EMAIL PROTECTION 101

Email is the most critical communication tool for your business. Communicating via email is fast and easy, just like using a phone, but also leaves a legal trail of evidence that brings accountability to any communication. Unfortunately, when it comes to cybercrime, email is also one of the most commonly targeted elements. Emails have the potential to serve as an easy, backdoor entry for cybercriminals into your organization's IT systems. The Verizon Data Breach Investigations report states that emails were the primary source of two-thirds of malware. [1]Email is an easy target simply because there is more human touch involved in emailing. There's always a stray chance that someone might end up clicking on a phishing link or downloading the wrong attachment or simply including sensitive, confidential information that might be hacked. It's imperative that you deploy reliable security solutions for your email due to the critical role email has in your business environment. This whitepaper discusses how you can keep your email system clean and safe.

Train your employees

As discussed at the beginning of this whitepaper, emails are a soft target because of the human element involved. The first step to securing your email systems is training your employees. Train your employees to identify harmful email messages and to be aware of your firm's IT protocols and rules. There are 4 major ways in which your employees may end up compromising your email security.

- **Falling for phishing scams:**

  These emails will appear to have come from an authentic source and urge the reader to take an action. Usually, the action involves clicking on a link and/or sharing sensitive information via an online form that looks authentic. The phishing links and the webpage clone the original site so well that it is easy to mistake them for their authentic

[1] *https://www.dqindia.com/five-tips-corporate-users-ensure-email-security/*

counterparts. For example, an email that looks as if it is from the IRS, asking for sensitive financial data, or an email that seems to be from the bank asking you to log into your account.

Mistaking hacked emails as authentic ones:

These emails are actually from an authentic sender account, but their account may have been hacked. One of the ways to spot such email messages is if 'something feels amiss.' For example, an email that's ridden with typos, spelling and grammar errors, or if the writing style is different, or an unexplained instruction to download an attachment, fill a form or run a patch, etc.

Not following strict password hygiene:

There are 2 risks here. First is password sharing. Sharing passwords puts your email systems at risk. Often, people trust their coworkers and end up sharing system or email passwords without realizing the possible consequences. Sometimes, it is just so much easier to share the password than follow the protocol. For example, Bob from sales is too busy to prepare his commission report so he gives his password to Lisa from accounting so she can calculate his commission for the month and Lisa shares with her team so they can work on the reports. See! Before you know it, three other people apart from Bob have access to his system including his emails!

The second issue in password hygiene pertains to ignoring password basics. For example, having passwords that are too simple or obvious such as dictionary words, names, etc. or not changing passwords as recommended or having the same password for multiple accounts.

Exposing their own devices to safety threats and then using them for work purposes due to the BYOD environment:

This is a threat brought into picture due to the flexibility-oriented culture of the modern workplace. Businesses allow their employees to work from anywhere, using their own devices. For example, someone could be accessing and replying to an email from work, using their phone or iPad, connected to the open wi-fi at the mall's food court. The risk such open networks bring to the table is unimaginable.

You can organize classroom training sessions to educate your employees about your IT usage policies related to password management, use of personal devices, data sharing and internet access. You can also conduct IT drills and workshops to help your employees identify possible IT security threats and steer clear of those.

Another aspect of email security is, of course, deploying a suitable email security solution. But, with so many available in the market, what should you be looking for when opting for an email security tool? Here are some key features you would want in your email security solution.

Encryption:

Let's start with the worst-case scenario. Your corporate email server is hacked. By opting for an email security solution that offers data encryption, you can ensure that the thieves are never really able to read the data they stole. Data encryption is basically the coding of data in a different format when it is sent and decoding it once it reaches the recipient. Without decryption keys, no one in the middle would be able to make sense of the data they access.

Ditch the server-based email system:

In server-based email systems–the kind supported by most older versions of email software (Outlook, Thunderbird, etc.)–– emails are stored on servers and transmitted every time the email software establishes a connection with them. The newer, web-based systems offer additional security.

Strong filters:

Make sure your email security tool has strong filtering capabilities to keep spam and malicious emails out of your inbox. Training employees to identify spam and fraudulent emails is good, but getting an email security software that keeps most of them away is even better!

[2] *https://biztechmagazine.com/article/2018/03/4-tactics-to-enhance-your-businesss-email-security*

- **Intelligence:**

  When looking for email security software, consider artificial intelligence. According to Biztech, a leading business technology news magazine, newer anti-malware **relies less on signatures of known malicious content and instead uses threat intelligence, reputation services, and other near-real-time sources to pinpoint the location of threats** — domains and IP and email addresses, for example, to alert IT teams. [2]Cybercriminals are getting smarter by the day, and, always innovating, looking for ways to get around the anti-malware existing in the market. You need an email security solution that can keep up with them.

Apart from the above, be sure your emails are always backed up, archived, and stored safely. After all, email is your core communication tool, has legal value, and must be accessible at all times.

Another angle to look into is--how to protect your email system from internal threats, like the malicious intent of your own employees. There is the possibility that somebody who works for you could choose to corrupt your email system on purpose. You can avoid such instances from happening by continually monitoring your employee's IT behavior. You can do this by installing software programs that work to track employee access and activities related to access and sends alerts in case of unusual IT behavior. Examples of unusual IT behavior includes employees logging into work email at a time of day they are not expected to, sending attachments to email addresses that are outside of your organizational network, etc. Also,invest in CCTV cameras and biometric access if you can. That can help serve as a deterrent to malicious employees.

Any breach of your email system is much more than that. An email hack has the potential to translate into data leakage, compromise sensitive vendor and client data, or install malware that can paralyze your business functions entirely. If you don't have the time to look into the security of your email system, consider seeking assistance from an MSP. They will be able to review your business requirements and suggest the right email security tool for you. They can also help you draft a sound IT policy if you don't already have one and also conduct employee training and drills from the security perspective.

SAFE PC SOLUTIONS

For more information please contact,
Madinah Ali
President
SafePC Solutions
P: 1-404-631-6620
msali@safepcsolutionsusa.com
http://www.safepcsolutionsusa.com
1100 Peachtree Street, Suite 200 NE, Atlanta, Georgia, 30309