



El Phishing

¿Qué es el Phishing?

El Phishing es un engaño que se realiza a través del correo electrónico; simulan ser una empresa, o un banco con la única finalidad de obtener información confidencial (contraseñas, datos bancarios, etc..).

¿Cómo funciona un ataque de phishing?



Lo más destacable de los phishing es que tienen apariencia real, pero no son auténticos.

Estas comunicaciones muestran habitualmente un link que nos dirige hacia una página web en la que nos solicitan datos personales.

También nos pueden enviar adjunto un archivo, conteniendo un troyano o malware, el cual si se ejecuta da acceso al contenido del equipo.

¿Cómo detectar estos ataques?

El primer punto es comprobar que la URL de destino es auténtica. En las ocasiones que la dirección esté oculta, podemos pasar el ratón por encima del enlace para que nos muestre la dirección; ésta aparecerá en la barra de estado o sobre el propio enlace.

Otro punto a tener en cuenta es el nombre del remitente y la dirección de correo, pueden falsificarse ambos para que parezca de un origen conocido.

Suele ser muy común en estos correos destacar la urgencia en confirmar nuestros datos y las nefastas consecuencias de no hacerlo, hay que desconfiar.

Ante todo hay que evitar, dar datos personales, descargar y/o ejecutar ficheros adjuntos.

La Universidad de Zaragoza no solicita nunca ninguna credencial (usuario y contraseña) por correo electrónico, ni otros sistemas de mensajería.

Debemos acceder siempre a los servicios a través de la dirección que ya conocemos y no a través de enlaces que nos puedan llegar. Ejemplo: la web de Unizar es <https://www.unizar.es/> o la del Campus Virtual es <https://moodle.unizar.es/>. De esta forma siempre estamos seguros de que accedemos al recurso correcto.