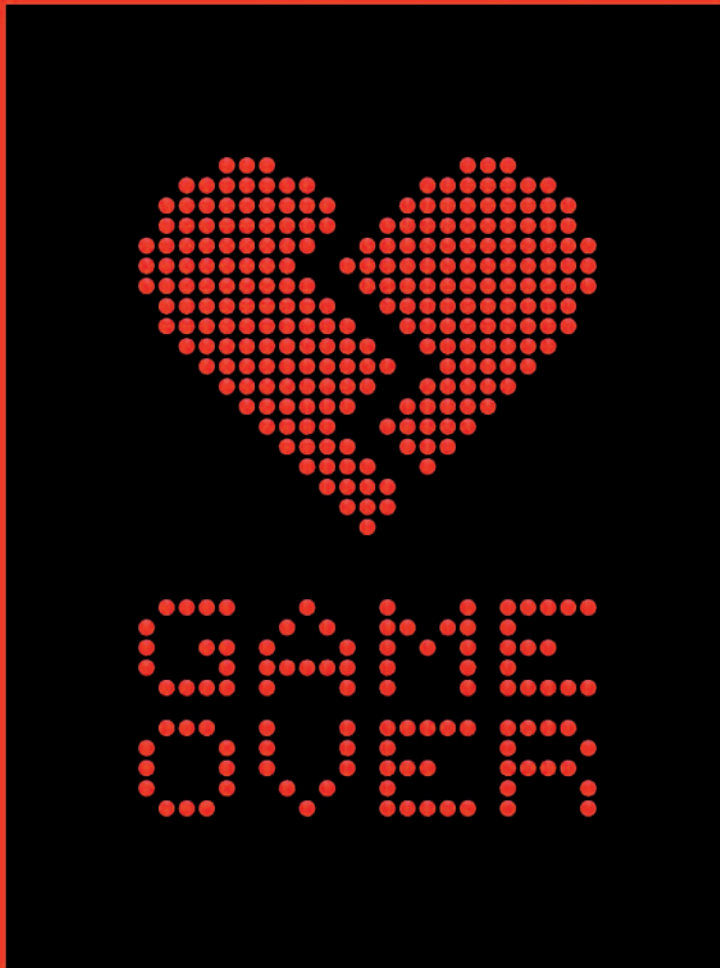


Divorcio digital

Pautas básicas de seguridad

JAVIER MORENO MAESTRO



Quien más o quien menos conoce a alguien en proceso de divorcio o ha experimentado en sus carnes el mismo. Es, sin duda, un asunto espinoso y complicado, no sólo a nivel sentimental, sino que supone el inicio de un largo y complejo proceso de reparto de bienes, batallas por la custodia de los niños, etc.

Pues bien, el mundo digital en el que vivimos viene a complicarnos un poco más la existencia.

Tengamos en cuenta que durante nuestra vida en pareja compartimos no sólo la hipoteca, los hijos y otros bienes, sino gran cantidad de contraseñas de servicios online, claves de operadores de telefonía, credenciales bancarias, etc. Por este motivo, si nuestra relación no acaba del todo bien, numerosas empresas de seguridad digital nos aconsejan tomar una serie de precauciones en el terreno digital, para evitar disgustos futuros como usurpa-

ciones de identidad, acceso fraudulento a cuentas bancarias o a cualquier tipo de servicios digitales.

En este sentido, Bruno Pérez, CEO de la empresa evidenciadigitals.cat y perito informático forense nos advierte, "Alguien que conoce nuestro DNI y tiene acceso a nuestra cuenta principal de correo electrónico, puede entrar prácticamente a todo nuestro universo digital." Por ello nos recomienda modificar todas nuestras contraseñas y números PIN para evitar problemas cuando iniciamos la separación de nuestra pareja.

De esta manera, disponer de las contraseñas de una cuenta de Google, puede resultar un arma muy peligrosa en manos de alguien que desea hacernos algún tipo de daño. Y es que, según este experto en seguridad informática, esto nos va a permitir acceder no sólo a gran cantidad de información privada, sino también a algo que puede resultar más peligroso, la ubicación GPS de nuestro teléfono móvil y, por tanto, a nuestra situación geográfica.

Otro peligro con el que nos podemos topar durante el proceso de divorcio es el de las tarjetas SIM clonadas por la ex pareja. Según Bruno Pérez, no suele ser muy frecuente, pero se ha encontrado casos en que antiguas parejas guarden tarjetas clonadas de sus ex. A través de esta tarjeta se puede obtener información sobre



llamadas recibidas y enviadas o tener acceso a los SMS de verificación que diferentes portales nos envían para comprobar nuestra identidad y efectuar operaciones online de cualquier tipo.

También hay que tener en cuenta otro posible agujero en nuestra privacidad y que nunca tomamos demasiado en serio, se trata de las redes wifi. De hecho, con unos mínimos conocimientos informáticos y la contraseña de red, se puede acceder a información sobre: búsquedas efectuadas, páginas consultadas y conversaciones de plataformas de mensajería. Por lo que sería fundamental cambiar la contraseña del propio router para evitar intromisiones no deseadas de nuestra ex pareja.

Muchos expertos en seguridad informática nos alertan también de un nuevo peligro a tener en cuenta. Se trata de los accesorios para teléfonos móviles como cargadores, cables, etc. Así Bruno Pérez ha constatado la existencia de numerosos accesorios de este tipo que albergan camuflados en su interior sencillos sistemas de rastreo por GPS o telefonía móvil o incluso cámaras espía. Muy retorcido pero totalmente posible.

No se trata de provocar una paranoia entre las personas que estén pasando por el proceso de ruptura, al igual que hay que tener en cuenta que no todas las ex parejas son un peligro potencial o van a tratar de hacernos pasar un mal rato. Son, según numerosos expertos, una serie de pautas básicas de seguridad digital, que más allá del terreno del divorcio podemos extender también a nuestro día a día. ■

