PERIÓDICO	PÁGINA	FECHA	SECCIÓN
EXCELSIOR	5	17/08/2022	ARTÍCULOS Y COLUMNAS

Jorge Salazar, empleado de una tienda de autoservicio, tenía su cuenta en un reconocido banco nacional. Después de unos meses de abierta la cuenta, le llegó un correo electrónico pidiendo restablecer su contraseña, junto con otros requisitos que le parecieron normales en ese momento. Lo siguiente que supo —unos días después— es que le vaciaron los fondos de su cuenta bancaria. Acudió al banco para reclamar, donde le dijeron que investigarían.

Han pasado meses desde aquel episodio y el banco le da largas. Denunció el fraude en el Ministerio Público, quienes no sólo desconocían bien a bien qué hacer, sino que le pidieron dinero para poder avanzar en la "investigación".

Y es que **Jorge** no está solo. No obstante, las distintas medidas tomadas por las autoridades y los bancos, los fraudes cibernéticos han ido en aumento. De 2019 a 2020, los reportes de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) sobre fraudes se incrementaron 25% y han ido en aumentos similares desde entonces.

Se trata de un fenómeno que, de acuerdo con un estudio de Norton sobre cibercrimen en 24 países, cuesta a los gobiernos y ciudadanos alrededor de 114 mil millones de dólares al año en pérdidas. Este estudio estima que ataques de esta naturaleza u otras modalidades de cibercrimen son más grandes que el mercado negro de drogas en los 24 países estudiados.

El problema es cada vez más presente en México. Los delitos a través de internet son cada vez más frecuentes no sólo contra usuarios como **Jorge**, sino en contra de instituciones y empresas públicas y privadas.

Además del robo de activos, las instituciones son víctimas de hackeo de sus bases de datos o sabotaje de sus sistemas. En México, en años pasados, han sido atacados los portales de instituciones financieras, como BBVA y Banorte, o dependencias gubernamentales, como la Secretaría de la Defensa Nacional, el Cisen, la Presidencia de la República, la Secretaría de Seguridad Pública y el Congreso de la Unión.

En un reciente artículo de la organización Red de Defensa de los Derechos Digitales (R3D) se reporta cómo una base de datos con alrededor de 1.4 gigabites de información personal de clientes de Banorte se filtró en una página de internet. La base de datos incluye el nombre completo, Registro Federal de Contribuyentes, sexo, domicilio (calle, número, municipio, entidad y código postal), números telefónicos, correo electrónico y el balance de la cuenta.

En Europa y Estados Unidos, las leyes son claras para sancionar estos delitos. Existen sistemas policiacos y de investigación bien articulados que funcionan eficientemente en contra de estos delitos. Sin embargo, la realidad en México es que estamos poco preparados. Los ataques que han sufrido los portales de las instituciones públicas y privadas son una clara advertencia de los riesgos que significan para la seguridad este tipo de actividades. El Código Penal Federal no establece de forma clara estos delitos, cada vez más frecuentes.

Por ello, es cada vez mayor el número de usuarios o instituciones que sufren estos delitos. Bajo este escenario, llegaremos a un futuro no muy lejano en donde el mercado ilegal de bases de datos y fraudes cibernéticos será más lucrativo que el mercado de algunas drogas.

Si no hacemos algo ahora, **Jorge Salazar**

y miles de usuarios más estarán en el abandono ante este fraude oculto en todas sus modalidades.

El Código Penal Federal no establece de forma clara estos delitos, que son cada vez más frecuentes.