THE IMPORTANCE OF NOT ENTERING CREDENTIALS

ON FAKE SITES

A "**credential**" is made up of a **username** and **password**; they are the platform access data and/or applications.

Cyber attackers launch phishing campaigns with the goal of confusing you. The body of the message usually varies but the structure and objective are the same:

Steal your access!

¡SUSPICIOS!

If the email tells you that **the password is going to expire soon,** there is a **new service update** and it can no longer be used from XX date.

Make sure the recipient is legitimate.

UPDATE NOW

https://websmail.contrOl536HDgtñil

¡DO NOT BELIEVE!

If in the text of the email the recipient **incites you to click on a fraudulent link** to change your password or update it.

Never click without first hovering over the link or button and verifying that it is real.

¡DON´T TRUST!

If in the text of the email **they directly request your access data;** informing you that they will execute the changes automatically.

Never give out your personal data.

Do not hide or minimize it, it´s very important that you notify it!

Report it immediately to the security area.

TU LOGO AQUÍ