PERIÓDICO	PÁGINA	FECHA	SECCIÓN
EL UNIVERSAL	16	21/04/2022	NACIONAL

Fraude, principal ciberdelito dirigido a adultos mayores

SSC detecta que son víctimas de acoso, extorsión y suplantación de identidad; inexperiencia con internet los hace vulnerables, alertan

PREVENCIÓN

De acuerdo con la Unidad de Policía Cibernética de la SSC, los delitos aumentaron durante la pandemia.

- **Llamadas telefónicas:** si los posibles ciberdelincuentes se intentan comunicar por este medio, es recomendable **no dejarse llevar por la información que solicitan**, en algunos casos haciéndose pasar por trabajadores de bancos, amigos o familiares para tener acceso a datos personales o financieros.
- **Navegando por internet:** las autoridades sugieren no caer en los precios bajos u ofertas y **corroborar datos y no abrir enlaces sospechosos** vía e-mail o SMS.

KEVIN RUIZ
—*metropoli@eluniversal.com.mx*

La Secretaría de Seguridad Ciudadana de la Ciudad de México (SSC) identificó que ciberdelincuentes han concentrado sus operaciones delictivas contra adultos mayores que no tienen mucha experiencia con el manejo de internet y las redes sociales, por lo que generan una interacción para cometer fraude, acoso, extorsión y suplantación de identidad.

Datos de la Unidad de Policía Cibernética de la SSC refieren que los delitos más comunes que involucran a personas mayores de 60 años son fraude, con 52%; 19% por acoso cibernético; 19% por extorsión, y 10% por suplantación de identidad.

La suboficial Fátima Colín explicó que el fraude, acoso y extorsión se hicieron más frecuentes con la pandemia de Covid-19, y desde entonces se muestra un aumento en estas prácticas.

Sobre todo el fraude, debido a la interacción de las personas en internet, la cual no es con precaución; sin embargo, los adultos mayores son los principales objetivos debido a que realizan una "ingeniería social", es decir, generan una comunicación que llega a ser personal.

"Con la situación de la pandemia aumentó [el fraude], y ahorita es poco tiempo para decir que ya disminuyó o se redujo, que ya desapareció este incidente, porque apenas hemos tenido poco tiempo en semáforo verde", aseguró la agente Fátima Colín en entrevista con EL UNIVERSAL.

El *modus operandi* de los cibercriminales consiste en generar un lazo con las víctimas para interactuar y obtener información personal, financiera o usuarios y contraseñas.

Se hacen pasar por personal de bancos, familiares o amigos, jefes y compañeros de trabajo, a veces mandan ligas vía mensajería SMS, en donde promocionan algún servicio, pero los enlaces que proporcionan son malignos.

En ocasiones realizan llamadas telefónicas para cometer estos delitos y, de acuerdo con la información de la policía capitalina, no les toma más de una llamada para obtener datos que los ayuden a delinquir.

FÁTIMA COLÍN
Suboficial adscrita a la Unidad de Policía Cibernética de la SSC

"Los cibercriminales utilizan la ingeniería social para interactuar con las posibles víctimas y obtener así la información"

Fátima Colín, adscrita a la Unidad de Policía Cibernética de la SSC, comentó que "los cibercriminales utilizan la ingeniería social para interactuar con las posibles víctimas y obtener así la información. ¿Cómo? Ganándose la confianza [de las personas] y que no se vea tan obvio que les están solicitando datos o información personal [para cometer un delito]".

Con esto, los ciberdelincuentes pueden obtener información como usuarios, contraseñas, concretar transferencias bancarias y, quizá, hasta redes sociales. En este sentido, la suboficial explicó que los principales objetivos que se han detectado son los adultos mayores, aunque en el mundo del internet cualquiera puede caer en manos de estos delincuentes.

"Depende de las víctimas si entabla conversación, quizá ella sola se expanda en hablar o en si el cibercriminal le solicita más y más información y la persona, pensando en que es verdad, le proporciona estos datos", dijo.

Ante esta alta incidencia, las autoridades recomendaron no dejarse llevar por la información que se solicita, en caso de que la interacción sea a través de llamadas telefónicas.

Para las ocasiones en donde se usa alguna página de internet, las personas no deben dejarse llevar por ofertas, precios bajos en artículos, corroborar los datos y, finalmente, no abrir enlaces que lleguen a enviar vía SMS o correo electrónico.

"Confío que con la alerta emitida por la SSC las personas sean más precavidas a la hora de navegar, pues existen muchas personas detrás que buscan delinquir", concluyó Colín. ●