How to get rid of “phishing” (password theft) in a few simple moves
"Phishing" is a type of fraudulent email that attempts to steal a user's credentials (user name and password).

The user is urged to open a web page and type in his or her credentials, which are then stolen and used for illegal purposes.

Fortunately, it's easy not to fall victim of phishing email, as we will see in the following pages.
How to tell if it's phishing

Usually, a phishing email can be spotted as it lures the user to “confirm”, “validate”, or “renew” his or her password by clicking on a link.

The phishing message is often written in English, or in more-or-less broken Italian.

The web page provided by the phishing email does not belong to University of Verona, even if it looks like it does: it belongs to the attacker!
Phishing examples

In the next few pages we will examine some examples of phishing (actual email I received), highlighting the elements that mark the messages as phishing.

As a comparison, we will also examine the legitimate (and only one!) email message provided by University of Verona when a user's password is about to expire.
This is the legitimate message that is sent when a password is about to expire. Please note that the message is written in Italian; it does not include links; it contains instructions that point to the Univr home page and Intranet site; it refers to the GIA code both in the “To:” field and in the message body; “From:” is gia@univr.it; it does not urge the user to “validate” or “confirm” his or her password; the subject is “GIA Notifica Scadenza Password”.

The legitimate Univr email
This email is phishing because 1) it **does not come** from gia@univr.it; 2) it contains the word **"convalidare"** (validate); 3) it contains a **link**; moving the pointer on it (**without clicking**) 4) a **hidden address** is revealed, and it's different than the link shown; 5) it's written in broken Italian; 6) “From” and Subject are wrong; 7) instead of “A:” (To:) there is “Rispondi A:” (Reply to:).
This email is phishing because 1) it does not come from gia@univr.it; 2) it contains the word “convalidare” (validate); 3) it contains a link; 4) the Subject is not written in Italian (“Alerta de Emergência!!!”); 5) “From” and Subject are wrong; 6) instead of “A:” (To:) there is “Rispondi A:” (Reply to:).
This email is phishing because 1) it does not come from gia@univr.it; 2) it contains the word “aggiornamento” (update); 3) it contains a link; 4) it's written in broken Italian; 5) “From” and Subject are wrong; 6) instead of “A:” (To:) there is “Rispondi A:” (Reply to:).
This email is phishing because 1) it does not come from gia@univr.it; 2) it's written in English; 3) it contains the word “validate”; 3) it contains a link; 4) “From” and Subject are wrong; 5) instead of “A:” (To:) there is “Rispondi A:” (Reply to:).
Example 5: phishing in English

Attention:
An Attempt has been made to Your Account from a new computer. Please kindly confirm your account. To Confirm Your E-mail Account Kindly click : [http://clubpeng.in/1IU7agD](http://clubpeng.in/1IU7agD)

@univr.it IT Help Desk.
Thank you for your cooperation.
System Administrator.

As an exercise, the reader is invited to try and identify the elements that make this email a phishing email!
Let's examine again the legitimate message that is sent by the GIA system when a user's password is about to expire. Please compare this message with the phishing examples!
In conclusion

Beware of phishing!

Now you have all the information you need to avoid phishing. Don't bite the bait and delete all suspicious messages. If you have any doubt, please contact your department's IT staff at once.

Good luck with your work!