Vulnerability in Microsoft Outlook makes users believe in phishing emails

A new vulnerability has just been discovered by a security researcher on the Microsoft Outlook platform.

A new vulnerability has just been discovered by a security researcher on the Microsoft Outlook platform. This vulnerability makes users believe in phishing emails.

The cause of the problem was that Outlook's Address Book displayed the user's contact information including information from the Internationalized Domain Name (IDN). Meanwhile, IDN consists of letters from different scripts such as Cyrillic with face shapes similar to those in the Latin alphabet.

Therefore, bad guys can easily take advantage of this vulnerability to impersonate individuals from reputable organizations. Users will be easily fooled when looking at contact information with fake domains that look like the real thing.

This vulnerability was discovered by a security researcher nicknamed Dobby1Kenobi. He reported it to Microsoft and Microsoft confirmed the issue but refused to patch the vulnerability at the time.

Microsoft believes that Outlook users should not trust the sender's identity without a digital signature. Although spoofing issues can occur, Microsoft decided not to patch to avoid false positives.

However, recently Microsoft finally released the necessary patch. As reported by Windows Central, in Outlook 16.0.14228.20216, Microsoft fixed the issue reported by Dobby1Kenobi. Therefore, to be on the safe side, you should update your Outlook to the latest version.

In addition, to avoid being scammed, always pay attention to the identity of the sender. In case of an important transaction, in addition to online identity verification, you need to combine direct contact to ensure safety.