tranxfer | secure file exchange

Cómo evitar ser objeto de phishing

El phishing es un delito muy habitual que consiste en engañar a otras personas para que compartan información confidencial como contraseñas o números de crédito.

Si dudamos del remitente:

1. Comprobaremos de quién es ese **dominio** (lo que va detrás de la @) en Whois. También podremos comprobar si esa URL aloja algún malware utilizando el servicio gratuito de análisis de URL de Virustotal.
2. En caso de que el correo electrónico no sea visible, analizaremos los **detalles de la cabecera** del mensaje (aquí puedes ver cómo ver las cabeceras en distintos clientes de correo y cómo entenderlas) para comprobar la dirección de correo del remitente, aunque este dato no es del todo fiable, pues podrían estar suplantándolo.

Si el mensaje tiene adjuntos sospechosos:

1. **Tendremos habilitada** la opción que permite mostrar la extensión de los archivos en el sistema operativo
2. Si dudamos de un archivo que hemos descargado podemos comprobar, antes de ejecutarlo, si contiene malware en la web de Virustotal.
3. Deshabilitaremos las macros en Microsoft Office. Esta es la forma de hacerlo en Mac OSx y en Windows.
4. Para impedir la ejecución de archivos ejecutables a los usuarios, se pueden utilizar **aplicaciones de lista blanca** como AppLocker.

Si el mensaje nos invita a hacer click en enlaces:

1. Ante la mínima sospecha copiaremos el link y lo analizaremos en Virustotal o en otra página similar.
2. Los enlaces acortados pueden esconder sorpresas desagradables pues a priori no podemos saber dónde nos llevarán. Una opción es copiarlos en unshorten.me para extenderlos antes de hacer clic en ellos.

tranxfer | secure file exchange

Cómo evitar ser objeto de phishing

El phishing es un delito muy habitual que consiste en engañar a otras personas para que compartan información confidencial como contraseñas o números de crédito.

Si dudamos del remitente:

1. Comprobaremos de quién es ese **dominio** (lo que va detrás de la @) en Whois. También podremos comprobar si esa URL aloja algún malware utilizando el servicio gratuito de análisis de URL de Virustotal.

2. En caso de que el correo electrónico no sea visible, analizaremos los **detalles de la cabecera** del mensaje (aquí puedes ver cómo ver las cabeceras en distintos clientes de correo y cómo entenderlas) para comprobar la dirección de correo del remitente, aunque este dato no es del todo fiable, pues podrían estar suplantándolo.

Si el mensaje tiene adjuntos sospechosos:

1. **Tendremos habilitada** la opción que permite mostrar la extensión de los archivos en el sistema operativo

2. Si dudamos de un archivo que hemos descargado podemos comprobar, antes de ejecutarlo, si contiene malware en la web de Virustotal.

3. Deshabilitaremos las macros en Microsoft Office. Esta es la forma de hacerlo en Mac OSx y en Windows.

4. Para impedir la ejecución de archivos ejecutables a los usuarios, se pueden utilizar **aplicaciones de lista blanca** como AppLocker.

Si el mensaje nos invita a hacer click en enlaces:

1. Ante la mínima sospecha copiaremos el link y lo analizaremos en Virustotal o en otra página similar.

2. Los enlaces acortados pueden esconder sorpresas desagradables pues a priori no podemos saber dónde nos llevarán. Una opción es copiarlos en unshorten.me para extenderlos antes de hacer clic en ellos.