PROTEJERSE DE CORREOS PELIGROSOS

Una forma favorita que usan los ciberdelincuentes para introducir malware es enviando correos electrónicos. Buscan confundirnos y hacer creer que se trata de algo legítimo y a veces usan ingeniería social para provocar miedo y la necesidad de descargar un archivo o hacer clic en un link.

Hay correos muy peligrosos: Tienen un link o enlace que al abrirlo, instalan un programa troyano en el equipo sin que nadie se de cuenta y sin que se note. Los filtros de correos electrónicos no los detectan ni los Antivirus tampoco. Abrenuna puerta oculta por la que pueden robar información confidencial o incluso instalar programas.

Vamos a explicar cómo evitar caer en engaños y defendernos de estas amenazas. Utilizar el sentido común es lo más importante.

Una técnica muy usada es utilizar un nombre de correo casi calcado al real. Esto hace que la víctima crea que está ante un e-mail de una empresa legítima, por ejemplo. Modifican caracteres del nombre, pero sin que sea llamativo. Un ejemplo es poner una l en vez de una i en los nombres.

Cómo evitar ser víctima de correos falsos

Nunca abrir correos que conozcamos su remitente. Pero claro, como hemos mencionado en ocasiones "calcan" el e-mail real. Hay que **prestar atención a pequeños detalles que puedan delatar al ciberdelincuente:** Letras cambiadas, algún símbolo que no tenga sentido o cualquier otra pista que demuestre que ese correo no es realmente lo que pretende ser.

Observar bien el asunto del mensaje. Aquí puede haber pistas. Hay que mirar si se dirige realmente a nosotros o es un mensaje genérico. También posibles errores de traducción que delatan que ese e-mail ha podido ser traducido a varios idiomas para afectar a víctimas de diferentes países.

Nunca respondas a correos que veamos que son spam o posibles fraudes. Algunos del tipo "*responde a este e-mail para recibir tu premio*". Realmente lo que los ciberdelincuentes buscan es confirmar que detrás de nuestra cuenta hay un usuario activo.

Nunca abrir archivos adjuntos sospechosos. Puede ser incluso un archivo de Word que pueda parecer inofensivo. En caso de dudas, consulta directamente con la supuesta empresa que nos remite el e-mail, de manera separada. Esto significa mandar un correo directamente al e-mail oficial.

Tener instalado un buen programa Antivirus es esencial y aunque no pueden en todos los casos, evitar que nuestro equipo se infecte si abrimos estos correos, sin embargo, sí que protegen de mucha basura peligrosa y variedad de malware proveniente de los correos recibidos.