CENTRO DE ESTUDIOS GARRIGUES

Centro de Estudios Garrigues

Legal Essay Competition 2020

Premio Otorgado. Categoría Grado

Realidad virtual y ciberseguridad, una pareja inestable

Lucía Do Nascimento Fernández

4º Grado en Derecho

Universidad Rey Juan Carlos

El pasado 14 de marzo, el Presidente del Gobierno de España compareció ante los medios de comunicación anunciando la inminente declaración del Estado de alarma como consecuencia de la crisis sanitaria ocasionada por la COVID-19. En ese momento, la mayoría de la población no era consciente de la repercusión que la pandemia tendría en servicios públicos tales como la sanidad o la educación, tampoco en su vida cotidiana.

En un lapsus de tiempo brevísimo, nuestra rutina se vio alterada hasta el punto de que actos como hacer la compra, trabajar desde nuestro domicilio o seguir las clases *online* se convirtieron en auténticas carreras de obstáculos que eran sorteadas por los más rápidos, o por los besados por la suerte. De este modo, la "nueva realidad" obligaba a adaptar los hábitos de toda la población a la realidad virtual en pro de la economía y de la salud mental de animales sociales como los humanos.

Sin embargo, no es oro todo lo que reluce. A pesar de que el Real Decreto-Ley 15/2020, de 21 de abril, de medidas urgentes complementarias para apoyar a la economía y el empleo, estableció el sistema de "teletrabajo" como prioritario al efecto de mantener activa gran parte del tejido empresarial, no tardaron en manifestarse las ostensibles deficiencias de nuestro país -en general- y de los empleadores -en particular- en materia informática y ciberseguridad: la sobrecarga de los sistemas, la ralentización de la velocidad de la conexión a Internet, la ausencia total o parcial de informatización de los datos de los clientes o la carencia de protocolos de ciberseguridad en más del 60% de las empresas españolas han sido algunas de las contingencias más comunes durante los últimos meses.

Asimismo, con la generalización del uso de la informática para realizar casi cualquier tarea, y, por tanto, con el aumento del intercambio de datos a través de la red, se ha incrementado también la actividad de los conocidos como "ciberdelincuentes". Los datos son alarmantes: tal y como informó RTVE el día 14 de abril del corriente, el Centro Criptológico Nacional, organismo encargado de la seguridad de los entes públicos, certificó que los ataques de *phishing* se han intensificado hasta en un 75% durante la crisis sanitaria ocasionada por la COVID-19.

En efecto, no han sido pocas las noticias publicadas en la prensa o emitidas en los informativos nacionales en las que se informaba a los ciudadanos sobre la tentativa de sabotaje a los equipos informáticos de los hospitales españoles en pleno auge de los contagios, de la creación de

páginas web falsas que prometen diagnosticar al usuario que las visita al efecto de determinar si está infectado de coronavirus, o de la recepción de *emails* presuntamente enviados por entidades como la Agencia Tributaria o Correos, todo ello con el único objetivo de aprehender los datos personales o bancarios del receptor.

Pero, si en la actualidad la mayoría de la población tiene acceso a un equipo informático y lo utiliza haciendo gala del archiconocido nivel medio de Office, ¿por qué siguen sucediéndose robos de datos a través de intentos de *phishing*? La respuesta parece encontrarse en el desconocimiento. La posibilidad de usar un dispositivo con acceso a Internet para efectuar procedimientos tan habituales como la petición de cita previa para renovar el Documento Nacional de Identidad (DNI) o la consulta de las posiciones de nuestra cuenta bancaria, unida a la comodidad derivada de la obtención del resultado esperado a golpe de *click*, parecen avalar la falta de interés generalizada del usuario medio por la toma de las precauciones debidas.

Lo cierto es que, como consecuencia de ello, los ciberdelincuentes cada vez encuentran más facilidades para realizar el cometido para el que se han especializado: *grosso modo*, redactan un *email* haciendo uso de una cuenta de correo electrónico robada o suplantan direcciones de correo oficiales, insertan texto solicitando las credenciales personales o bancarias de la víctima para un cometido ficticio, y adjuntan un archivo en formato PDF o Word o un *link* en los que, al hacer *click*, el usuario descargará *malware* a su PC que usurpará todos los datos que tenga almacenados en él, o cederá sus credenciales personales al estafador.

Los supuestos de *phishing* no dejan de tratarse de estafas cometidas a través de medios electrónicos con el objetivo de utilizar los datos de la víctima para obtener un lucro; por tanto, se encuentran explícitamente incluidos en el contenido del artículo 248.2 del Código Penal (incluido a través de la reforma efectuada en 2016), que tipifica este tipo de comportamiento como delito especial.

El Tribunal Supremo ha tenido ocasión de examinar en los últimos años cierto número de casos de *phishing*, en cuyas resoluciones (STS 509/2018, de 26 de octubre; STS 379/2019, de 23 de julio; entre otras) ha esclarecido cuáles son los elementos que deben concurrir en el caso concreto para que la actuación del presunto estafador sea subsumible en el tipo referido: a) **manipulación informática** o artificio semejante a través del que se efectúa la estafa, que puede revestir las modalidades de *phishing* de redireccionamiento, *malware-based phishing*, *spear*

phishing o *pharming*; b) **ánimo de lucro**, habida cuenta que la sustracción de los datos de la víctima se lleva a cabo para beneficio económico del cibercriminal; y c) **acto de disposición económica** efectuado haciendo uso de los datos personales o bancarios robados, que se concreta en una transferencia de fondos no consentida. Resultan evidentes las nefastas consecuencias derivadas de este tipo de ataques, ya que, si no se han adoptado medidas en materia de ciberseguridad tendentes a evitarlos -como la instalación de un antivirus que evite la infección del equipo por *malware* o la verificación de los datos del remitente del *email*-, las únicas soluciones plausibles son el bloqueo de los movimientos sospechosos en la cuenta bancaria y la denuncia.

La sustracción de estos datos no sólo tiene relevancia penal, sino que también se encuentra prevista en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y garantía de los derechos digitales, y en el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. Como sabemos, toda persona física o jurídica que ofrezca sus productos o servicios al público a través de la red está obligada a proteger los datos de los usuarios que se los ceden a través de su inscripción en el Registro de Actividades de Tratamiento.

No obstante, al igual que lo sucedido con las estafas practicadas sobre particulares, es posible que los *hackers* accedan a los datos proporcionados por los usuarios a una determinada empresa; a este respecto, recordemos el reciente ataque a la compañía eléctrica portuguesa EDP, en la que los piratas informáticos solicitaron un rescate de 10 millones de Euros para desbloquear los servidores que previamente habían intervenido. En cualquier caso, los perjudicados estarán legitimados para acudir a la jurisdicción civil al efecto de reclamar a la compañía los daños y perjuicios soportados, y ésta deberá informar del robo de datos a la autoridad competente en materia de protección de los mismos en el plazo de 72 horas una vez detectada la brecha de seguridad.

Tal como se desprende de las estadísticas, ningún ciudadano se encuentra libre de la amenaza de las estafas informáticas. Por ello, ante una situación como la experimentada, es la que es necesario el uso e intercambio masivo de datos de carácter delicado, y la creciente especialización de los ciberdelincuentes para operar en la red sin ser rastreados, es necesario

proveerse de las herramientas necesarias, tanto tecnológicas como intelectivas, con las que esquivar un más que probable ataque contra nuestras credenciales.

Por ello, resulta primordial la universalización del conocimiento sobre técnicas de seguridad en la red, sin que constituya patrimonio propio de los estudiantes o profesionales de la ingeniería informática, o de aficionados *amateurs*. En este sentido, dado que la utilización de equipos informáticos se ha extendido a la mayoría de ámbitos laborales, la impartición de seminarios o cursos de carácter práctico sobre la citada materia en el seno de las empresas constituye un punto de partida cuasi obligatorio para concienciar a los usuarios de la necesidad de proteger las bondades de las que la tecnología nos ha proveído, habida cuenta que, de este modo, salvaguardamos algo tan valioso como nuestros datos. Como dijo el estadista inglés Benjamin Disraeli, “ser consciente de la propia ignorancia es un gran paso hacia el saber”.

Referencias

1. **Legislación**

   Real Decreto-Ley 15/2020, de 21 de abril, de medidas urgentes complementarias para apoyar a la economía y el empleo. Boletín Oficial del Estado, núm. 112, de 22 de abril de 2020, pp. 1 a 59.
   Recuperado de https://www.boe.es/boe/dias/2020/04/22/pdfs/BOE-A-2020-4554.pdf.

   Cita en el texto:
   Real Decreto-Ley 15/2020, de 21 de abril, de medidas urgentes complementarias para apoyar a la economía y el empleo.

2. **Artículo de periódico**

   Marta Juste (3 de abril de 2020). *Los ciberdelincuentes no hacen cuarentena: los ataques aumentan por el coronavirus*, Expansión.
   Recuperado de https://www.expansion.com/economia-digital/companias/2020/04/03/5e84cf48468aeb4b198b45b7.html.

3. **Artículo de periódico**

   Carol Espona (14 de abril de 2020). *Las estafas a través de "phishing" siguen estando en el top del ránking de los ciberdelincuentes*, RTVE.
   Recuperado de https://www.rtve.es/noticias/20200416/aumento-phishing-coronavirus/2012163.shtml.

4. **Jurisprudencia**

   - Tribunal Supremo (Sala de lo Penal, Sección 1ª), Sentencia núm. 509/2018, de 26 de octubre.
   - Tribunal Supremo (Sala de lo Penal, Sección 1ª), Sentencia núm. 379/2019, de 23 de julio.

   Cita en texto de ambas resoluciones:
   (STS 509/2018, de 26 de octubre; STS 379/2019, de 23 de julio; entre otras).

5. **Legislación**

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y garantía de los derechos digitales. Boletín Oficial del Estado, núm. 294, de 6 de diciembre de 2018, pp. 1 a 68.
Recuperado de https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf.

Cita en el texto:
Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y garantía de los derechos digitales.

6. **Legislación**

Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). Diario Oficial de la Unión Europea, de 4 de mayo de 2016, p. 119.
Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES.

Cita en el texto:
Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos.

7. **Artículo de periódico**

Manuel Fernández (16 de abril de 2020). *Hackeo a la eléctrica EDP: piden 10 millones para desbloquear sus archivos*, El Español. Recuperado de https://www.elespanol.com/omicrono/20200416/hackeo-electrica-edp-piden-millones-desbloquear-archivos/482951878_0.html.