Phishing

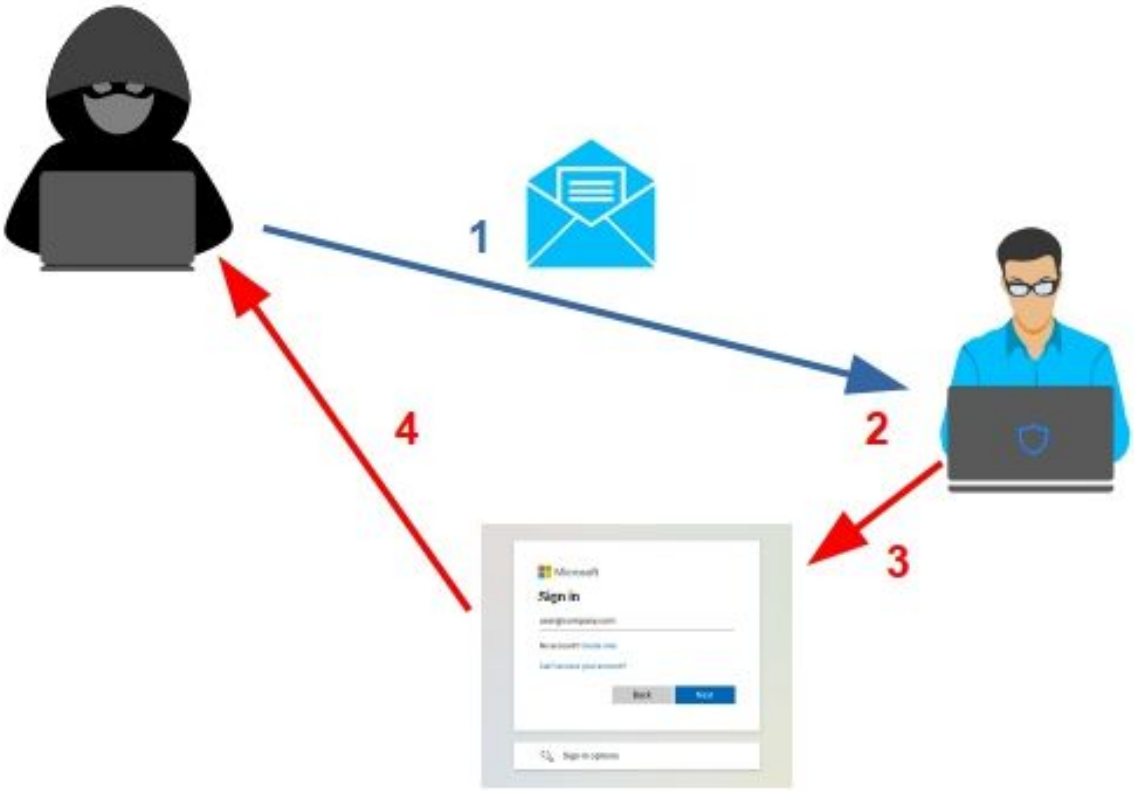
Phishing is currently the most current way to get a ransomware into your computer or network, or to have your data stolen. According to a Guardian Digital report, 91% of successful cyber attacks begin with a phishing email.

Despite the number of technological solutions designed to counter phishing attacks, from antimalware software to multifactor authentication, the best defense against phishing is user awareness. Indeed, a successful phishing attack always requires the user to perform an action, like entering their credentials into a form or clicking on a dangerous link.

Read on to see how you can detect and act on basic phishing.

How phishing works

1. The attacker sends a phishing mail including a link to a fraudulent site.
2. The user receives the mail and clicks on the link.
3. The user is redirected to a site controlled by the attacker, mimicking a legit site, and enters their username and password.
4. The harmful site sends the username and password to the attacker.



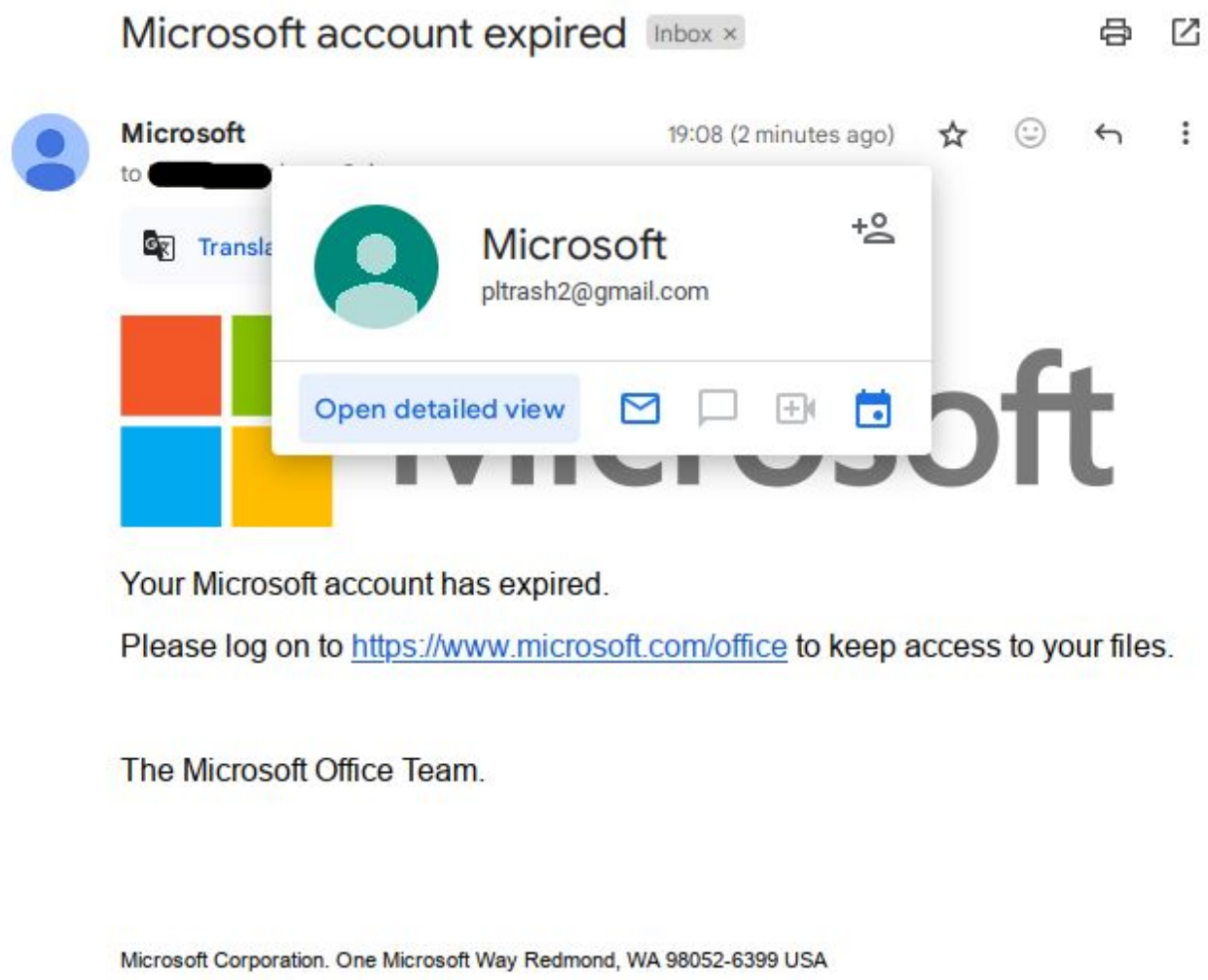
How to avoid phishing as a user

There are several elements that can alert you about the legitimate status of the mail.

Check the sender's address

A mail can contain 2 addresses for the sender: the 'real' one, used to log into their email system, and another one, called the display name, that can usually be freely set. In Gmail, it can be displayed by default, or a click on the down arrow near to the recipient name reveals the real sender's address, written between square brackets (<>).

In this example, the real name of the sender is *pltrash2@gmail.com*, but I have modified the display name to look like a legit one. If the 2 names are different and the 'real' sender name does not correspond to a known person or company, beware!



Check the link

Links are not always what they seem to be. The text they present is not always the real destination they link to. If you hover with your mouse on the link, it will reveal its real destination. Look at the bottom left corner.

In this example, the link seems to point you to a Microsoft site (*www.microsoft.com/office*), while it redirects to an evil site, potentially mimicking the real Microsoft login screen and capturing your credentials.

How to combat phishing as an IT literate

- Enable antiphishing software.
- Add fraudulent domains to your email filters, proxies, DNS, firewalls.
- Train your users.
- Report phishing emails to authorities.
- Report phishing emails to the domain owners.
- Report the phishing sites to browser makers.
- Report the phishing sites to registrar or hoster.

All these actions will be explained in future blog entries.