



Acceder a bases de datos de bancos o diferentes entidades, sin permiso, sustraer archivos de computadores, ingresar a redes sociales y correos ajenos y clonar tarjetas bancarias, son algunas de las modalidades de delitos informáticos que se presentan en el país y que según expertos de la Fiscalía van en aumento.

Pero para quienes hacen parte del Grupo de Delitos Informáticos, dependencia adscrita al CTI, todo parte de descuidos de las víctimas y de las grandes estructuras delincuenciales que hay alrededor de este tipo de hechos.

Para la Fiscalía, es necesario que los mismos usuarios prevengan las conductas que los afectan, para esto deben adoptar [costumbres](#) como la de sacar su dinero en máximo dos cajeros (deben ser siempre los mismos), para que la entidad bancaria tenga cómo hacerle seguimiento ante un eventual hurto. Así mismo, es importante cubrir con su mano al momento de digitar la clave, no aceptar ayuda de extraños y cambiar la contraseña mínimo una vez al mes.

Sin embargo, hay otro tipo de conductas delincuenciales que aunque no atacan el bolsillo, sí hacen mucho daño a la personas. Son la violación a sus cuentas de correo o de redes sociales. Allí muchas veces se cambian las claves y se envía información a nombre del afectado a los contactos o se publican contenidos que van en contra de su honra.

Entre las recomendaciones de la entidad investigadora, que dice que detrás de este tipo de hechos hay grandes [grupos](#) criminales que se alían con expertos en tecnología, está el buen manejo de los computadores y celulares. Las cadenas de correos como las religiosas en su mayoría contienen virus que al ser reenviadas se llevan consigo información personal. No se deben abrir el correos en los café internet o hacer transacciones bancarias a través de redes públicas como las encontradas en aeropuertos y centros comerciales.

También es importante, de acuerdo a los expertos, no contestar encuestas donde le requieran sus datos personales o escribirlos en rifas de almacenes (en caso de hacerlo le



deben explicar cómo serán guardados y protegidos) y menos [responder](#) mensajes electrónicos con su información a cambio de supuestos premios.

Es necesario que al pagar cuentas con tarjetas débito o crédito éstas no se pierdan de vista porque se pueden presentar clonaciones.

Otra de la modalidades que 'caza' incautos, es en los centro de pagos de [servicios](#) públicos manejados por delincuentes. Hasta allí, según las autoridades, llegan las personas con su dinero en efectivo y resulta que las cuentas son canceladas con tarjetas clonadas a otras víctimas y al momento de investigar quién aparece figurando en la factura, es vinculado al proceso. Por eso es necesario que los pagos sean en lugares conocidos y acreditados.

Según el Colegio Colombiano de Juristas, [Colombia](#) es el tercer país donde más se cometen delitos informáticos en Latinoamérica, después de Brasil y México. Así mismo, se calcula que 187 denuncias mensuales son interpuestas por fraude a los bancos.

La ley 1273 de 2009 que regula la [protección](#) de la información y de los datos, se ha fortalecido para conseguir penas entre cuatro y ocho años de cárcel a quienes cometan delitos informáticos.

A esto se le suma el agravante de utilizar medios electrónicos para dicho fin, lo que le puede dar hasta 12 años de prisión al infractor. Según la Fiscalía, esta conducta viene unida a delitos como el concierto para delinquir, ya que nunca una persona actúa sola.

La Fiscalía actualmente tiene 23 grupos que combaten los Delitos Informáticos en todo el país y que se divide en la parte forense e investigativa. Según dicha dependencia, en las capturas que han hecho como mínimo siempre son detenidas 15 personas.

Las víctimas

Este tipo de conductas delictivas no distinguen a sus víctimas, va desde una persona del común, a quien le pueden hurtar desde 500 mil pesos; hasta las empresas que en una sola



transacción le retiran más de 1.500 millones de pesos.

Los más afectados en los delitos contra la horra son los personajes famosos, como actores o cantantes. Pero la Fiscalía también es clara en señalar que el compartir la clave con la pareja también pone en riesgo a éstas, puesto que muchas veces las relaciones sentimentales se terminan de mala manera y por venganza publican información íntima.

Entidades como gobernaciones y hasta ministerios han caído en manos de los delincuentes, en donde se le han clonado las tarjetas de los empleados.

Lo que no se debe hacer

Utilizar para las claves fechas conocidas por demás personas como cumpleaños, aniversarios, el nombre de algún familiar o el número de la cédula, etc.

Escribir las contraseñas de los correos electrónicos y guardarlas bajo el computador o el teclado.

Escribir la clave de su tarjeta débito o crédito y pegarlas al respaldo.

Actualizar los datos personales de sus cuentas bancarias que lleguen por enlaces en internet, es necesario entrar a la propia pagina web de la entidad o ir personalmente a las instalaciones.

El acceder a una cuenta de correo electrónico o de redes sociales diferente a la suya, es considerado un delito, como también lo es instalar un software malicioso en el PC para expiar a alguien, así esa persona sea de su familia.

Se recomienda

Usar claves diferentes para cada correo o cuenta de banco. En el primer caso debe ser conformada por letras y número y mínimo ocho caracteres. Es necesario cambiarla



periódicamente y contener un signo especial, ya sea un asterisco, la letra numeral o el signo pesos.

Acceder en sitios seguros y no generar inicios de sección en los correos electrónicos de manera automática, así sea su propio computador.

No prestar su cuenta bancaria para que le consignen dinero que no sea el suyo.

Las zonas más afectadas

Una de las ciudades más afectadas por esta modalidad, según la Fiscalía, es Bogotá, por sus mismos nivel poblacional, pero también sufren el flagelo lugares como la Costa Caribe, Cali, Medellín, Pasto y la zona Andina, aunque ninguna parte del país se salva de este tipo de delincuentes.

FUENTE: Vanguardia