¿Qué es el keylogging?

La ciberdelincuencia evoluciona constantemente, lo que hace que sus estafas y engaños también lo hagan con la intención de que las potenciales víctimas no las distingan y detecten que se tratan de amenazas y así bajar la guardia y caer en sus trampas.

A parte de ser precavido y desconfiar siempre de lo que nos parezca sospechoso, la clave para detectar las evoluciones de las estafas es saber cómo son, para poder reconocerlas y detectarlas antes de que sea demasiado tarde. Aunque lo cierto es que existen algunas amenazas que no nos vienen de frente, esas son de las más peligrosas, y entre las más populares que nos encontramos está la de Keylogging.

Qué es el Keylogging

El Keylogging es una forma que utilizan los ciberdelincuentes para espiar a sus víctimas sin que se enteren y recopilar información personal, bancaria y contraseñas de estas de una manera sigilosa. Esto es porque consiguen monitorear el teclado de los dispositivos de estas personas para registrar el orden en el que las pulsan para acceder a sus cuentas y hacerse con la claves de acceso.

Para llevar a cabo este tipo de ataque/vigilancia, los ciberdelincuentes tienen que instalar un virus espía en el dispositivo que quieren monitorear. Para ello usan técnicas de phishing para que descargues sin saberlo un archivo que lo contiene. o en casos más extremos incluso podrían enchufar un dispositivo a tu ordenador y espiarte desde ahí.

A partir de ahí, registran las pulsaciones de teclas y son capaces de observar y guardar todas las contraseñas que ingreses. Como decíamos, este tipo de ataque es muy complicado de detectar, ya que no afecta al rendimiento o funcionamiento de tu dispositivo, y en muchos casos pasa desapercibido por los antivirus.

Cómo evitar el Keylogging

Autenticación de dos factores (2FA): activar 2FA en todas tus cuentas bancarias y servicios da una capa extra de protección.

Utiliza contraseñas seguras: es recomendable que incluya números, mayúsculas y algún carácter especial.

Actualización de ‘software’: un antivirus y antimalware actualizados pueden detectar y eliminar keyloggers antes de que sea tarde.

Atención con los correos electrónicos de desconocidos: no hacer clic en enlaces ni descargues archivos adjuntos de remitentes desconocidos o sospechosos.

Usa teclados virtuales y gestores de contraseñas: los teclados virtuales pueden disminuir el riesgo de que registre tus credenciales, mientras que los gestores de contraseñas nos evitan la necesidad de teclearlas.

Con información de El Economista