PROTEJERSE DE CORREOS PELIGROSOS

Una forma que usan los ciberdelincuentes para introducir malware o robar datos es el envío de correos que asusten, nos confundan o hacernos creer de que se trata de algo legal. Usan la ingeniería social para provocar el miedo y la necesidad de **descargar un archivo** o bien de que **hagamos clic en un enlace o link**.

Casos ya típicos son recibir mails o de la Agencia tributaria, o del Servicio Postal de Correos o un mail de Notificación de Multa no Pagada firmado por la DGT y el Ministerio del Interior.

En éste último caso, por citar solo un ejemplo, al hacer clic en el email, se abre una Sede Electrónica de la DGT falsa (parecida a la oficial) donde piden que metas tus datos personales y bancarios. **¡No lo hagas!** Es una estafa para robar tus datos bancarios. Recuerda que la DGT sólo notifica multas por mail si estás suscrito a su sistema de notificaciones electrónicas; así que mejor comprobarlas en la sede electrónica de la DGT o en el 060 antes de hacer ningún pago.

Como vemos hay correos muy peligrosos: Hace años casi todos venían en inglés pero ahora ya los traducen al español y vienen con ese dañino link o enlace que al abrirlo **instala 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. Abren puertas ocultas para robar información o instalar programas ocultos.

¿Qué hacer si recibes este tipo de correo? Siempre bórralo inmediatamente y **nunca hagas click en ningún enlace** que traiga.

A veces observándolos, se delatan: Hay técnicas frecuentes como usar un nombre de correo casi calcado al real; Por ejemplo, modifican caracteres del nombre, pero sin que sea llamativo. Otro ejemplo es poner una l en vez de una i en los nombres, etc.

Nunca abrir correos que desconozcamos 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 parece inofensivo. En caso de duda, 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 correos recibidos.