

What is email encryption? Why does it play an important role in email security?

How to secure email? What is email encryption and why does it play an important role in email security?

There are millions of emails (emails) sent back and forth every day on the internet environment. Many of these messages are random conversations among friends, but there are also a lot of work emails that contain sensitive, high-value, sent data that are not protected by Any additional security method, the simplest is email encryption.

This is like a lucrative bait for cyber criminals who appear abundantly in every corner of the internet. By installing malicious code or simply using some sophisticated phishing techniques, crooks can easily access these unsecured emails, hijacking sensitive information about an individual or certain organizations, businesses, and use it to extort money, gain illicit profits, or impersonate and destroy the victim's reputation. In short, regularly sending emails containing important data without using additional security measures can cost you dearly!

1. Tracking email and privacy infringement - old problems that are not old



Email encryption is an important area in data security

So how to secure email? What is email encryption and why does it play an important role in email security? We will find out now.

Encrypt emails and things to know

1. What is email encryption?
2. Why should we encrypt emails
3. Why email encryption can prevent large-scale hacks

4. Make a habit of encrypting emails right from today

What is email encryption?

Encrypted email (short: encrypted email) is one of the cybersecurity systems that every company, organization, or individual can use and should use to keep information secure. sensitive information hidden in e-mail, away from the peeking of hackers.



Email encryption helps your data stay away from hackers

In other words, encrypted email is the type of email that contains sensitive information concealed and protected by an intensive encryption program, only the person who has the corresponding decryption tool can access these emails. Email after encryption will be kept absolutely secure during the move from the sender's mailbox to the recipient's mailbox, any third party actors will not be able to read the content even when approaching be with email.

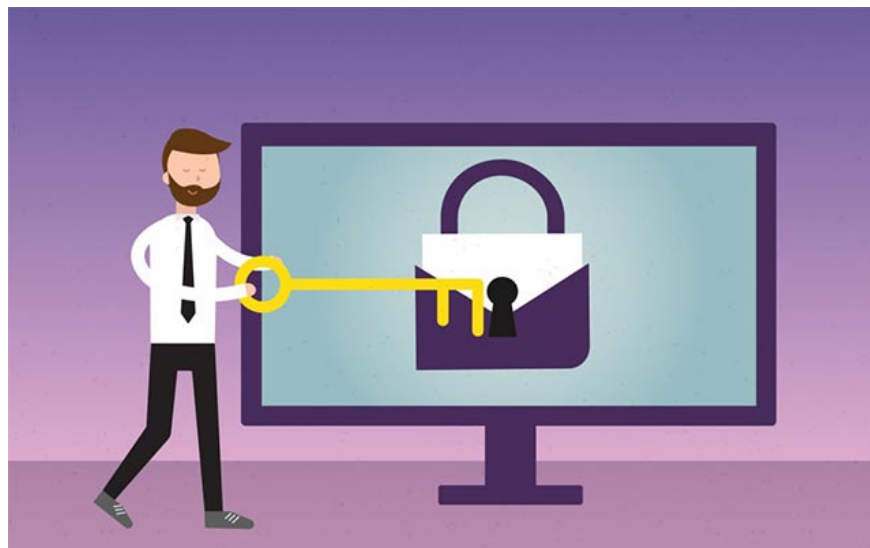
People who do not pay attention to online security or do not really understand what encrypted email tends to underestimate the importance of this most basic security method, as well as how but encryption can prevent 'security disasters' for them and their network itself.

1. Be wary of disguised Microsoft OneNote Audio phishing emails

Why should we encrypt emails

As mentioned above, the ultimate purpose of email encryption is to keep the email safe from bad Internet agents. Therefore, if you think deploying email encryption forms should only be done by banks, businesses, or organizations that often handle a large amount of sensitive information every day, that thought completely wrong. Even company employees and managers should do this whenever they send messages over the internet.

You too, create your own coding habits before sending important content.



The ultimate purpose of email encryption is to keep the email safe from bad actors on the internet

Do you think the current email environment is safe? The same is true, but not really. Email can be safer than some messaging, online chatting tools and even social networks, but in fact, there are always dozens of people who are always on the hook and ready to access and steal information. believe in emails you send over the internet. When your 'naked', unsecured emails are successfully accessed by crooks through man-in-the-middle attacks or DNS hijacking (DNS hijacking), surely all the information in the email will fall into their hands. How severe then the consequences will depend on the importance and sensitivity of the stolen information.

Another reason you should use encrypted email is because in many cases, your email may be in someone else's inbox rather than the intended recipient, in other words you send it. mistaken email to someone else's address. The cause of the wrong sending is endless, probably because the information authentication error is the most common error of data entry from the email sender. If you accidentally mistakenly sent an important information or attachment containing the company's confidential documents to another person, that would be disastrous. However, this disaster can be completely prevented remotely with a very simple operation: Encrypt email before sending.

In case the email is encrypted, the recipient will not be able to access the email unless they are in the process of replacing the decryption tool.

1. 7 reasons not to use desktop email software

Why email encryption can prevent large-scale hacks

From the perspective of cyber criminals, unsecured email is a great way to spread malware into a large-scale system with many security barriers. The implementation is not too complicated. After accessing the email, hackers can easily change the content of your message and insert malware, thereby infecting malicious code onto the recipient's device, further the entire system. network of an organization. In contrast, hackers can also change the content of email responses and 'inject' malware into your device.



Hackers can insert malicious code into an unencrypted email

Besides, once hackers have gained access to your inbox via malware, stealing other information will become extremely simple. They can then use your identity and email to continue to infect other accounts in the email, resulting in a large-scale malicious attack.

Again, email encryption can help prevent all these problems.

1. Microsoft 365 added control over encrypted emails, increasing user privacy

Make a habit of encrypting emails right from today



Do not let yourself become a victim of new attacks that are coming out that can stop early

There is no denying the important role of email encryption for privacy and security issues. However, there are still many users of email services, especially general users, lack of knowledge about data security, do not know how valuable their email is to hackers as well as their vulnerability is not protected by additional layers of security. If you have never coded email before, it is not too much to start from now. Do not let yourself become a victim of new attacks that are coming out that can stop early.

If you do not know how to encrypt email, you can refer to some of the following articles:

1. How to encrypt email
2. How to encrypt email on Microsoft Outlook
3. How to encrypt Gmail, Outlook and other webmail
4. How to send encrypted email on Android using OpenKeychain

You finished reading the article "**What is email encryption? Why does it play an important role in email security?**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.