EMAIL SECURITY

Email is vital to businesses; it's an efficient and effective way to transmit all kinds of electronic data.

Due to the nature of it being a vital aspect of any business, email is also vulnerable to criminal enterprises who would exploit this through phishing, invoice-related scams, copied or spoofed email addresses, malware attacks and more. Most email accounts related to your business will also hold your company's most important email contacts.

As such, having a high level of security for your email accounts is important.

The majority of external email-related cyber attacks come in the form of what is referred to as a 'malicious' email. This is an email that appears to be from a legitimate sender but is in fact not.

The consequences of falling victim to an email-related cyber attack could have high levels of both financial and reputational impact and so it is key that your business has a robust strategy in place to deal with these potential attacks and improve your business's cyber security.

There are several measures that can be taken that will help to reduce the risk of malicious emails getting through within your organisation or that could minimise the impact if anyone does click on them / the links within.

MEASURES TO PUT IN PLACE

SPAM & Attachment Filters

The majority of email platforms and providers include filters designed to block potentially malicious content. Ensuring these filters are turned on is the minimum that your business should do.

Backup

Malware is a type of software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. It is often found within links or attachments in malicious emails and if it gets past your cyber security systems then the consequences can be of enormous negative impact.

Unfortunately, with malware the consequences can often be irreversible; data can be deleted, or damaged. As such, keeping regular backups of data stored within email systems and accounts will provide you with the option of restoration after a malware attack, ie: delete / clear the malware infection on any affected devices, systems and networks before then restoring from a recent backup.

It is possible to set up automatic backups. It is also a good idea to ensure that some of the backups are stored outside of the networks you work within to ensure the backups too cannot be affected by any malware, etc.

Separation

Following on from the Backup section above, separation of systems that could be vulnerable to email-related attacks can help ensure further cyber security.

For example, keeping CRM systems, or financial information systems, etc. on separate networks ensures that if an email-related security breach does occur, it won't affect these crucial systems.

Encryption

The majority of major email platforms will offer encryption on outbound emails, often by default. Ensuring that this feature is turned on with your emails can ensure that unauthorised access or modification of your emails isn't possible.

Update Browser Security

Ensuring your browser is up to date with the latest updates will ensure its security levels are as high as they can be; a large amount of updates to browsers are specifically related to security measures. If possible, set updates to occur automatically to remove user responsibility (or forgetfulness).

Additional security measures you can take with regards to your browsers would include use of an ad blocker and turning off features such as Flash and Java; both of which are often used by malware.

Anti-Virus & Anti-Malware

Most modern anti-virus and anti-malware systems can detect virus and malware attacks - sometimes before they've even been reported. Ensuring your anti-virus/malware systems are up to date across all devices upon which emails are accessed is key to help you preventing attacks.

As with browser security, where possible it is recommended that you set updates to occur automatically.

Phishing Training

Phishing is the term used when attackers attempt to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware, or direct them to a dodgy website.

Phishing is used by cyber criminals to trick email recipients into revealing valuable personal details such as usernames and passwords.

Often this will take the form of links that direct a user to a fraudulent website where passwords, logins or personal details will be requested. These websites have become harder to spot with many being legitimate in appearance.

Training people within your organisation that receive emails as part of their daily work on phishing and its dangers is a preventative measure that is key to helping you avoid phishing attacks. The National Cyber Security Centre provides useful information on dealing with suspicious emails; how to spot the most obvious signs of a scam, and what to do if you've already responded.

Two-Step Verification

Two-step verification (sometimes referred to as two-factor authentication) adds an extra layer of security to your account(s) in case your password is stolen. Once set up, two-step verification will mean that you will sign in to your account(s) in two steps using:

- Something you know (like your password)
- Something you have (like your phone)

Two step verification requires users to enter a second code that would usually be generated via an app on their phone or sent via text message to then login from somewhere new, or after a certain time period.

The benefit of this extra security measure is that if a malicious email link is clicked and a user does reveal their password(s), etc. then the criminal or malware won't be able to access the accounts without the additional code - which is directly linked to the users device (phone, etc.).

Domain-based Message Authentication, Reporting & Conformance

Domain-based Message Authentication, Reporting & Conformance (DMARC) is an email authentication protocol that helps protect email senders and recipients from spam, spoofing, and phishing. This will help you to protect your customers, clients, etc. as it allows the emails that you send to them to be verified as coming from you.

Many email system providers (such as Google and Microsoft) will have options available for DMARC that you and your business can utilise.

FURTHER INFORMATION

The above list is not an exhaustive list but should be considered as essential steps in helping you to ensure high levels of email-related cyber security. Each email provider will have their own unique security features that we would recommend researching and implementing where possible.

More information on email security can be found in the links in our Useful Links section below.

USEFUL LINKS:

- National Cyber Security Centre - Dealing With Suspicious Emails And Text Messages: https://www.ncsc.gov.uk/guidance/suspicious-email-actions
- National Cyber Security Centre - Phishing Attacks: Defending Your Organisation: https://www.ncsc.gov.uk/guidance/phishing
- National Cyber Security Centre - Mail Check: https://www.ncsc.gov.uk/information/mailcheck

Save trees, save paper. Please consider the environment before printing this document.

BETTER BUSINESS NETWORK