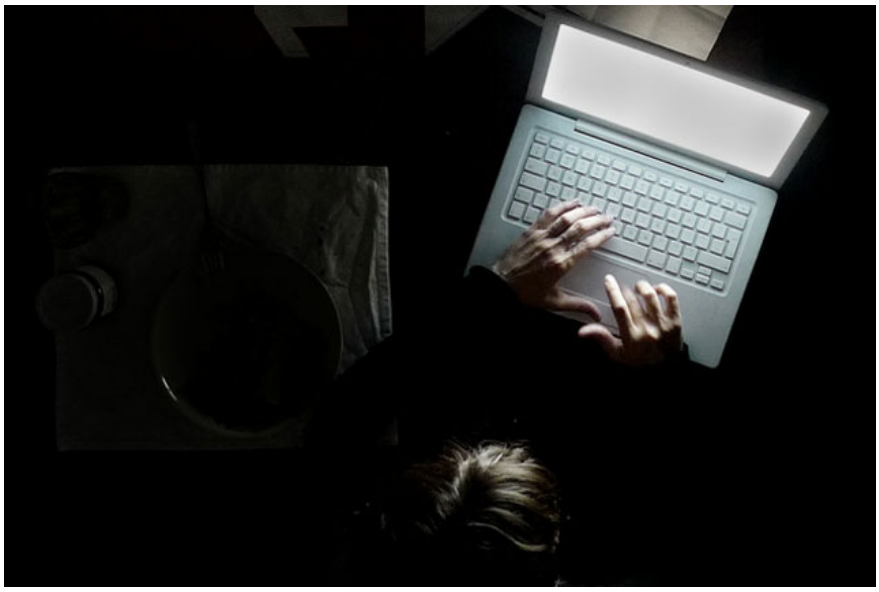
Steps to protect email against malicious threats

The following ways seem to be very simple and popular, to the extent that 'everyone knows and of course', but not everyone seriously takes it to stay away from any risk of fraud or malicious code attacks.

The following ways seem to be very simple and popular, to the extent that 'everyone knows and of course', but not everyone seriously takes it to stay away from any risk of fraud or malicious code attacks.



Attachments in email 'anonymous'

Do not open them. These emails often have language that entices people to open attachments to read. These files may contain malicious code that is automatically downloaded to the computer. The rule is simple: if you don't know the sender, don't open the attached file.

Links

The same principle applies to links in emails coming from people you don't know. As with attachments, scammer always tries to convince the user to download malicious code to the system. Clicking on the link can lead users to a malicious website. Therefore, if you do not know the sender or do not trust the link, do not click on it.

Be careful with emails that look "real"

Hackers often try to persuade users to open attachments, click on links or file personal information through emails that look very much like emails from trusted organizations, such as banks, government agencies or vendors. online retail. Users should not click on any links or send any information, unless they are confident of those legitimate emails. Users should also not run the cursor over the link to see where it really will be.

Scan virus

Users need to have a virus scanning routine for all attachments before opening them. Doing so can avoid giving them a lot of headaches, not only for users but also for their contacts. Often the malicious code in the attachment will infiltrate the system and spread through emails sent by the owner to those in the address book.

Computer protection program

Users and businesses need to ensure that the computer system has comprehensive protection measures. According to security companies, there are two things to consider when choosing an antivirus solution. First, users must take measures to protect email to detect both viruses and spam, including unprecedented new viruses. Second, that solution must be updated. In addition, users should regularly scan the entire system.

Do not forward spam

Forwarding spam only helps spread the virus that can be hidden in them, making your friends and others at risk. It also takes time and costs bandwidth.

Be cautious with the risks of Web 2.0

Most social networks, including Facebook and Google+, provide users with email and private messaging services. If users accept files via these social networks, they need to make sure they have a full virus scan before opening them.

No share

Users should never share personal information, as they can be used in phishing scams. Sometimes, information may be leaked when responding to email requests for account verification, or logging into accounts on unsafe computers.

Strong Password

Users want virtual criminals to have trouble trying to break into email accounts that require strong passwords. If a hacker cannot break into a user account, they cannot have an address, personal information or other personal data.