**Securing your email – 5 Best Measures**

With the advent of time sharing systems in 1960s, Ray Tomlinson paved the path for the arrival of a new method for communication which became the most celebrated offspring of the Internet era. Having widely recognised in the mid-1970s, there was a massive migration of people from writing letters to typing them and sending via the store-and-forward model method**. Electronic mail (Popularly known as E-mail or Email)** is still the most preferred messaging technique although the world is witnessing an explosion in case of building new instant messaging software and applications day by day. Primarily it was ASCII text-only which was extended later by MIME (Multipurpose Internet Mail Extension). From ARPANET to the most used outlook and Google mail, Email has earned the trust of its users worldwide... OR HAS IT!

Now that we have established that email is the most popular message sharing platform, being a technology of utmost importance, we should also consider the pros and cons of using email. Talking of the advantages, today email provides the best of all service with latest updates that pushes its way through any modern instant messaging application. Yet the risks are eminent. From email leaks that had played a vital role in Hilary Clinton losing the 2016 American Presidents election to the YOU-HAVE-WON-1MILLION spam, we’ve been exploited by intruders (hackers) a handful amount of times. The main issues involve spamming, malware; email spoofing, and email bombing and other privacy concerns that effect information leak. The question here is how we can defend ourselves from these menaces. Here, we will go through the 5 important measures to secure your email.

Firstly, let’s look at the most fundamental and primary issue regarding email- Accessing them. What do we have here? - An id to identify us from the million others, and a unique password which only the person should have the knowledge about. The password is the key to our email account and when it falls into someone else’s hands they may open the door and take stuff. So the first thing to keep in mind is to keep your password to yourself and never share your password with anyone else... as Fury said – “Trust no one”. Also care about from where you are accessing your mail. You may accidently save your passwords in public systems or internet cafes. So, maximum avoid accessing your email from other than your PC or trusted systems and beware of key loggers.

Now that we know how the password should be kept, we shall also look into how the password should be. Ever heard of Bill Burr? He was the well known cryptography technology expert who proposed an eight page document on passwords which specifies the best method of initialising passwords. His proposed method was to use irregular capitalization, special characters and at least one numeral which would result in something like Password@123. The truth is that a password like this could be cracked by an expert with a 2 or 3 days’ crack job. Most of today’s passwords are of this structure which makes it easier for someone to exploit your account. Bill Burr himself had apologised for such an advise upon regret, but the trend seems to be so struck that many password columns has been structured to be typed so. Recommending a password structure would be stupid. It is supposed to be unique. Today the best password is the one which would take the most days to decrypt. We are living in a society where passwords are difficult for humans and easier for machines to understand.

Now that we have got into our account, let’s talk about how to manage email safely.

The second measure is to identify and avoid spam. Most of the email platforms filter spam into a spam folder which ultimately gets deleted. Somehow, spam still gets through and reaches up to you. The first thing to do is to make sure that you know and trust the sender before opening the mail. Avoid mails with ridiculous titles like YOU HAVE WON A MILLION. No agency rewards such a big amount for doing nothing. Once you have opened the mail, check out for the content. It all depends upon your common sense to identify the spam here. Hover over any attached links to check whether the destination is to where it is said to be. Spam can have titles including insurance, rewards, lease, loans etc. It is not any technological skills that matters here, it is our wisdom that plays a great role in identifying threats like these.

Thirdly, never share any sensitive information via email. However secure email maybe, there is always someone who knows better than the expert that manages your email security. Your email client may have encrypted the mail you sent like the Gmail does since 2014. But some browsers may not support this encryption and your mail may be sent without being encrypted.

Using VPN might be a best way to secure your email, which is the fourth measure according to me. VPN creates an encrypted tunnel which ensures the email to be sent without letting the guards open for the hackers to exploit.

The fifth, final and the most important thing to keep in your mind is to use a trustworthy and secure email service.

To conclude, let me brief you with the foretold measures. Ultimately, all you have to do is to not be stupid. Don’t go on clicking every links that you have received, and try not to share any personal or sensitive information to any unknown third party. Whenever you are using a public Wi-Fi, try to tunnel up using VPN. Your data is valued more than a million dollars by some abracadabra enterprise. And be awake with your conscience active. Be Careful and be thoughtful about your data security, because your data is your most valuable asset.