Warning of phishing attacks based on fake Zoom meetings

According to Forbes, the Covid-19 pandemic caused unemployment to skyrocket. Uncertainty everywhere is an opportunity for cybercriminals to exploit.

This was warned by researchers at Sophos Labs after discovering a new phishing campaign by enticing users with bogus Zoom invitations. These invitations with tactics related to meetings, payrolls . and even words like termination are put in to increase the element of fear.
Like many similar campaigns, there are key scenes where users should clearly see if emails are phishing attacks and are legitimate invitations. Even the emails claim users' presence is important for the meeting to make it easier to deceive.
Upon receiving this email, users will see the links in the message that when clicked they will be taken to a website whose login window looks similar to Zoom. Quickly check the address bar of the browser, users will find that they are not really on the site zoom.us. The purpose of this fake Zoom site is to steal users' emails.
To avoid being cheated, users click on the padlock icon next to the website address to see information about its SSL certificate. Zoom.us website will have a certificate issued by GoDaddy in 2019.
A closer look at the fake login reveals another important detail, which not only requires the email address and password like the actual Zoom, but also the user's email address and email password. According to the report, the scammers behind these attacks do not really want the user's Zoom credentials, but rather the email password. Email passwords are more useful for an attacker - so make sure to enter it only on the website the user actually checks.