How to access my email from outside the university network?

The email service of the university is accessible from any place on the Internet, if the following points are taken into account:

- Whenever possible, use secure connections (SSL / TLS) to encrypt communication and ensure the confidentiality of the password and data as much as possible.
- Always, the easiest way to access is through the secure www interface ("https" instead of "http"): https://correo.uv.es.
- It can also be accessed with any email client program, for this:
  - For the reading of mail, no special configuration is required, it is used the same as for the university network, preferably encrypting (server post.uv.es, gate IMAP 143 with TLS or IMAP 993 with SSL).
  - For sending mail,
    - (Recommended solution) Configure your email client to use post.uv.es as an outgoing mail server, through the MSA delivery gateway, encrypting the communication and authenticating yourself with your username and password when sending, ie using SMTP_AUTH, SSL and MSA gate.
    - There is a help to configure mail programs with SMTP AUTH. In all cases, the configuration to use a secure SSL / TLS connection is also included (beware, the change from SMTP gate 25 to gate 587 has not yet been incorporated into the documentation).
    - The advantage of this solution is that the configuration will be the same regardless of where you connect from and you do not need anything more than your mail client.
    - You can also configure your email client program in the same way as if you were in the university network if you accessed using VPN (note that some providers do not allow the use of the VPN).
    - Similarly, you can configure your email client program in the same way as if you were in the university network if you use the university as an access provider. This is only possible for people who have a POST account and have requested and obtained a modem account.

Be careful! When you set up a mail client, always remember that if you tell it to use POP3, it will bring all the messages to the computer on which you are using it and delete them from the server ... unless you explicitly configure it contrary.

As far as security is concerned, remember that it is always a risk to use a computer that has been installed and / or configured by third parties. For example: it is extremely easy to put a hidden program that notes everything we write on the keyboard ...

(*) It is increasingly common for an Internet access provider to prohibit the use of your SMTP server if the email address you put in the return address is not from your network.