secon
cyber

SECON CYBER
White Paper.

Email Security: Protecting critical communication

CONTENTS

ABOUT US

Established in 1999 we have long standing experience of providing class leading cyber security solutions to customers ranging from small to large enterprises. Our expertise lies in our deep understanding of the cyber security market and unique position in bringing some of the best of breed products and services to provide a fit for purpose and value for money security solution.

EXECUTIVE SUMMARY

Email is the business critical application. Every day your employees are connecting with customers and each other and if this line of communication goes down, your business can come to a standstill. If you're in need of a security strategy, email is a good place to start.

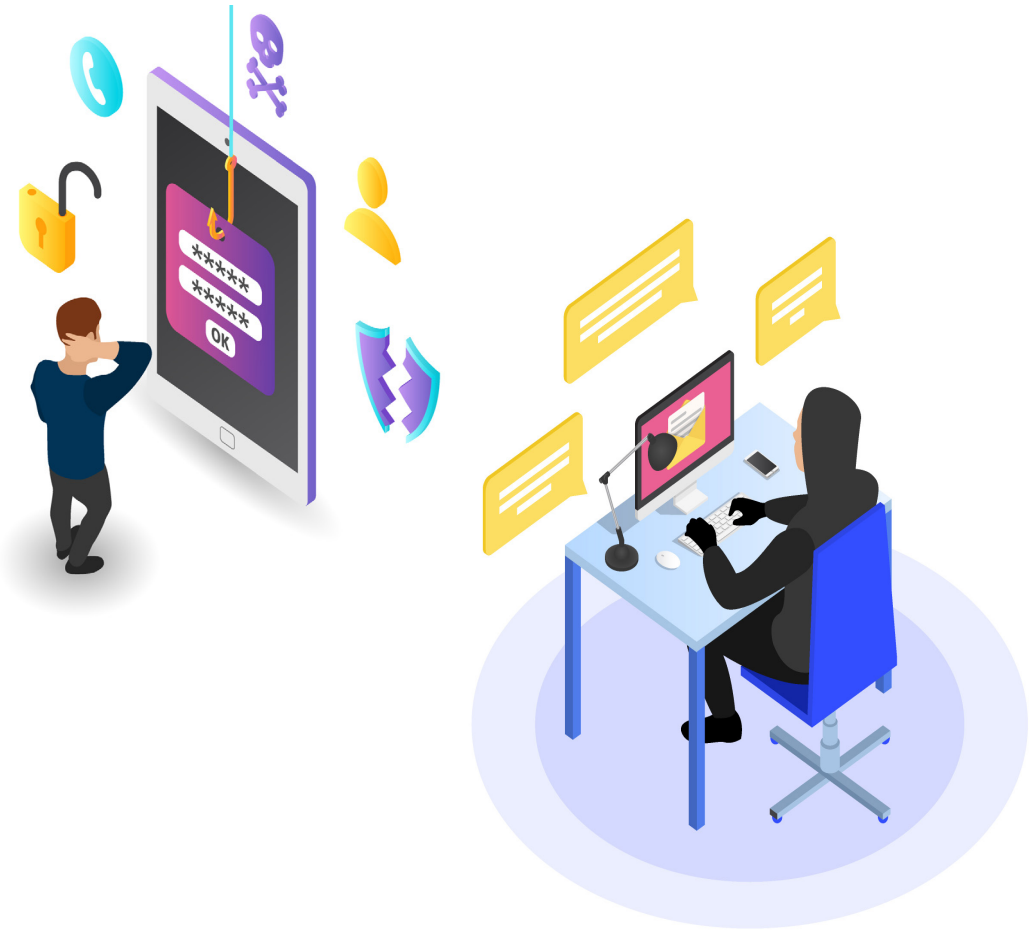
Bad actors have been targeting email for a long time because it's a cheap and effective way to exploit potential victims. In fact, it is estimated that around 90% of threats begin with an email. To ensure your email is working smoothly and you're protected from threats, you need to put a number of measures in place, including both email security solutions and a programme of user education.

WHY IS EMAIL SO EASY TO EXPLOIT?

Email is a huge target for bad actors for two reasons. The first is because everyone has an email address and thus there are billions of potential targets. It's extremely easy for attackers to either purchase a list of email addresses or work out the emails of everyone in an organisation.

The second reason is the cost of conducting malicious email campaigns is essentially nothing. If a bad actor has a list of 10 million people and sends out a spam email containing a link to a product, they only need one person to buy the product in order to make a profit.

The pull of these two factors help explain why spam is so prevalent. In fact, the average daily volume of legitimate emails for March 2019 was 50.97 billion while the daily spam volume was 295.67 billion. With legitimate emails making up a measly 14.81%, spam is constantly being sent to your users, and not all of it is harmless.



HOW DO THREATS DISGUISE THEMSELVES?

Phishing is one of the most common methods attackers will use to obtain credentials. Seemingly harmless emails could be harbouring malicious links that can download malware. Another frequent trick is duping users into entering confidential details into a page that looks like it's from their bank or IT department. Bad actors put a lot of effort into making phishing emails look as real as possible so users need to be on the lookout for any signs they might be harmful.

As url reputation solutions came into place, bad actors found workarounds to continue sending out dangerous links. A common attack you'll see today is an email will be sent out with a legitimate link on Sunday night, so url reputation will deliver it to a user's mailbox. Then on Monday morning, the attacker will compromise the site and send anyone who clicks to a malicious page.

More and more organisations are also being caught out by whaling, which is simply tricking people into thinking they're communicating with someone else. One of the most common examples used is spoofing an email from the CEO to the CFO asking them to make a payment. Users are quick to reply to trusted colleagues so this can easily catch people out and lead to dangerous situations.

How do bad actors impersonate trusted contacts? Usually one letter of a domain will be changed so at a quick glance the email will look identical to the trusted one. To a standard user who hasn't been trained to look out for these kind of attacks, these emails appear genuine.

TELLTALE SIGNS OF MALICIOUS EMAILS

- One or two changed letters in a domain name
- Many misspelled words or other noticeable errors
- A sense of urgency that encourages you to quickly log in, send money or click a link
- An email from a bank asking for your personal details (most banks explicitly state they will never ask for these in an email)
- Spammy words like 'free of charge' or 'discount'

THE IMPORTANCE OF USER EDUCATION

One of the best things an organisation can do to protect themselves is educate their users on how to spot malicious emails. It only takes one person to click on the wrong email to cause trouble. There are many tools out there, including Trend Micro's Phish Insight which can be found on Secon Cyber's website, which can run simulated phishing tests to discover how prone your users are to phishing attacks.

Typically, when an organisation uses one of these tools for the first time, they see a 40-50% click rate if there hasn't been any prior user awareness. Since it takes just one person to click a link in an email to expose your organisation, having half of your users click is quite dangerous.

We recommend running these tests fairly regularly and over time, the click rate will start to go down. Unfortunately, it's difficult to find a company who has a perfect click rate. Thankfully, a by-product of this process is users will begin reporting genuine phishing attacks to IT since they're eager to prove they've passed a test.

WHAT SOLUTIONS ARE AVAILABLE?

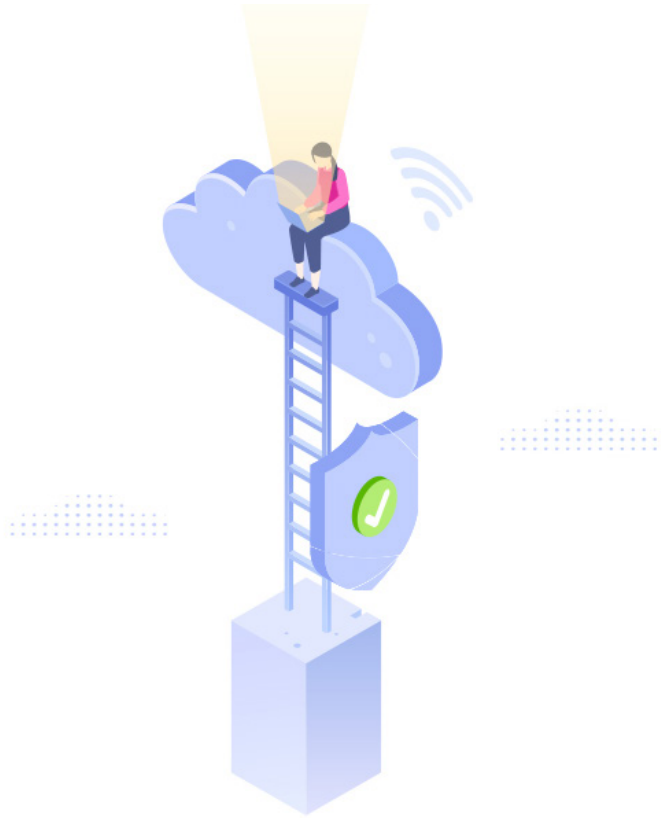
Although user awareness is extremely important, you don't want to place all your trust in your users. Since 90% of threats originate in an email, you need to ensure you're enabling all possible security capabilities to protect your organisation and minimise your reliance on user decision making.

Today's email security solutions include url reputation, antivirus, sandboxing, and email filtering to help protect users from attacks. Many of these elements operate similarly to components of endpoint security. For example, the sandbox will open up the email to see if anything bad executes and then stop the email from delivering if something malicious is detected.

Email security solutions can also incorporate url sandboxing, or url rewriting, which opens up a link in a sandbox as soon as it's clicked to check whether the target page is currently safe.

If you use an on premise solution for your email (such as Microsoft Exchange Server), you also need to be wary of what you're downloading. Around 85% of all email sent is spam and if you're paying to download all your email over your internet connection, you're wasting money as well as making your internal systems work harder to filter this large volume of emails.

When you move your email to the cloud, this no longer becomes an issue and all spam, bad content, malware, and threats like phishing and whaling are dealt with in the cloud so it never can get close to your endpoints. Also, cloud providers automatically update your email tool for you, which ensures you are always up to date to stay on top of threats.



Other than protecting against spam, you can employ other methods to protect your email communications. If you need to ensure your email conversation is private, there are email encryption solutions which can encrypt the email from the sender to the receiver. This can be done at a domain level or on an individual basis. Most emails are sent in plain text, but if your organisation needs to email confidential information or requires regulatory compliance, email encryption may be necessary to secure your conversations.

Also, there are tools that enable you to send encrypted emails even if the recipient doesn't have an encryption agent. In this case, a link will be sent to verify the recipient is correct and then the recipient can download the content via a web portal. Additionally, if there are certain people or organisations you always need a secure connection with, there are options to encrypt all communications so you are not relying on a user to press the encrypt button every time a message is sent to one of these groups.

Email security can also help protect personal information to ensure you are GDPR compliant and prevent sensitive data from leaking. Also, depending on what sector you're in, there may be a legal requirement to retain emails for a certain period of time. If this applies to your organisation, you need to be able to prove the solution you have can't be tampered with, i.e. emails can't be deleted or manipulated once they are archived. Our solutions are secure enough to be admissible as evidence in court so you can concretely prove your emails have not been tampered with.

Content filtering on email solutions can also ensure you're not held legally liable for offending an employee. Most content filtering solutions use dictionaries and lexical analysis to identify harmful words and determine whether they are offensive within the context of the message. If a message is found to be expletive or against any of your set policies on acceptable language, the solution stops the email from being delivered.

In addition, content filtering can be used more cleverly to identify other phrases that are specific to confidential information. For example, if you have an internal project which only a few people in the business are privy to, you can block everyone but this group from receiving emails that contain the name of the project. With features such as this, you can be very granular with what comes in and out of your organisation.

WHAT DOES IT LOOK LIKE IN THE REAL WORLD?

Secon Cyber helped to deploy an email security solution in one organisation, but they did not take the proper steps to educate their employees. In one specific example, this organisation enabled users to manage their own spam folders so they could double check whether the emails marked as spam really were non-legitimate.

One user went to their spam quarantine and saw an email addressed to the finance department which seemingly contained an invoice. This user was not in finance and thought they were doing the right thing by removing the email from the quarantine folder and forwarding it along to the accounts department. Since the email now came from a trusted employee, someone in the accounts department opened it and clicked the link, which automatically downloaded malware.

Although the organisation had put security measures in place, a user was still able to cause a security breach. Security solutions can do a lot of the work for you by screening emails for malware and explicit content, but ultimately user education needs to be put into place to firmly stop attackers from breaching your organisation.

secon cyber

WORK PLAY LIVE

COMPANY ADDRESS

Hersham Place Technology Park
41-61 Molesey Road
Hersham
KT12 4RZ

PHONE

Phone: +44 (0)845 567 8777
Support: +44 (0)845 567 8666

ONLINE

Email: hello@seconcyber.com
Website: www.seconcyber.com

@seconcyber