full of potentially juicy information that cyber criminals would love to get hold of.

Data breaches have always been damaging, but 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 any more. You're now looking at huge financial losses, legal action, furious customers and irreparable brand damage.

5 steps to better email security

DRAGON

In order to truly 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 email accounts secure, such as:

Be vigilant

Unfortunately, we now live in a world where complacency is dangerous. Just like it would be a bad move to take a walk at midnight through an unlit street in a high crime area, 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 always be more effective than humans scanning for potential issues.

Educate your team

It's essential that everyone with computer access 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 that can't be easily guessed and are changed regularly. Yes, it's a pain having to use special characters and numbers and keep updating your password once a month, but it's a lot better than using "1234" and being hacked. And never, ever share passwords (more about that in a minute). Read more on password security here.

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.

It's not just emails that include sensitive information like bank account numbers and login credentials that need to be encrypted either. If hackers are able to gain unauthorised access through other routes, they are also able to find their way into your systems and even totally hijack entire email accounts. Encryption means that even if someone does gain access, they won't be able to read any of the content without the correct security.

Two handy ways to lockdown your email server is to use DMARC and DKIM technology, which does not involve any cost apart from implementation.

Update your policies

Having two-factor or multi-level authentication policies for wire transfers can stop Business Email Commerce attacks in their tracks, 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.

A lax approach to passwords is unacceptable; never write them down and leave them on display. It's amazing how many computer monitors 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 help you control of all inbound and outbound communications. It quarantines spam, phishing emails and adult content, and help 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.

Dragon IS, 6 Bassett Court, Newport Pagnell, Milton Keynes, MK16 0JN
T · +44 (0)330 363 0055
W · www.dragon-is.com