Publicado en Madrid el 13/02/2023

El 20% de los españoles ha conocido a su pareja en Internet

El 40% de los encuestados por Kaspersky en España usa o ha usado apps para ligar

Cupido tiene ya preparadas sus míticas flechas del amor apuntando a todos aquellos que desean encontrar pareja este San Valentín. Pero, desde hace tiempo, parece que el famoso querubín del amor se ha vuelto más tecnológico que nunca, ya que Internet se ha convertido en un gran aliado para conocer a otras personas. Tanto es así que 2 de cada 10 españoles han conocido a sus parejas a través de Internet. Así lo revela una encuesta1 realizada por Kaspersky, empresa global de ciberseguridad, a más de 2.000 personas en España. De ella también se desprende que el 40% usa o ha usado en alguna ocasión estas aplicaciones de citas 'online' para ligar. Además, el estudio indica que en Canarias, Ceuta y Comunidad de Madrid es donde más se recurre al uso de este tipo de plataformas. Por su parte, Asturias, Castilla León y Baleares son las que menos las utilizan.

Sin embargo, en lugar del amor, lo que muchas personas encuentran son estafas. Y es que, a medida que aumenta la actividad de los usuarios en estas aplicaciones, también pueden crecer los riesgos asociados a ellas. En particular, los expertos destacan que el doxing (proceso de recopilar y publicar los datos personales de una persona, a menudo como acto de venganza) es una de las principales amenazas que se encuentran los usuarios de estas apps de citas. De hecho, según otro estudio2 de Kaspersky, uno de cada siete usuarios españoles de aplicaciones de citas (14%) ha sido víctima de esta práctica, porque muchas de estas plataformas suelen requerir un registro a través de redes sociales, donde se alberga gran cantidad de fotografías e información personal.

El doxing no solo es una práctica que amenaza a los solteros y solteras que buscan el amor. Cada vez son más las parejas que, debido al alto nivel de confianza que tienen, renuncian a su privacidad y comparten el acceso a sus dispositivos para mostrar que no hay nada que esconder. Pero ¿qué puede ocurrir tras la ruptura? Algunas personas se vengan de sus exparejas publicando fotografías recopiladas a lo largo de la relación.

Los expertos de Kaspersky recuerdan que, además del doxing, el amor online también se enfrenta a otras amenazas. Por ello, comparten los principales términos relacionados con las formas de estafa o acoso en redes sociales y apps de citas:

Catfishing. Crear una cuenta o identidad falsa en redes sociales con el objetivo de engañar a otras personas para que compartan información personal o crean que están conversando con una persona o cuenta real.

Deepfake. Es una técnica de inteligencia artificial que permite crear vídeos falsos de personas que aparentemente son reales, utilizando algoritmos de aprendizaje y vídeos o fotografías ya existentes de personas reales. Es posible utilizarla para hacerse pasar por personas famosas, despertando el interés de la víctima.

Flamear. Lanzar mensajes hostiles o insultantes que no tienen la intención de ser constructivos, sino

que buscan establecer una posición de autoridad y/o superioridad.

Gaslight (luz de gas). Manipular la autopercepción de la otra persona para hacerla dudar de su propia realidad, su memoria, su percepción y/o su cordura. Puede incluso consistir en la escenificación de situaciones extrañas con el fin de desorientar a la víctima.

Gossip. En esta práctica se utilizan los programas de mensajería o las redes sociales para extender rumores. Además de los riesgos derivados de la falsedad de la información, extender estos rumores en Internet puede ser un detonante de conductas de ciberacoso.

Grooming. Acciones deliberadamente emprendidas por un adulto a través de Internet con el objetivo de ganarse la confianza y amistad de un menor de edad, creando una conexión emocional.

Sexting. Envío de contenidos de tipo sexual producidos de forma voluntaria por la propia persona emisora. Hay que ser cauteloso y enviar solo este tipo de contenidos a personas de confianza o evitar mostrar el rostro en las imágenes.

Stalkear. Forma de acoso y espionaje que consiste en monitorizar de forma compulsiva la actividad de una persona en las redes sociales.

En este sentido, cabe destacar que la probabilidad de que un usuario se vea afectado por estas amenazas puede depender de las medidas de seguridad implementadas en cada aplicación y de las vulnerabilidades que contenga. Concretamente, según un tercer estudio3 sobre las aplicaciones de citas más populares, 6 de ellas permitían averiguar la ubicación del usuario; 4 permitían averiguar el nombre real del usuario y encontrar sus cuentas en otras redes sociales; y otras 4 permitían interceptar datos enviados por la aplicación que podían contener información sensible.

Además, desde Kaspersky recomiendan seguir estos consejos:

En las redes sociales, no aceptar peticiones de amistad de personas que no se conocen.

No vincular Instagram (u otras cuentas de redes sociales) al perfil de la app de citas. Eso aporta demasiada información personal que puede ser utilizada de forma malintencionada. Incluso si ya se tiene configurado Instagram para una mayor privacidad y seguridad, hay más riesgo que beneficios en la vinculación de las cuentas.

No divulgar demasiada información personal en un perfil de citas, tampoco a alguien con quien solo se haya hablado por Internet. Los estafadores pueden aprovechar datos como apellido o lugar de trabajo para robar la identidad.

Acceder a sitios de citas fiables y mantener conversaciones a través de su servicio de mensajería. Los estafadores querrán cambiar rápidamente a los mensajes, redes sociales o al teléfono. Así, no constará que han pedido dinero en el sitio de citas.

Tomárselo con calma. Hacer preguntas a la presunta cita y fijarse en las contradicciones que hagan pensar que puede estar tratando de engañar.

Sospechar del exceso de elogios. Pegar el texto en un motor de búsqueda y comprobar si hay palabras que coinciden con las de sitios web que denuncian estafas románticas.

No tener una sensación de seguridad errónea porque "seas tú quien haya iniciado el contacto". Los estafadores irrumpen en las webs y aplicaciones de citas con perfiles falsos y esperan a que las víctimas acudan a ellos.

No enviar fotos comprometedoras a desconocidos en la red con las que podrían hacer chantaje en un futuro.

Interrumpir el contacto inmediatamente si se empieza a sospechar que el individuo es un estafador. Comunicarlo al sitio web o a la aplicación de citas en la que se le conoció.

No hacer clic en enlaces o descargar de las BIOS de los usuarios, tampoco en aquellos mensajes que no sean pertinentes en la conversación que se está teniendo.

Si se decide reunirse con la supuesta cita en persona, contárselo a la familia y amigos dónde se va a ir y quedar en un espacio público. No es recomendable viajar al extranjero para quedar con alguien a quien no se ha visto nunca.

No enviar dinero o tarjetas regalo ni revelar los detalles bancarios a alguien que se haya conocido en la red.

Utilizar una solución de seguridad para evitar que se haga clic en enlaces maliciosos que un estafador pueda enviar, además de evitar otras amenazas como virus, ransomware y ataques de phishing en general.

"Las aplicaciones de citas se han vuelto más seguras desde un punto de vista técnico en los últimos años, en particular en cuanto a la transferencia de datos. A pesar de ello, siguen representando un riesgo importante cuando se trata de exponer demasiada información personal de los usuarios, lo que los hace vulnerables a amenazas como el ciberacoso y el doxing", afirma Marc Rivero, Senior Security Researcher de Kaspersky.

Datos de contacto:
Mónica Iglesias
690 196 537

Nota de prensa publicada en: Madrid

Categorías: Nacional Sociedad E-Commerce Ciberseguridad