Guía para no ser estafado en San Valentín a través de aplicaciones de citas

13/02/2023

San Valentín es una fecha en la que muchos usuarios encuentran en aplicaciones de citas alguien con quien celebrar. Lo que se convierte en una oportunidad para que los ciberdelincuentes aprovechen para robar datos y dinero.

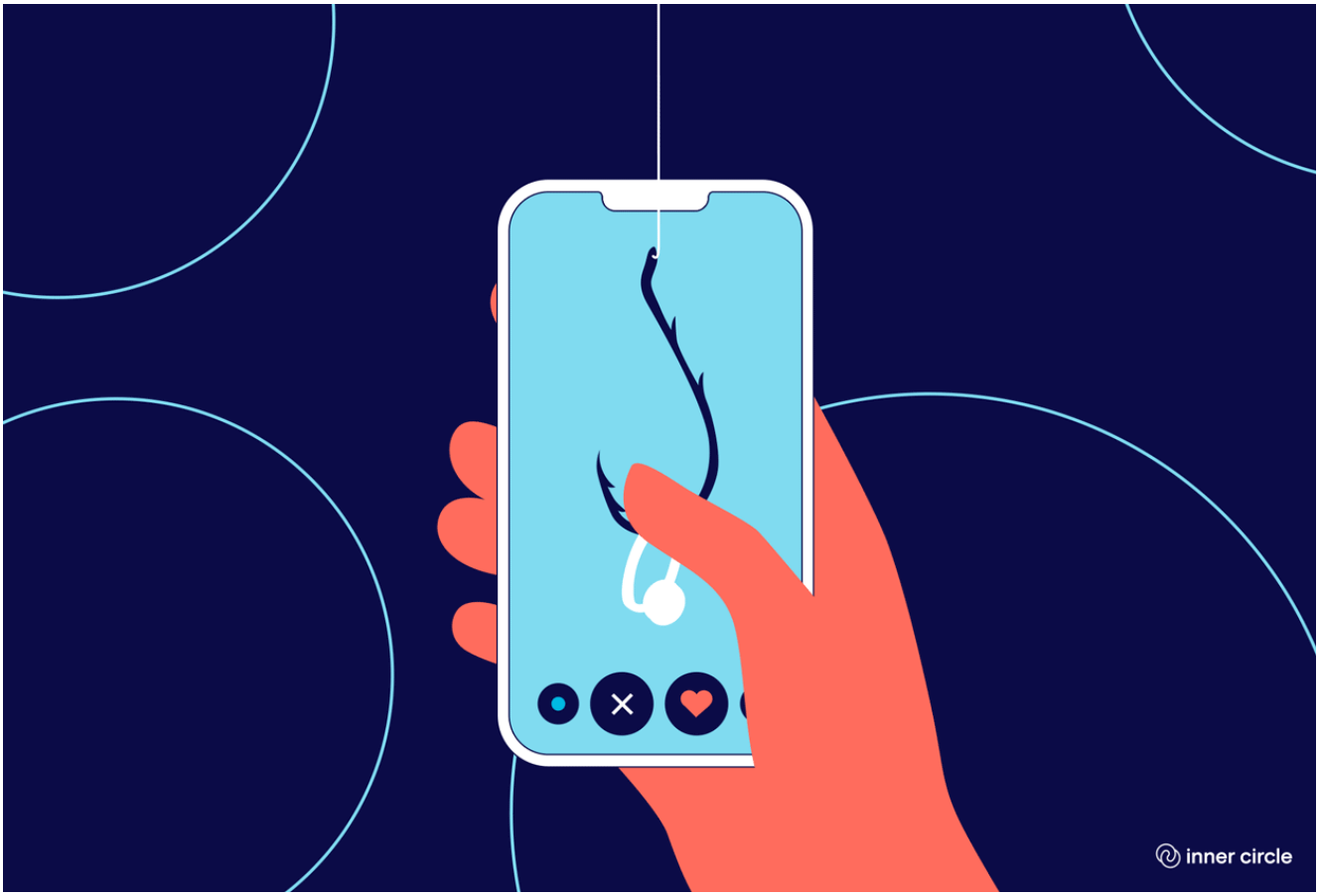
Estas situaciones no se dan solamente en casos en los que se concreta un encuentro físico, sino que, además, los atacantes tienen técnicas para tomar esa información de forma virtual, por medio de engaños.

Para entender mejor esta situación, hay unos tips para tener en cuenta, estar atentos y no dejarse llevar por la situación, arriesgando mucho más que el dinero.

Ciberataques en aplicaciones de citas

Un primero punto para tener en cuenta es el tipo de víctimas que buscan los delincuentes. **Kaspersky**, empresa de ciberseguridad, asegura que las personas con 50 años o más son las que más interés generan, especialmente si cuentan con bienes, inmuebles o fondos de pensión.

La misma compañía asegura que en el mundo el 15% de los usuarios han sufrido de algún ciberataque y que el 31% han sido contactados en algún momento por delincuentes que los intentan estafar.



Los delincuentes suelen pedir dinero o fotos para robar información de los usuarios.

A este panorama se le suma que, en 2016, la **Comisión Federal de Comercio de EE. UU**. recibió 11.235 quejas sobre estafas en relaciones y cuatro años después, ese número aumentó a 52.593

y las pérdidas financieras de estas estafas superaron los 300 millones de dólares en 2020 en ese país.

Así que el riesgo es latente, aún más en fechas como **San Valentín** en las que muchas personas buscan no estar solas, por lo que hay que tener en cuenta las modalidades más usadas para robar en las aplicaciones de citas:

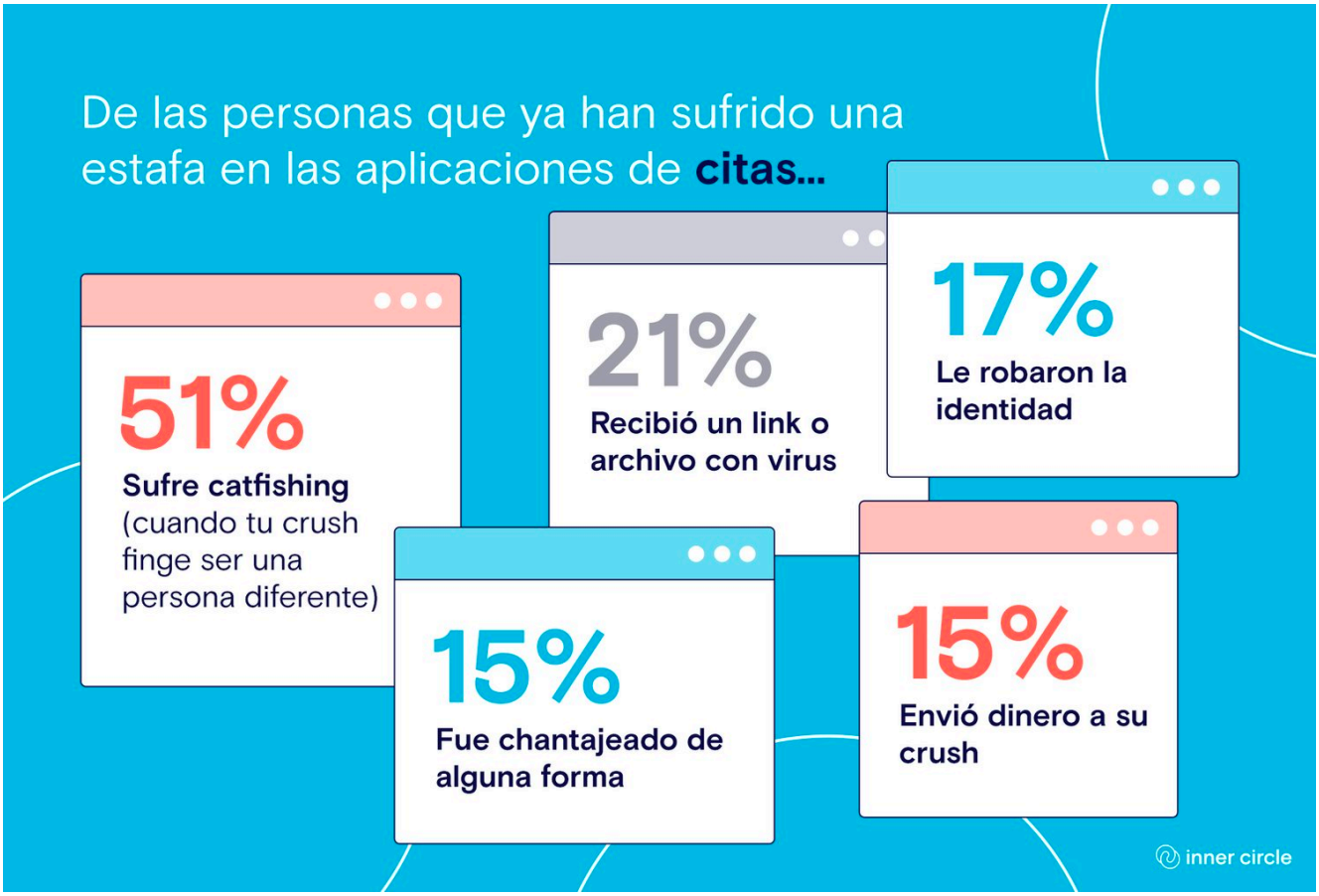
– Estafa romántica: el estafador crea una falsa identidad en Internet para ganarse la confianza de su víctima y obtener información que después le permita robar dinero y hasta extorsionar.

– Phishing: se puede identificar si el estafador intenta obtener información personal como datos bancarios, número de cédula, contraseñas, etc. Esto lo hacen mediante técnicas para ganarse su confianza como preguntas personales o enviando links.

– Sextortion: es un tipo de extorsión virtual en donde el agresor construye un vínculo emocional con la víctima, logra conseguir material fotográfico para amenazar a la víctima con hacer públicas sus fotos y videos a cambio de dinero.

A estas se suman otras dos, como la estafa de inversión, que consiste en influenciar a la otra persona en poner dinero para comprar acciones o en fondos falsos. Así como el engaño cripto pidiendo dinero digital, lo que les permite pasar más desapercibidos.

“Los estafadores de romance ponen mucho esfuerzo en construir una conexión emocional con sus víctimas, lo que a menudo significa que la gente baja la guardia y se vuelve menos vigilante ante los signos de una posible estafa”, afirmó **Masha Kodden,** CEO de **Inner Circle.**



Los delincuentes suelen pedir dinero o fotos para robar información de los usuarios.

Cómo evitar caer en estas estafas

Hay cinco puntos fundamentales para una persona no caiga en este tipo de trampas, que se dan en un contexto complejo para algunos porque hay sentimientos de por medio.

– Desconfiar de preguntas personales.

– Estar atentos a inconsistencias de sus discursos.

– No quiere encuentros personales o videollamadas.

– Peticiones de ayudas financieras.

– Los encuentros son solo en sitios privados

Pero hay otros puntos que **Kodden** ve también importantes, como por ejemplo que “sospeche si alguien a quien aún no ha conocido en persona de repente le cuenta una historia muy

emocional y le pide que le envíe dinero, no salga con alguien en secreto, siempre busque el consejo de sus seres queridos o amigos sobre las personas con las que está saliendo, y haga algunas investigaciones en línea para intentar validar a las personas con las que está hablando”.

Fuente: Infobae