Hacia una necesaria guía práctica preventiva para la ciudadanía contra la delincuencia informática

Vicente Magro Servet

Magistrado de la Sala de lo Penal del Tribunal Supremo

Doctor en Derecho

Diario La Ley, Nº 9911, Sección Doctrina, 13 de Septiembre de 2021, **Wolters Kluwer**

ÍNDICE

Resumen

Análisis de la necesidad de que se elabore una Guía práctica de contenido preventivo para que los ciudadanos puedan conocer las distintas modalidades delictivas en materia informática y enseñarles qué no deben hacer, o en qué trampas no deben caer para evitar ser víctimas de delitos informáticos

- Comentario al documento Expone el autor la necesidad de que desde la Administración Pública se elabore una Guía de prevención para el ciudadano ante la delincuencia informática, que tanto daño está haciendo a los ciudadanos que, en su amplia mayoría, no disponen de los conocimientos para evitar ser víctima de los delincuentes informáticos que se aprovechan, precisamente, de esta ignorancia ante el cúmulo de posibilidades con las que los autores perpetran sus delitos. La gran potencialidad que están demostrando estos delincuentes fuerzan a empresas y Administración Pública a rearmarse ante los delincuentes informáticos para estar más por delante que por detrás

de ellos, dado el tremendo perjuicio económico que la falta de recursos de protección ante esta delincuencia puede provocarnos a todos. Pero resulta muy eficaz para reducir las altas tasas de delincuencia informática patrimonial enseñar a los particulares mediante una herramienta preventiva cómo deben actuar y qué deben evitar hacer en estos casos. Por ello, se ofrecen algunos consejos básicos que los expertos en seguridad informática recomiendan y que podrían ser trasladados a esta guía práctica preventiva y ser facilitada a la ciudadanía para combatir más eficazmente esta delincuencia.

I. Introducción

La tecnología ha supuesto un tremendo avance para la sociedad en muchas parcelas de la vida, pero está claro que en otras ha producido justo un efecto contrario. Por ejemplo, en la delincuencia informática la estadística nos demuestra los elevadísimos índices de esta modalidad delictiva que está causando estragos a nivel mundial, utilizando las bondades de las tecnologías, pero para delinquir y apoderarse de dinero de terceros, hacer compras con sus tarjetas y datos personales, apoderarse de datos informáticos y acceder a los personales de muchos ciudadanos para muy distintos fines.

En esta temática, cuando accedemos a los datos nos damos cuenta del volumen de los que están relacionados con los fenómenos delictivos que utilizan la tecnología como herramienta con la que cometer el ilícito penal. Así, en el VII Informe sobre Cibercriminalidad, correspondiente a la delincuencia informática se destaca que el aumento de la ciberdelincuencia viene propiciado por el elevado número de potenciales víctimas, ya que el número de usuarios a nivel mundial se cifra en 7.796.615.710. No existe delito en el que el número de víctimas sea tan elevado, y eso potencia la «dedicación» de los delincuentes en aprovecharse de las tecnologías. Sobre todo, a sabiendas de que son cuatro los datos o claves que sirven para facilitar la delincuencia informática, como son:

a. El general **desconocimiento de la mayoría de los usuarios de las tecnologías acerca de las trampas y estrategias** de los delincuentes informáticos para disfrazar su instrumento delictivo con apariencia de legalidad.
b. El **exceso de confianza de la mayoría de los usuarios** a la hora de facilitar sus datos y claves a quien se los reclama, para con ellos cometer el delito.
c. El **desconocimiento de los usuarios para poder detectar el fraude.**
d. La falta de una debida información pública a los ciudadanos acerca de las prevenciones que deben adoptar para evitar ser víctimas de un delito informático.

Pues bien, sobre estas cuatro ideas gira la base por la que los autores de estos delitos se aprovechan y valen para extender sus redes delictivas actuando, además, de la aparente impunidad de un ordenador que utilizan para operar su *modus operandi delictivo informático.*

Resulta evidente que las estadísticas de la delincuencia informática sean tan elevadas, habida cuenta que con ese volumen de usuarios, las potenciales víctimas que no guardan ninguna medida de prevención permite un caldo de cultivo muy abonado que facilita el ataque delictivo informático.

Es, precisamente, la ausencia de conocimientos informáticos, por un lado, de la mayoría de los consumidores, y la ausencia de un canal de información que les aconseje cómo actuar preventivamente, por otro, es lo que hace extender el volumen de delincuentes informáticos ante el «efecto llamada» que produce y provoca esa ausencia de medidas de precaución de los ciudadanos ante la confianza de que todo lo que recibe está «limpio» de cualquier intención delictiva. El «conocimiento» en la mayoría de los casos se está adquiriendo *a posteriori* cuando las víctimas ya lo son y han sufrido ataques a sus cuentas, o por operaciones informáticas en las que han sido estafados.

Con una mayor difusión de una publicidad sobre las distintas formas de actuar con la que opera la delincuencia informática se podría extender una política de potenciar la prevención en la ciudadanía

La idea que planteamos es que con una mayor difusión de una publicidad sobre las distintas formas de actuar con la que opera la delincuencia informática se podría extender una política de potenciar la prevención en la ciudadanía a la hora de no caer tan fácilmente en las trampas de esta clase de delincuencia, porque con una mayor eficacia preventiva descenderían las víctimas de estos hechos y no se extendería el mensaje que manda la excesiva confianza y desconocimiento que los ciudadanos tienen cuando realizan compras en internet, o facilitan sin control alguno sus datos a terceros desconocidos por ellos.

Así, esta Guía práctica de medidas preventivas de los ciudadanos ante las prácticas que están llevando a cabo los delincuentes informáticos sería un gran paso que reduciría exponencialmente estas cifras estadísticas de este tipo de delincuencia si la ciudadanía conoce mejor cómo actúan estos delincuentes y toma medidas de autoprotección, ya que en estos casos la protección es personal, y una mayor y mejor información de estos casos reduciría esta delincuencia tan dañina para la economía mundial y la particular de muchos ciudadanos.

Resulta interesante destacar que a nivel internacional para poder tener mejor control en cuanto este ámbito y definir el marco de referencia en el campo de las tecnologías y los delitos para la Unión Europea, en noviembre de 2001 se firmó en Budapest el «Convenio de Ciberdelincuencia del Consejo de Europa», el cual se planteó, y tuvo como objetivo, la protección integral de los sistemas que utilicen tecnologías de información, prevención y sanción de cualquier delito cometido contra dichos sistemas o los cometidos a través de estas tecnologías.

Pero no es suficiente determinar y fijar cuál es la delincuencia informática, secuenciarla, incluirla en los textos penales de la UE para dotar de tipicidad a las conductas delictivas y respetar el principio de legalidad para poder perseguirlas. Porque sabemos que siempre es más eficaz que la represión penal actuar desde la prevención ante el delito. Y en este campo de delincuencia tecnologizada, donde el desconocimiento ciudadano es muy extenso, y la sofisticación a la hora de cometer el delito es cada vez mayor, se nos presenta como urgente y necesaria esta guía de prevención ante el delito informático a la que se pueda dotar de la mayor publicidad para que pueda llegar a todos los hogares españoles.

II. *Tipos de delitos informáticos*

Hay que destacar, en primer lugar, que las estafas informáticas representan más del 80% de los delitos informáticos, según los últimos informes anuales publicados por la Fiscalía General del Estado, y es respecto a este delito sobre el que habría que hacer un importante esfuerzo divulgador en prevención para alertar a la ciudadanía acerca de cómo autoprotegerse. Porque el desconocimiento de quién está detrás de internet para hacernos daño y sus malignas intenciones es lo que más nos debe preocupar y lo que más se debe trasladar a los ciudadanos para que conozcan cómo actúan, cómo se nos puede engañar, cómo debemos actuar para ello, y actualizarnos constantemente acerca de las nuevas modalidades que utilizan, por cuanto resulta claro que el delincuente informático está en permanente actualización.

Así, a la hora de elaborar una Guía de prevención de la delincuencia informática es preciso llevar a cabo una relación de cuáles son los delitos informáticos que se están cometiendo y sanciona nuestro Código Penal a lo que debemos añadir las últimas adiciones incluidas en la reciente LO 8/2021, de 4 de junio de protección de la infancia y la adolescencia frente a la violencia.

Exponemos la clasificación de estos delitos según la página de la Brigada de Investigación Tecnológica de la Policía Nacional Española (www.policia.es)

1. Ataques que se producen contra el derecho a la intimidad:

Delito de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos. (Artículos del 197 al 201 del Código Penal)

2. Infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor:

Especialmente la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas. (Artículos 270 y otros del Código Penal.

3. Falsedades:

Concepto de documento como todo soporte material que exprese o incorpore datos. Extensión de la falsificación de moneda a las tarjetas de débito y crédito. Fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad. (Artículos 386 y ss. del Código Penal.

4. Sabotajes informáticos:

Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos. (Artículo 263 y otros del Código Penal.

5. Fraudes informáticos:

Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito. (Artículos 248 y ss. del Código Penal.

6. Amenazas:

Realizadas por cualquier medio de comunicación. (Artículos 169 y ss. del Código Penal.

7. Calumnias e injurias:

Cuando se propaguen por cualquier medio de eficacia semejante a la imprenta o la radiodifusión. (Artículos 205 y ss. del Código Penal .

8. Pornografía infantil:

Entre los delitos relativos a la prostitución al utilizar a menores o incapaces con fines exhibicionistas o pornográficos.

La inducción, promoción, favorecimiento o facilitamiento de la prostitución de una persona menor de edad o incapaz. (art 187)

La producción, venta, distribución, exhibición, por cualquier medio, de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido. (art 189)

El facilitamiento de las conductas anteriores (El que facilitare la producción, venta, distribución, exhibición...). (art 189)

La posesión de dicho material para la realización de dichas conductas. (art 189)

A estas es preciso añadir los nuevos delitos informáticos añadidos en la Ley orgánica 8/20201, de 4 de junio de protección a la infancia:

«La distribución o difusión pública a través de Internet, del teléfono o de cualquier otra tecnología de la información o de la comunicación de contenidos específicamente destinados a promover, fomentar o incitar al suicidio de personas menores de edad o personas con discapacidad necesitadas de especial protección» (art. 143 bis CP).

«La distribución o difusión pública a través de Internet, del teléfono o de cualquier otra tecnología de la información o de la comunicación de contenidos específicamente destinados a promover, fomentar o incitar a la autolesión de personas menores de edad o personas con discapacidad necesitadas de especial protección» (art. 156 ter CP).

«La distribución o difusión pública a través de Internet, del teléfono o de cualquier otra tecnología de la información o de la comunicación de contenidos específicamente destinados a promover, fomentar o incitar a la comisión de los delitos previstos en este capítulo (delitos relativos a la prostitución) y en los capítulos II bis (delitos de abusos y agresiones sexuales a menores de 16 años) y IV (delitos de exhibicionismo y provocación sexual) del presente título» (art. 183 bis CP)

«La distribución o difusión pública a través de Internet, del teléfono o de cualquier otra tecnología de la información o de la comunicación de contenidos específicamente destinados a promover o facilitar, entre personas menores de edad o personas con discapacidad necesitadas de especial protección, el consumo de productos, preparados o sustancias o la utilización de técnicas de ingestión o eliminación de productos alimenticios cuyo uso sea susceptible de generar riesgo para la salud de las personas» (Art. 361 bis CP)

Se han incluido, pues, en la LO 8/2021, de 4 de junio) estos tipos penales dirigidos a sancionar estas conductas tendentes a influir en la toma de decisiones de menores y personas con discapacidad para evitar que la mala fe de algunas personas les lleve a cometer actos que le causen un daño personal. No se trata en estos casos de la consecución de un beneficio económico para los delincuentes, sino de causar el mal por el mero placer de causarlo mediante la ejecución de mensajes que van dirigidos a doblegar la voluntad del sujeto pasivo y llevarles a cometer diversos

actos fijados en los tipos penales, prevaliéndose el autor del déficit personal de la víctima que le desprotege ante la maldad del mensaje del autor y su maliciosa intención de causarles daño.

En estos casos, la prevención opera sobre sus padres o tutores para evitar un libre uso de internet cuyo descontrol facilite a los autores llevar a cabo sus conductas de llegar a sus víctimas para convencerles de que ejecuten los actos que les incitan por cualquier canal de internet. La política de prevención debe ir dirigida en estos casos a los encargados de tutelar a los posibles sujetos pasivos de estos hechos, por lo que en la Guía de prevención debe existir un apartado específico para estos delitos y su dirección a padres y tutores,

Del mismo modo, también es preciso incluir la referencia al delito de sextorsión on line. ¿Qué es este delito?

Se trata de una forma de explotación y chantaje sexual en el que una persona es extorsionada por el autor del delito que por un virus gusano introducido en un correo electrónico ha accedido al ordenador de su víctima, y, por ello, si esta tiene fotos personales comprometidas aquél va a poseer imágenes suyas de índole sexual. Esta técnica de extorsión suele ser empleada en los servicios de mensajería instantánea, redes sociales o chats, y lo que hacen es extorsionar a sus víctimas para que tengan sexo on line con los autores, lo que constituye un delito contra la libertad sexual.

Los autores del delito advierten a las jóvenes de que, o tienen conductas sexuales con ellos on line, o difundirán sus imágenes en internet

Los autores advierten a las jóvenes de que, o tienen conductas sexuales con ellos on line, o difundirán sus imágenes en internet. Por ello, hay que alertar a estos jóvenes para que no caigan en trampas, o errores, on line que puede llevar a extorsionadores a cometer este delito contra la libertad sexual de abusos o agresiones sexuales on line cometidos por la extorsión; de ahí su nombre.

Podemos destacar, para poner un ejemplo, la sentencia Tribunal Supremo, 377/2018 de 23 Jul. 2018, Rec. 10036/2018, sobre sexo virtual destacando que se puede condenar por delito contra la libertad sexual sin precisar contacto directo si se ejercita la intimidación on line para tener sexo por esta vía sin ese contacto directo y así se condenó en este caso concreto por llevarlo a cabo con varias víctimas. Se utilizan, así, herramientas informáticas para apoderarse subrepticiamente de archivos personales con contenido sexual de las víctimas, para atermorizarlas con su difusión y conseguir así que éstas accedieran a realizar conductas sexuales que grabó en su ordenador.

Por ello, en la Guía de prevención de la delincuencia informática debe constar un apartado específico dirigido a padres e hijos advirtiendo de que estos hechos están ocurriendo en la actualidad y de que tengan sumo cuidado de no abrir mensajes de desconocidos o de la descarga de archivos que no sepan su origen, para evitar la entrada de virus que puedan permitir a terceros delincuentes acceder a los archivos personales del ordenador de la víctima para acabar extorsionándoles.

III. *Consejos de carácter preventivo para evitar ser víctima de la delincuencia informática*

La plasmación de la herramienta de la que estamos tratando tiene diversas ideas expuestas por distintos expertos en delincuencia informática a la hora de ofrecer consejos de sumo interés para tomar medidas precautorias. No obstante, la eficacia de esta Guía práctica preventiva se manifiesta y muestra su mayor eficacia cuando más sencillo sea la plasmación en la misma de cómo se opera en la delincuencia informática y qué medidas de autoprotección debe llevar a cabo la ciudadanía. Y ello debe llevarse a cabo por la Administración Pública de una manera sencilla y fácil de llegar y que sea aprendido por los ciudadanos con pocos o nulos conocimientos de la informática; incluso, con dibujos y mensajes sencillos, ya que debemos tener en cuenta que hablamos de una Guía práctica que pueda ser utilizada por todos, no solo por los que tienen algún conocimiento informático y esto les sirva de complemento.

Por ello, de lo que se trata ahora es de elaborar una herramienta sencilla, fácil de manejas, que pueda conocerse su contenido con gráficos y de ágil comprobación de lo que se debe hacer y lo que no se debe hacer.

Mientras tanto, veamos los tipos de consejos que los expertos (1) están dando a la hora de prevenirse los usuarios frente a la delincuencia informática.

1. *Medidas básicas de seguridad a aplicar*

1. **Cambiar las contraseñas periódicamente,** haciéndolas cada vez más complicadas: Tener la misma contraseña para todo es un riesgo, ya que si descubren una, tendrán acceso a todas. Debe ser imprevisible y se debe cambiar cada poco tiempo.

2. **Cerrar sesión en todas las cuentas** al terminar de utilizarlas: sobre todo si el ordenador es de uso compartido.

3. **Instalar un antivirus**: para prevenir ataques de malware, es fundamental en un ordenador.

4. **Utilizar un firewall o cortafuegos**: para acceder de forma segura a Internet.

5. **No hacer transacciones en redes públicas**: si es necesario, entonces utiliza servidores VPN de red privada más segura o páginas https.

6. **Realizar copias de seguridad**: respalda tu información y evita pérdidas importantes de datos.

7. **Desconectar Internet cuando no lo necesites**: para evitar que de forma secreta traten de entrar a tu red.

2. *Medidas complementarias (2)*

1. Controles de acceso a los datos más estrictos

2. Proteger el correo electrónico. utilizar filtros antispam y sistemas de encriptado de mensajes, para asegurar la protección y privacidad de toda esa información.

Ahora bien, estas medidas, aunque necesarias, requieren de unos conocimientos informáticos que no todos los usuarios tienen, y con independencia de que deberían ser incluidos en esta Guía práctica para que sea completa y llegue a todos los ciudadanos, tanto los que tienen conocimientos informáticos como los que no los poseen, la idea giraría más sobre un contenido más asequible y que se extendiera también, y sobre todo, en relación al usuario medio sin conocimientos y que acceden a internet para compras, acceden a sus cuentas on line, o usan su correo electrónico de forma habitual, tres modalidades que son utilizadas con gran frecuencia en la delincuencia informática.

3. *Medidas de prevención con respecto al uso del correo electrónico*

Por eso, para estos usuarios, quizás, sea más eficaz la plasmación en una Guía práctica preventiva de los siguientes consejos (3):

De esta manera, *Softzone.es* da los siguientes consejos que sí son muy prácticos para el usuario medio-bajo on line.

1. No abrir mensajes desconocidos: Recibimos correos de multitud de fuentes, muchas de ellas conocidas, pero no todas. Es por ello que debemos desconfiar de aquellos correos que nos llegan de contactos que no conocemos o que nos resultan extraños. Lo mejor que podemos hacer llegado el caso, es marcarlos como spam.

2. Cuidado con los ficheros adjuntos: Uno de los grandes peligros de los correos son los adjuntos que llegan con los mismos. Estos son ficheros que en su nombre puede poner cualquier cosa, pero en realidad ser un archivo malicioso. Es por ello que normalmente debemos desconfiar de todos los adjuntos, tanto de contactos conocidos como desconocidos. Antes de abrir un adjunto del que tengamos sospechas, es mejor contactar con quien nos lo haya enviado para asegurarnos de que es un archivo fiable.

3. Desconfiar de los enlaces a ofertas absurdas: Muchas veces nos llegan correos de sorteos, premios o regalos que nos pueden resultar un tanto sospechosos. De hecho, estos vienen acompañados de enlaces a sitios web igualmente sospechosos para que pinchemos y, en ocasiones, nos lleven directamente a sitios maliciosos. Esto es algo que, como os podréis imaginar, también debemos evitar a toda costa, ya que suelen ser engaños en los que no debemos caer.

4. No enviar nunca contraseñas o datos personales: Otro punto que debemos tener en cuenta es que ninguna entidad seria nos va a solicitar nunca datos privados como una contraseña o clave de acceso, por correo. Al hablar de entidades serias nos referimos al banco, Hacienda, etc. Por tanto, si nos piden datos de acceso a plataformas por correo, lo más probable es que sea falso.

En efecto, muchos de los delitos informáticos que sufren los ciudadanos vienen por la recepción de correos electrónicos que se reciben y que no son detectados como sospechosos, y sobre los que muchos usuarios no aciertan ni a pensar que son una trampa para que caiga el usuario. De ahí que la urgencia de esta herramienta, y que se publicite por la Propia Administración Pública, sea un tema de primera necesidad, a fin de que cuando un ciudadano recibe mensajes con citas tales como «pinche aquí» «facilite sus datos o se les bloqueará su cuenta corriente», «Debe pagar una multa adjunta» y similares no sean aceptados y cumplimentados por tratarse de un fraude.

4. *Medidas de seguridad de la banca*

De suyo, la banca ya está informando constantemente a sus clientes que ellos nunca piden los datos por correo electrónico, ni contraseñas, ni datos personales, a fin de que los clientes no caigan en estos errores de facilitarlos a terceros desconocidos o aceptar archivos o entrar en aplicaciones que se proponen y que permiten al delincuente acceder al ordenador de la víctima.

La delincuencia informática por el acceso a las cuentas corrientes de los clientes es uno de los delitos informáticos más extendidos, precisamente por la falta de prudencia, cuidado y vigilancia de los ciudadanos que caen en las trampas y redes que les tienden los delincuentes con mensajes de alertas de perder sus cuentas, o exigirles datos. Las entidades bancarias constantemente llevan a

cabo políticas de consejos, pero es precisa una mayor publicidad, no solo de la banca, sino que por medio de la Administración Pública central se elabore este manual que englobe los ataques de los delincuentes informáticos a los ciudadanos en todas y cada una de las modalidades delictivas de los delitos informáticos. Y realizado con un mensaje claro y directo entendible por cualquier persona, ya que si se utiliza un lenguaje técnico la mayoría de los que no comprenden la terminología anglosajona que se suele utilizar en estos casos por los expertos en seguridad informática no va a ser entendida por una gran parte de las potenciales víctimas.

Las medidas de seguridad pueden empezar por conocer lo que hay y cómo pueden engañarnos. Así, podemos destacar los consejos que facilita Lisainstitute (4) Veamos:

A) *Phishing*

Las campañas de phishing, las cuales consisten en enviar correos electrónicos, whatsapp, mensajes en redes sociales o SMS de forma masiva, suplantando a una entidad (en este caso, bancaria).

En ellos, se incluye un enlace fraudulento cuyo objetivo es dirigir al usuario a un sitio web falso y, así, robar sus credenciales y datos personales. Entre los datos personales del cliente destacan: los nombres de usuario, las contraseñas y los números y «pines» de tarjetas.

Dado que es muy común que el phishing esté relacionado con una suplantación de identidad, ya sea como causa o consecuencia del mismo, Lisainstitute recomienda lo siguiente en los casos de suplantación de identidad:

Los pasos a seguir si te han suplantado la identidad en Internet son los siguientes:

a. Comprobar si te han robado o has perdido tu documentación o tarjetas de débito o crédito. Paralelamente y de forma preventiva dar de baja tus tarjetas bancarias.
b. Si sigues teniendo acceso, cambiar todas tus contraseñas, tanto en las páginas web que te han suplantado, como en el resto de perfiles o cuentas de correo electrónico.
c. Realizar capturas de pantalla sobre las evidencias de la suplantación.
d. Imprimir las capturas de pantalla sin borrar las capturas originales.
e. Dirigirte a un notario o a una empresa que certifique el contenido del perfil o de la página web suplantada para que dé fe de lo ocurrido (esto debes hacerlo solo en caso de que quieras tomar medidas legales y llegar al fin del asunto)
f. Denunciar el perfil desde la página web donde se ha suplantado tu identidad para que lo investiguen y pongan las medidas oportunas. Si quieres saber cómo actuar ante

suplantaciones en Facebook, Linkedin, Twitter o Instagram al final de este artículo te lo explicamos.

g. Ir a la Policía para denunciar la suplantación de identidad online y, en su caso, el robo o desaparición de tu documentación.

h. Avisar a tus contactos mediante una publicación o mensaje informándoles que te suplantaron la identidad, para que no abran ni hagan clic en ningún mensaje ni archivo que les hayas enviado anteriormente.

i. Sin embargo, si «solo» han utilizado tus datos bancarios para realizar compras fraudulentas debes:

Anular la tarjeta de manera inmediata.

Realizar la denuncia a la Policía.

Acudir con la denuncia a tu entidad bancaria para solicitar la devolución del importe defraudado.

B) *Los enlaces sospechosos*

Una de las técnicas más comunes entre los hackers y los estafadores es enviar correos electrónicos con enlaces sospechosos, los cuales piden que se verifique la identidad o ingresar determinada información de la cuenta. Un enlace sospechoso es aquel que, aparentemente, es fiable, pero cuando se pincha sobre él, redirige a una página falsa que parece ser real o que incluye malware. Por eso se recomienda por Lisainstitute que hay que acceder directamente introduciendo la página web del banco desde tu navegador web, sin hacer clic en ningún enlace, especialmente si el enlace es HTTP (identidad web no validada), en vez de HTTPS (identidad validada).

C) *Los ciberataques de Ransomware*

El ransomware es un tipo de malware, cuyo objetivo es conseguir el control de un equipo (ordenador o smartphone) para cifrar el acceso al mismo y/o sus archivos o discos duros.

El usuario podrá acceder de nuevo a su dispositivo e información a cambio de una condición que suele ser el pago de un rescate. El acceso a tu dispositivo y los archivos que él contiene pueden volverse totalmente inaccesibles a no ser que se pague el rescate.

Según Incibe, los cinco consejos que debes seguir para evitar ser víctima de cualquier tipo de fraude son los siguientes:

No abrir ningún correo electrónico que desconozcas y eliminarlos *ipso facto*.

Desconfiar de cualquier documento, aunque provenga de conocidos.

Comprobar que los enlaces proceden de contactos conocidos y que, además, son correctos.

Para evitar ser víctimas de Ransomware se debe actualizar tanto el antivirus como el sistema operativo de los equipos informáticos

Actualizar tanto el antivirus como el sistema operativo de los equipos informáticos.

Utilizar contraseñas complejas, nada de claves simples y fáciles de recordar.

D) *Consejos para operar con cuentas bancarias de forma segura*

Se destacan por Lisainstitute los siguientes:

a. Claves únicas para operar en banca on line. Es importante seleccionar un nombre de usuario y una contraseña que sean fáciles de recordar, pero que a su vez sean complejas de descifrar.

b. Utilizar antivirus en todos los dispositivos

c. La autenticación de doble factor (2FA o TFA) es un modo robusto de identificarse en el que se utilizan dos factores que aporta el usuario: algo que sabe (como puede ser una contraseña) con algo que tiene (como puede ser un teléfono o un token), o con algo que es (como puede ser una huella dactilar).

Para seguridad bancaria se suele utilizar el envío de un SMS al teléfono que consta que está asociado a dicha cuenta bancaria y que, se supone, que solo tiene acceso al mismo el propio usuario.

d. Acceder a la cuenta bancaria desde una red segura

e. Desactivar el bluetooth

f. Verificación periódica de la cuenta bancaria desde una ubicación segura. En caso de notar alguna actividad sospechosa ha de notificarse al banco de inmediato. Existe un período de días máximo, diferente en cada banco, para reclamar cualquier cargo anómalo o robo de dinero.

g. Muchos bancos ofrecen la posibilidad de notificar a sus clientes cualquier actividad en sus cuentas, ya sea a través del correo o por mensaje de texto. Merece la pena registrarse a estas alertas porque el usuario se sentirá más seguro y protegido al estar informado de lo que ocurre en todo momento.

h. Actualmente, los navegadores de internet como Google Chrome o Firefox ofrecen una gran suma de facilidades, entre las que destaca el inicio de sesión automático.

A priori, puede parecer que no tener que recordar la contraseña y entrar de manera directa es una gran idea. Sin embargo, es fundamental desactivar esta opción en el caso de los sitios web para banca online.

i. Para proteger el dispositivo móvil también es recomendable hacer uso de una capa adicional de seguridad a través de un PIN o una identificación de huella digital.

j. 7 consejos de seguridad para la banca online

Accede a la banca online mediante tu navegador y no a partir de enlaces o correos electrónicos.

Verifica que la URL es HTTPS y que al lado (parte superior del navegador) aparece un candado cerrado. Eso determinará la autenticidad del sitio web.

Cambia la contraseña de acceso de forma periódica. Además, ha de ser compleja, añadiendo diferentes caracteres, números y letras minúsculas/mayúsculas.

Ten siempre actualizado el navegador y el sistema operativo.

Evita llevar a cabo operaciones en ordenadores públicos y a través de redes públicas.

Recuerda que los bancos nunca solicitan información personal a través del correo ni el teléfono.

Cierra la sesión tras realizar las operaciones o al retirarte del ordenador, aunque sea solo un momento.

k. Lista de 10 consejos de seguridad al utilizar tarjetas bancarias en Internet

Desconfía de ofertas sorprendentes o exageradas: si suena demasiado bien, lo más probable es que sea un engaño.

Antes de comprar, investiga la página web o a la empresa en busca de opiniones o referencias.

Si te llega una oferta a través de WhatsApp, SMS, email, un anuncio en una red social o una ventana emergente, no hagas clic. Accede directamente desde el navegador a la empresa que ofrece ese producto y servicio para informarte y, si te interesa, comprarlo.

Nunca hagas clic en una ventana emergente con una oferta, multa o premio, haciendo clic puedes instalarte un programa malicioso.

Por sistema, desconfía de cualquier enlace que no sea «https://...», ya que eso implica que no dispone de certificado digital confiable.

Siempre que sea posible, compra en páginas web de empresas de ámbito nacional: la mayoría de los fraudes y las estafas se producen en empresas extranjeras a las que resultará muy difícil reclamar o denunciar e incluso investigar para la Policía. Puedes comprobar de dónde es la empresa en los «Términos y Condiciones» o en el «Aviso legal» que suelen estar a pie de página.

No introduzcas tus datos personales o bancarios utilizando un wifi público gratuito o abierto: paga siempre desde una conexión segura a Internet, a poder ser de tu titularidad y a quien solo tú tengas acceso.

Paga desde un dispositivo seguro: que tenga las últimas actualizaciones del sistema operativo y con antivirus y firewall actualizados y activados.

Si se paga con la tarjeta bancaria, es más probable que se recupere el dinero, ya que la mayoría de los bancos tienen un seguro de fraude.

Si sospechas de un intento de fraude, informa rápidamente a la policía para que lo investigue y evite que otras personas caigan en la estafa.

I. 7 consejos de seguridad para operar en el cajero automático del banco

Comprueba que no hay ningún tercero extraño alrededor antes de llevar a cabo cualquier tipo de operación.

No tengas escrita la clave de acceso y que no la sepa nadie más. Por algo es secreta, personal e intransferible.

Ten cuidado al escribir la clave y tapa el teclado con la mano para impedir que sea vista, especialmente porque en ocasiones se instalan cámaras espía en los laterales o partes superiores de los cajeros automáticos.

No aceptes la ayuda de ningún tercero mientras se realizan transacciones con la tarjeta.

Fíjate en las novedades reportadas por el banco a través de la pantalla del cajero. Las entidades bancarias nunca informan mediante avisos o carteles.

Si por alguna razón has de irte del cajero automático sin haber finalizado la transacción, anula la operación antes.

Destruye los comprobantes de las operaciones antes de tirarlos a la basura y, a poder ser, tíralos en una basura que esté alejada de la sucursal bancaria.

II. 7 consejos de seguridad al utilizar tarjetas bancarias en comercios

No debes entregar la tarjeta bancaria, la tarjeta debes acercarla o pasarla tú mismo por el datáfono. Si la entregas, no debes en ningún momento perderla de vista.

No permitas que introduzcan o pasen la tarjeta por ninguna máquina distinta del datáfono.

Si su tarjeta es de chip evita que la deslicen por la banda magnética del datáfono.

Si la tarjeta es de chip, evita que la deslicen por la banda magnética del datáfono.

En caso de extravío o robo, avisa a la entidad financiera de inmediato y realiza una denuncia.

Si compruebas una manipulación anormal de los plásticos, hay que avisar a la entidad bancaria.

Ten cerca el número de contacto del banco a poder ser guardado en tu dispositivo móvil para acceder rápidamente. Si te roban la tarjeta, no podrás consultar el número que aparece en la misma.

No firmes las tarjetas bancarias por detrás, dado que verán cómo es tu firma habitual y podrán utilizarla en caso de robo.

m. 3 consejos de seguridad para aplicar en el propio banco

No retires altas sumas de dinero en efectivo. Pueden seguirte *a posteriori* y robarte el dinero en tránsito.

Presta atención a las personas que tengan una actitud sospechosa, ya sea al acceder al banco, en el interior o al salir del mismo. En caso de observar algo anómalo, avisa a los trabajadores de la

entidad y a la policía si fuese necesario. En caso de atraco o secuestro no te enfrentes a los atracadores y haz lo que te pidan hasta que se marchen o llegue la policía.

Al retirar el dinero en efectivo a través de la ventanilla, haz el conteo directamente delante del empleado del banco para reducir tu exposición e informarle si hay algún error.

Como vemos, estos consejos que facilita Lisainstitute.com facilitan la confianza del ciudadano de forma fácil y sencilla en torno a lo que no se debe hacer y lo que es aconsejable llevar a cabo para huir de una posible apropiación de datos que acabe en una muy posible apropiación de dinero.

E) *Medidas cuando los ciudadanos están de viaje y utilizan internet ajeno*

Uno de los momentos donde se incurre en una alta desprotección es cuando se va de viaje el ciudadano, ya que para evitar gastar sus datos personales recurren a los públicos, por lo que los expertos en seguridad recomiendan tomar ciertas precauciones a la hora de utilizar redes WiFi abiertas, ordenadores públicos o sus propios teléfonos móviles si no se adoptan las debidas precauciones, porque este uso abierto de internet facilita el acceso por terceros a los datos de las víctimas.

IV. *Conclusión*

Como vemos, se trata de instrumentalizar una herramienta sencilla, fácil de elaborar, didáctica y ausente, en la medida de lo posible, de términos técnicos que hagan inaccesible el conocimiento de lo que se recomienda, aunque puede utilizarse algún tipo de apartado para ciudadanos con un nivel medio alto de informática y otro de nivel medio bajo, a fin de delimitar ambas franjas de conocimiento para poder suministrar toda la información posible para que desde el punto de vista preventivo la ciudadanía pueda actuar evitando ser víctima del delito informático.

Resulta indudable que si desde la Administración Pública se pone el acento y esfuerzo en trabajar desde la prevención del delito informático, se podrán ver reducidas las cifras en estos delitos, porque la protección frente a estos tipos penales que se han expuesto es mucho más eficaz desde la protección que desde la sanción *ex post*. Y unas buenas medidas preventivas expuestas y reflejadas de forma clara y fácil de asumir por el lector permiten darnos una herramienta muy eficaz que a medio y largo plazo debilitará a los delincuentes informáticos y hará menos rentables los esfuerzos en este tipo de delincuencia.

(1)

https://ginzo.tech/blog/tipos-delitos-informaticos/

(2)

https://www.datos101.com/blog/las-9-medidas-de-seguridad-informatica-basicas/

(3)

https://www.softzone.es/noticias/seguridad/medidas-seguridad-evitar-virus-correo/

(4)

https://www.lisainstitute.com/blogs/blog/consejos-seguridad-bancaria