Email Security Practices You Should Follow

Emails have become an integral part of our lives, serving as one of the primary channels through which we exchange information and interact with others. While it is a wonderful resource for staying connected with coworkers, vendors, and clients, emails are frequently targeted by cybercriminals for malicious purposes.

From phishing attempts and scams to identity theft and social engineering - every dangerous malware can easily proliferate using these platforms. As email continues to be a critical tool for communication and a top target for cybercriminals, you'll need to ramp up your security practices.

Use these email security best practices to keep your network safe.

Train Employees About Safe Usage

We all make mistakes. But in today's hyperconnected world, it is all too easy for employees to accidentally click on a malicious email and expose the company's network to threats. In fact, lack of security awareness is responsible for 20% of cyberattacks, according to a security survey by EY Global.

Something as simple as downloading the wrong file or clicking on the wrong link could wreck havoc.

Make sure that all parts of your defense - including your employees - are well trained. Security awareness training should be mandatory for your employees, especially if they work from home. It is recommended to keep updating new security information. This is an essential step in protecting your business from phishing attacks.

Set Up Email Security Monitoring Tools

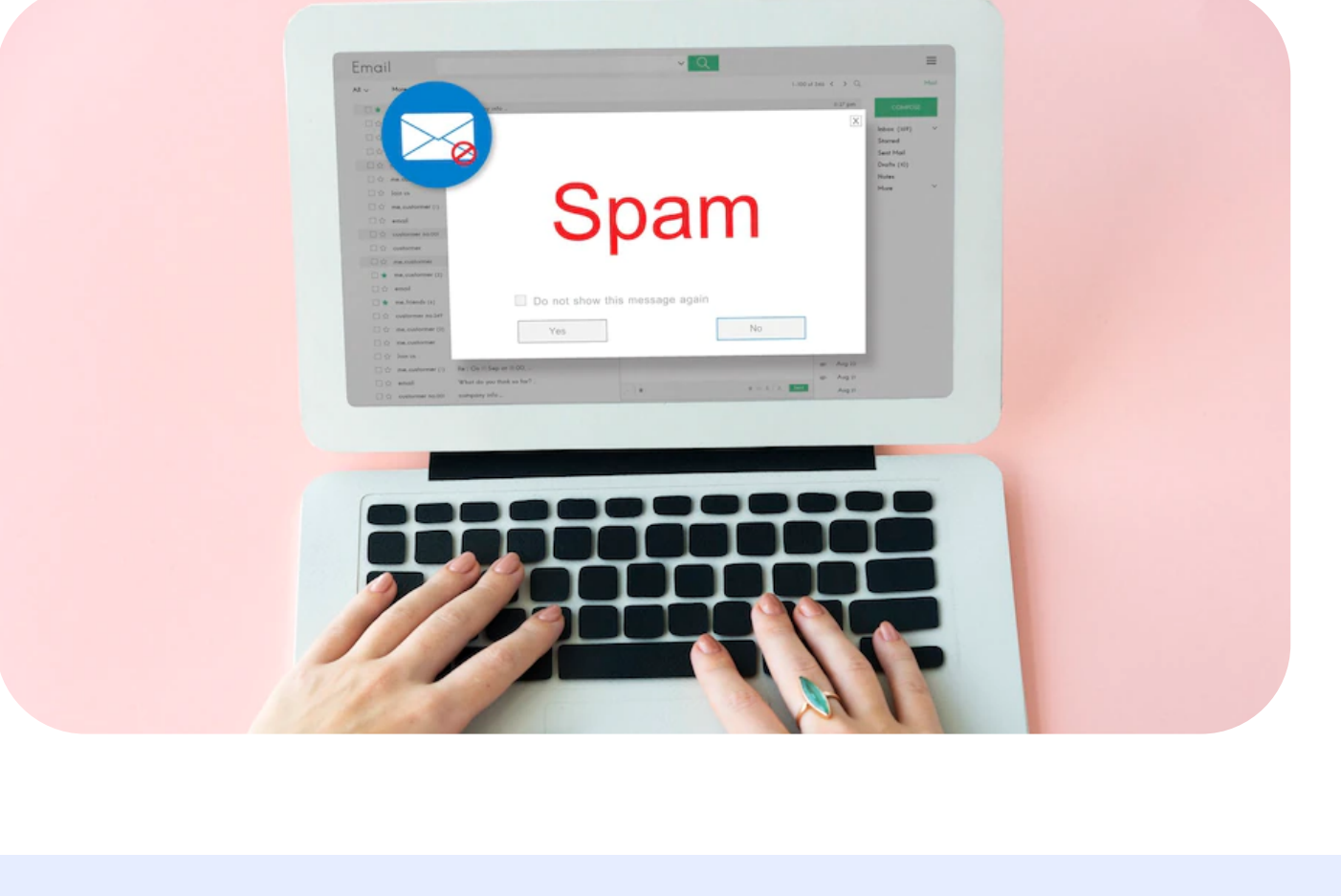
Gain direct access to your emails by installing a monitoring tool. Email monitoring software has evolved to match the growing aggressiveness of cybersecurity threats, and there are many sophisticated protection systems on the market.

Bonus points if the system can also detect phishing and impersonation attempts. It should be able to root out malicious links, spoofing, spam, and malware. You can get a free trial with most systems to see if they align with your workflows.

Use an Email Filter

Most email providers come with built-in spam filters. These tools use AI and machine learning to detect phishing attacks. They can also separate legitimate emails from malicious ones by sending them into your spam folder. Another advantage of using email filters is that they keep your inbox free of clutter.

Although an email filter won't stop every malicious message, it is worth adding to your security arsenal.



Use Strong Passwords

The first piece of the puzzle in figuring out email security is to set up unique passwords. This means the password should not be used on any other account. They should not be used by anyone else either.

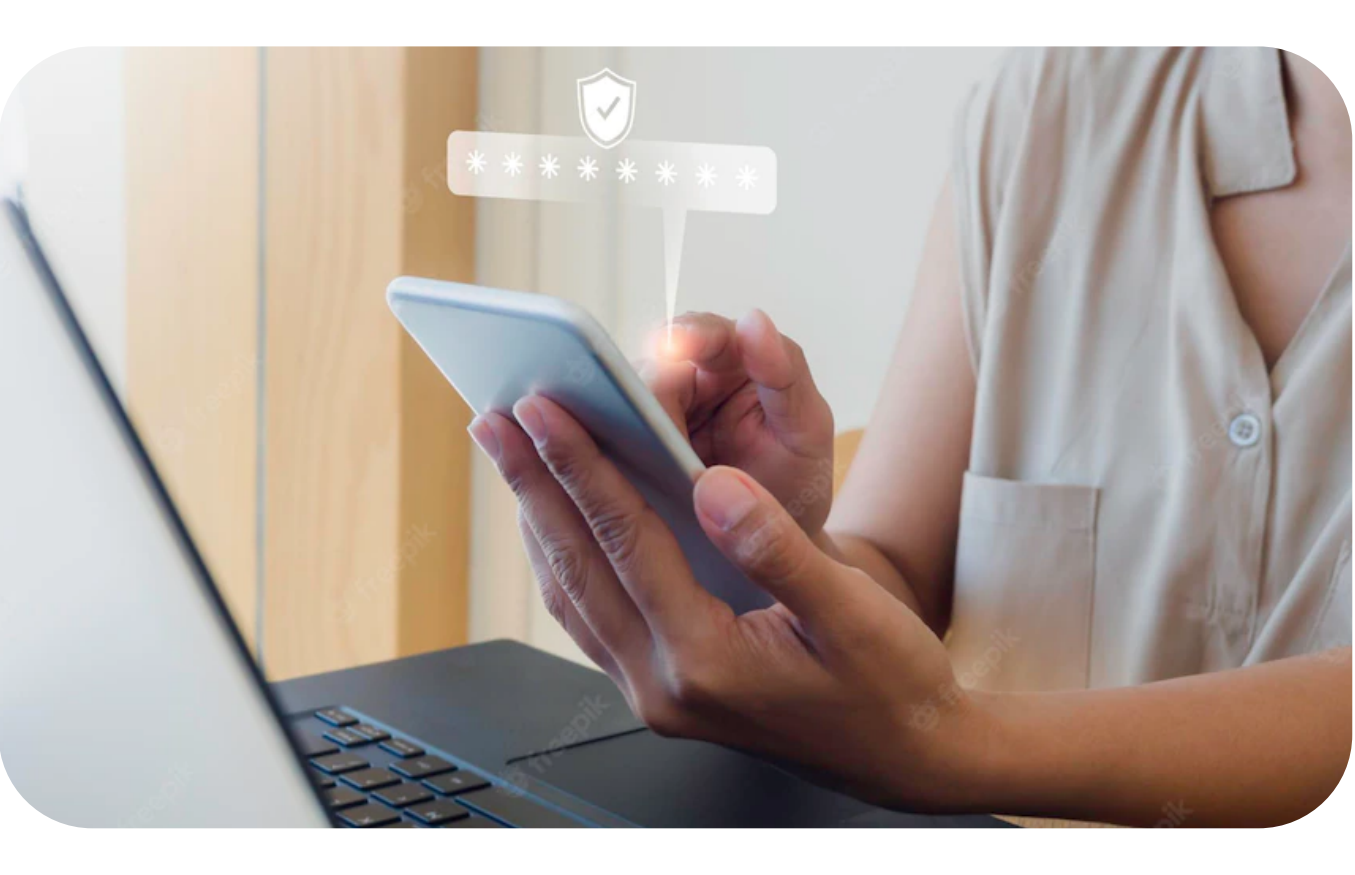
You can know if a password has been breached by visiting HaveIBeenPwned.com and comparing your login credentials there. If you find your information there, it's a major red flag that your data has already been breached. To sum up, avoid using the same password and keep updating them every six months.

If you find this task to be dreadful, you can use a password manager. These apps will help you create unique and robust passwords, and also remember them on your behalf.

Use 2FA

Simply put, multifactor authentication is when you apply an additional layer of security to your email account. This is especially useful if a cybercriminal steals your login credentials and tries to sign in. 2FA will prevent this from happening and you will be alerted to a login attempt.

The additional layer of authentication could be anything from a pin number sent to your phone, a secret code, your biometric information, or a security question. 2FA could render most data breach attacks useless and stops the perpetrator dead in their tracks.



Be Careful of Using Public WiFi

It may be tempting to use public WiFi because of its convenience and accessibility, but you should be well aware of the risks. For starters, you should verify if the WiFi network is encrypted. In all cases, it is a bad idea to use unsecured Wi-Fi to access your email because anyone could eavesdrop and steal your data.

In fact, you must ensure your workforce is not accessing emails on public WiFi. A much safer option is to use internet dongles or mobile data for access.

Use IAM Systems

One of the most effective ways of protecting against a phishing attack is to implement an Identity and Access Management system. IAM systems have the ability to deliver seamless authentication using security standards such as SAML. The user's identity is updated into your corporate network to the IAM solution, which serves as the Identity Provider.

If implemented correctly, an IAM system will serve as your first and last line of defense against criminal hackers who may have access to your credentials and passwords. It frees your employees from the paranoia of logging into their accounts and ensures frictionless usage of your digital systems that will boost productivity.

Learn the Basic Format of Phishing Emails

Most phishing emails are surprisingly obvious once you learn their format.

They are riddled with grammar errors, spelling mistakes, and other editorial issues that are not characteristic of any business worth their salt.

If you seem to get an email from your workplace that is asking for critical information, contact the person from your phone.

Finally, avoid clicking games and unauthorized websites to stay safe.

Remember to Log Out

Leaving your email account logged into your device is a major security risk, especially if you are traveling with your device. You can never really know if someone has access to your device, physical or remotely, and access to your account.

A good email security practice is to log out of all your accounts before leaving your device unattended. This is especially true if you are out traveling with your device in tow.

Use a VPN

VPN systems encrypt your data from the device to their server using HTTPS protocols. This also applies to emails and other online activities that are performed while the VPN is active. Most VPNs also utilize a host of advanced security features to protect your data from online threats, including eavesdropping from your own ISP.

Wrapping Up

Security issues with emails aren't new. However, they often store large amounts of confidential data, making them a prime target of cybercriminals. This is why it is crucial to follow essential email security best practices to avoid losing your data and, ultimately, your reputation.

Need help implementing email security practices? Our security consultants at Microsys can provide customized solutions to bolster your network infrastructure and keep it safe from data breach attacks.

Contact Microsys today.