Uso del Correo Electrónico

Cómo funciona el correo

Los correos electrónicos se depositan, para su envío, en servidores que pueden implementar o no controles de uso.

En los servidores sin control de uso, los correos pueden ser legítimos o maliciosos. Éstos últimos se caracterizan por la falsificación del remitente y/o contenido. Por lo tanto, cuando recibimos un correo que por su contenido o remitente nos genera dudas, lo primero que debemos hacer es comprobar que el remitente es quien dice ser, y no abrir antes de asegurarnos, que quien lo envía y su contenido son correctos.

¿Qué podemos hacer?

Cuando en un correo nos piden datos personales, credenciales, o que llevemos a cabo alguna acción (transferencias, códigos bancarios, ejecutar programas,…), no facilitar ni ejecutar lo solicitado sin que previamente nos aseguremos de su veracidad.

Una forma fácil de comprobar el origen del correo es observando su cabecera. Por ejemplo: Thunderbird botón mas/Ver código fuente

```
Return-path (dirección de respuesta, puede ser falsa): <pepe@xxx.com>
Envelope-to (destinatarios): xxx@unizar.es
Delivery-date (fecha envío): Mon, 18 Nov 2019 11:36:04 +0100
Received (servidores por lo que ha pasado): from outbound6sev.lav.puc.rediris.es
([130.206.19.181] helo=mx02.puc.rediris.es)…….
Received (servidor inicial del correo): from yyy.xxx.com (yyy.xxx.com [194.29.34.68])
     by mx02.puc.rediris.es  with ESMTP……..
     Mon, 18 Nov 2019 11:36:02 +0100
x-m-msg: CPCHECK
```

La cabecera muestra información de los servidores por los que ha pasado. En este caso el dominio del correo xxx.com debe ser igual entre la dirección remitente y el inicio del correo (se puede ver `pepe@xxx.com` y más abajo `yyy.xxx.com`).

Una forma de poder solucionar estos problemas es utilizando la firma electrónica, que garantiza tanto el remitente como su contenido.