The only secure email is the text-only email

It is annoying when opening an email that seems to come from a boss, friend or bank, it turns out to be a phishing email.

It is annoying when opening an email that seems to come from a boss, friend or bank, it turns out to be a phishing email. Any email in the normal looking email stack you receive every day may be trying to get you from login information or give identity theft or personal data.

Most people think that fraud is caused by the user, that they have right-clicked something. To fix it, just don't click around. But as security experts study malware, we may be wrong.

The real problem of the web mail system is that small information schools invite to click and roll users into a highly interactive web experience. Not just Gmail, Yahoo Mail or similar services. But email software on the desktop like Outlook also displays such messages.

Simply put, secure email is an email with only text, displaying text only without embedding a link or image. Webmail is convenient to advertise (and allows you to write beautiful emails with beautiful images and fonts), but with them are unnecessary and very dangerous dangers by the website (or email) that can be displayed. display something but do something else.

Putting email back into plain text even though it sounds primitive, makes it more secure. Even top government security experts have concluded that anyone, organization or government, interested in web security should return to using plain text.

Understand the problem

In recent years, web mail users are advised to pay close attention to each email that they open. Do not open email from strangers, do not open the attachment without checking it first. Organizations hire security companies to check if their employees are doing the right thing. But scams continue and become more and more popular.

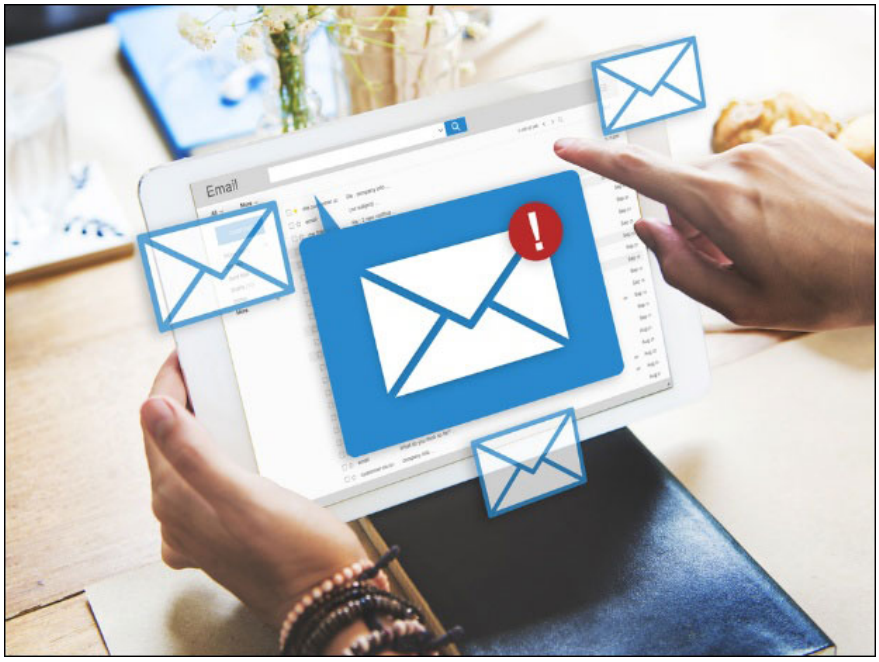
No shortage of phishing stories with just one click on email

But the real problem with webmail - a billion-dollar security mistake - is that if email can be sent and received via the website, they can do more than just display the text, even the website.

Danger available

Web browsers are very insecure tools. The browser is designed to mix all types of content from anywhere - text from a server, ads from one place to another, images, videos from a 3rd place . The site is a patchwork of many pages of the party 3rd, maybe up to a dozen. In order for this blend to be consistent, the browser not only shows where this piece comes from or where it will go when you click.

Worse, it allows the site - here is the email - lie. When typing google.com on your browser, you will definitely be taken to the Google page. But when you click on the link or where Google is attached, can you really go to the Google page? Unless carefully read the HTML source, there are many ways for the browser to trick you.



It's hard to know what will happen after clicking

That is no security at all. Users cannot predict the consequences of their behavior or decide in advance whether the results are acceptable or not. A secure link can be located next to the malicious link without any difference. When you see a website and decide on what to click on, there's no way to know what will happen, which you will interact with afterwards. The browser is designed to hide this information. But at least when browsing the web, you can choose to start with a reputable site. But webmail brings the website that the attacker directly into your inbox.

The only way to use secure webmail is to learn the skills of web developers. Only then, the HTML, Javascript . codes become clear, and only then will you know what will happen when you click. Of course it is unreasonable to require users to learn these complex things to protect themselves.

Until software designers, web developers revise the webmail system and the browser, so that users know where they will be directed when they click, we should follow CAR Hoare's advice, one of the pioneer of computer security: 'The price of trust is to pursue the simplest things'.

Secure email is email only text

Businesses are more vulnerable than individuals. A person only needs to care when he or she clicks, but each employee is a weakness. Just doing simple calculations will see: every employee with 1% is cheated, the total risk for the whole company will be much greater. Businesses with 70 or more employees are at risk of greater than 50%. They have to choose carefully the webmail provider.

For a long time we have seen many technologies that are actually a bad idea whether it looks good. Users interested in security need to ask the email provider to make an option to use only text email. Unfortunately, such choices are very few.