La seguridad TIC en la infancia. Actuar en el ámbito educativo

PID_00245597

Erik de Luis Gargallo

Universitat Oberta de Catalunya

Índice

Introducción

Vivimos en una época de *boom* tecnológico. Dicho de otra manera, nos encontramos en un momento de la historia que destaca por un desarrollo acelerado de las tecnologías, rápido e imparable, especialmente en lo que a las tecnologías en materia de comunicación se refiere. Este desarrollo ha hecho crecer la función de los medios digitales y electrónicos en la vida diaria de los niños y adolescentes, apropiándose de una buena parte de su tiempo, modificando la forma en que se relacionan con el entorno y con los demás.

Analizando el impacto resultante de la relación que se establece entre la tecnología y las personas, se concluye que, de la misma manera que los jóvenes y niños tienen una mayor capacidad para adaptarse a los cambios que la tecnología presenta, también pueden a su vez resultar más vulnerables en su interacción con ella. Así, los jóvenes pueden interactuar con las nuevas tecnologías mostrando sin temor sus experiencias, -relaciones con los demás y su entorno-o, si no especifica a **experiencias**: experiencias, y las relaciones... llegando al final a definir su perfil psicológico virtual perfectamente.

En el artículo 12 de la Convención sobre los Derechos del Niño de las Naciones Unidas se hace referencia a que:

> «Los Estados parte garantizarán al niño que esté en condiciones de formarse un juicio propio el derecho de expresar su opinión libremente en todos los asuntos que afectan al niño, teniéndose debidamente en cuenta las opiniones del niño, en función de la edad y madurez de este».

Asimismo, en el artículo 14 de dicha convención consta que:

> «Los Estados parte respetarán el derecho del niño a la libertad de pensamiento, de conciencia y de religión».

Finalmente, siguiendo en la misma línea, la convención destaca en su artículo 17 el derecho del menor a que:

> «Los Estados parte reconocen la importante función que desempeñan los medios de comunicación y velarán por que el niño tenga acceso a información y material procedentes de diversas fuentes nacionales e internacionales, en especial la información y el material que tengan por finalidad promover su bienestar social, espiritual y moral y su salud física y mental».

En dicha convención, cuyo objetivo es recoger los derechos económicos, sociales, culturales, civiles y políticos de todos los niños del mundo, hemos visto como se hace referencia en varios artículos a la libertad de conocimiento y pensamiento del menor, con la finalidad de promover su bienestar social, es-

piritual y moral, y su salud física y mental. Debemos, por lo tanto, permitir el acceso a la información tanto como nos sea posible, siempre que la finalidad de dicho acceso sea su proyección cultural y educativa.

Pero, tal y como muestran las estadísticas actuales, dos horas diarias de consumo de Internet (Facebook, Fotolog, Twitter...), más dos horas diarias de consumo de televisión (por medio de Internet en muchos casos y sin control parental) y un consumo difícil de medir de teléfono móvil indican que los menores dedican más de cuatro horas diarias a sus interacciones virtuales. Y lo hacen en una entorno tecnológico muy heterogéneo y difícil de controlar.

Según el informe "Seguridad infantil y costumbres de los menores en Internet", de la asociación sin ánimo de lucro Protégeles (2002), un 44 % de los niños y niñas se han sentido acosados sexualmente en Internet en alguna ocasión, y de ellos un 11 % reconoció haber sufrido esta situación varias veces.

Asociación Protégeles

La asociación Protégeles es una organización sin ánimo de lucro conformada por profesionales pertenecientes a distintos campos: expertos en seguridad infantil, psicólogos, abogados, técnicos en informática, pedagogos y expertos en marketing y comunicación.

Surge como organización en el año 2002 ante la necesidad de hacer de Internet y de las nuevas tecnologías unas herramientas seguras para los menores.

Queda clara la necesidad de que las familias y los Gobiernos, así como otros entes públicos, se impliquen en el menester de formar a los jóvenes en una detección temprana de los síntomas, y proporcionar métodos de protección de los riesgos de Internet. La finalidad, por lo tanto, consiste en desarrollar en el menor un espíritu crítico en el uso de las redes sociales, programas de televisión, uso de dispositivos móviles, etc.

Y es aquí donde entra la comunidad educativa. Aparte de elaborar proyectos o planes educativos cuyo objetivo sea desarrollar el anteriormente citado espíritu crítico, así como la conciencia de los niños y jóvenes ante los medios tecnológicos que los rodean, hay que acompañarlos de un esfuerzo continuo de formación en la materia a educadores, con el objetivo final de facilitar a los niños competencias y capacidades críticas suficientes para hacer frente a los peligros que las nuevas tecnologías presentan a los más vulnerables.

Objetivos

Los materiales didácticos de este módulo proporcionan los contenidos y las herramientas imprescindibles para lograr los objetivos siguientes:

1. Mostrar el estado actual de la relación entre los menores de edad y las tecnologías de la información.

2. Identificar los riesgos más comunes a los que menores y adolescentes deben hacer frente en la actualidad en su relación con las nuevas tecnologías, así como su vinculación con el ámbito educativo.

3. Presentar las recomendaciones de seguridad básicas, tanto para menores como para adultos, en su interacción con el mundo virtual.

1. Las nuevas tecnologías y la infancia

Como en la mayoría de los aspectos de la vida, el punto de vista de un adulto no es el mismo que el de una persona joven. Y el uso de Internet no es una excepción.

El objetivo al que destinan Internet los adultos suele tener una finalidad más definida, más objetiva, aparentemente más justificada. Una persona adulta suele realizar compras en línea, buscar información en buscadores como Google, consultar el correo electrónico, realizar gestiones bancarias o sencillamente leer un periódico, entre otras.

Da la sensación, por lo tanto, que desde un punto de vista adulto hace falta una necesidad o un requerimiento para hacer uso de Internet. Es una visión altamente funcional, en el sentido de que es necesario la existencia de una necesidad para hacer uso de las redes.

Pero la visión de un menor no es la misma. Los niños y las niñas, en general, hacen uso de Internet desde un punto de vista más inherente o nativo. Utilizan Internet para estudiar, chatear, escuchar música, ver la televisión, o, simplemente, jugar. Es decir, su interacción es más natural, lo que conlleva a su vez la posibilidad de definir un perfil virtual a partir de aquellas costumbres que ellos mismos vierten mediante su uso en la Red. Para ellos, usar Internet para comunicarse con los demás, jugar e interactuar durante horas, o simplemente ocupar su tiempo descubriendo las capacidades de Internet, resulta tan natural como la vida misma.

Lo primero que debemos plantearnos es por qué los menores se relacionan con las nuevas tecnologías de forma distinta a los adultos. La respuesta parece ser obvia y sencilla: son la primera generación que nació con los recursos de Internet y las redes de telecomunicaciones de forma nativa, es decir, originariamente. Desde sus primeros avistamientos y percepciones hasta sus primeros pensamientos, se han llevado a cabo rodeados de ordenadores, móviles, tabletas electrónicas..., familiarizándose de base con las tecnologías de la información y las comunicaciones.

Indudablemente, estas tecnologías les ofrecen y ofrecerán un abanico de innumerables opciones, todavía muchas por descubrir. Serán ellos los que no solo disfrutarán de lo que estas ofrezcan, sino que determinarán las necesidades futuras y los nuevos servicios TIC del futuro.

Pero como todo nuevo mundo por descubrir, el virtual presenta una serie de riesgos que los menores deben conocer. Y no siempre son conscientes de que se enfrentan a ellos a diario. Los menores pueden llegar a vulnerar los derechos

de propiedad intelectual, tener acceso a contenido sexual sin filtro de ningún tipo, ser objeto de ciberacoso, *grooming* y *sexting*, interactuar con software malicioso, e incluso abusar de las tecnologías de la información, todo ello sin una perspectiva madura de la ilicitud de los hechos.

La dificultad para los tutores o formadores radica en cómo afrontar las distintas situaciones de riesgo que se le puedan presentar al menor. Ambos, menor y formador, navegan por un nuevo mundo donde no se dispone todavía de las herramientas necesarias y efectivas para hacer frente a las distintas situaciones problemáticas que acontezcan.

Cuando afrontamos los riesgos de las TIC, podemos caer en la cómoda tentación de basarnos exclusivamente en soluciones tecnológicas, como, por ejemplo, en si un ordenador dispone o no de antivirus. La cultura de la seguridad en línea va claramente más allá de una simple solución tecnológica; debemos atender a los comportamientos responsables y a la educación para generar en el menor la adopción de unas pautas o hábitos dignos de una cultura de la seguridad eficaz.

Obviamente, proporcionar a formadores y niños educación y herramientas para afrontar los riesgos TIC no elimina la necesidad de disponer de aquellas soluciones tecnológicas que permitan evitar, dentro de un margen suficientemente amplio, los problemas de seguridad más comunes. Así pues, una adecuada cultura de la seguridad proviene, de un lado, de las herramientas disponibles en los equipos (herramientas software y soluciones de apoyo a la función de control parental) y, de otro, de los hábitos o pautas generales de comportamiento adoptados por el menor.

Impulsar la sensibilización y educación en la materia, así como el fomento de un entorno TIC seguro, para proporcionar pautas concretas para identificar los riesgos y la forma de afrontarlos, es necesario tanto en adultos como en menores. Así se puede salvar la brecha digital que los separa.

Evidentemente, es recomendable la inclusión, en el ambiente escolar, de formación respecto al uso seguro de las TIC, de manera que el aprendizaje de herramientas y prácticas de seguridad sea implícito e inherente al aprendizaje de uso de las nuevas tecnologías.

2. Ciberacoso, *grooming* y *sexting*

En este apartado veremos tres de las principales amenazas que pueden sufrir los menores en su uso de las TIC hoy en día.

El ciberacoso escolar o *ciberbullying* se puede definir como el daño psicológico intencional infligido por parte de un menor o grupo de menores hacía otro menor, sostenido en el tiempo y cometido con cierta regularidad, utilizando como medio las tecnologías de la información y la comunicación.

Debemos destacar cuatro características para su correcta identificación:

- Debe haber un daño psicológico sobre el menor; se vulnera su bienestar psíquico y su salud emocional.
- Debe ser intencional, es decir, tiene que haber dolo en la acción cometida.
- Debe ser sostenido en el tiempo, pudiendo servir un simple hecho siempre que este se mantenga activo el tiempo suficiente, como, por ejemplo, un vídeo vejatorio.
- Deben utilizarse medios tecnológicos para llevarlo a cabo.

Son varios los métodos que se pueden utilizar para infligir el daño. Cualquier medio digital es susceptible de ser utilizado para enviar un mensaje, grabación de voz o vídeo, fotografía, etc. Normalmente son insultos, amenazas, rumores, mensajes ofensivos, fotos o vídeos vejatorios, enviados directamente a la víctima por medio de las redes sociales, blogs, foros, mensajería instantánea o correo electrónico.

Puede parecer que, aparentemente, el *ciberbullying* guarda una relación directa con el acoso tradicional, y en parte es así, como comportamiento ofensivo e intimidatorio que persiste en el tiempo, pero debemos tener presente que el medio desempeña un papel muy importante en el acoso escolar.

En primer lugar, las nuevas tecnologías dan una falsa sensación o capacidad de invisibilidad a los acosadores, que, en otras circunstancias como puede ser el mundo real, no se hubieran atrevido a asediar a nadie. Esto conlleva que

estas conductas ilícitas puede que no se detecten en el mundo físico porque se realizan exclusivamente en el mundo virtual, lo que dificulta enormemente su detección.

Otro aspecto importante es la capacidad de ampliar el daño, ya que el ciberacoso no dispone de barreras físicas ni temporales. Dicho de otro modo, el acosador o grupo de acosadores pueden ejecutar su intimidación durante todas las horas del día, los siete días de la semana, independientemente de dónde se encuentre el acosado. Solo es necesario el acceso al entorno virtual para continuar ejerciendo presión sobre la persona perjudicada.

Como perjuicio psicológico que es, la detección de este tipo de conductas pasa por una observación suficientemente cuidadosa de los menores, buscando en ellos síntomas de comportamiento emocional inadecuado, como ansiedad, estrés, apatía o tristeza, problemas físicos como dolor de estómago, o incluso comportamientos agresivos.

La elaboración de planes de convivencia en las escuelas determinará las acciones de prevención, actuación y evaluación para la convivencia entre sus miembros mediante la mejora de la comunicación entre los distintos agentes de la comunidad educativa.

En estos deben contemplarse la elaboración de actividades que fomenten un buen clima dentro del centro escolar, la concreción de derechos y deberes de los alumnos/as y las medidas correctoras aplicables en caso de su incumplimiento.

El *grooming* se define como el ciberacoso ejercido deliberadamente por un adulto para establecer una relación y un control emocional sobre un menor para preparar el terreno para su abuso sexual. Se puede definir, por lo tanto, como las acciones ejercidas sobre un menor con el objetivo de ganarse su confianza y disminuir sus inhibiciones, y así obtener de él un beneficio de naturaleza sexual.

El *grooming*, aunque tiene algunos parecidos con el *ciberbullying*, es importante separarlo en el sentido de que en el caso del *grooming* la parte acosadora no es menor, sino que se trata de personas adultas en la mayoría de los casos. Por este motivo, el *grooming* se relaciona con la pederastia y la pedofilia.

Pederastia y pedofilia

La pederastia es la acción llevada a cabo por un adulto que conlleva la práctica sexual con un menor, lo que implica un abuso por parte del adulto.

La pedofilia es la inclinación de un adulto a sentir una atracción sexual primaria hacia niños y niñas o preadolescentes.

El *grooming* habitualmente está formado por cuatro fases. En la primera fase, denominada de «la amistad», el acosador se aproxima al menor con la intención de establecer una primera relación, analizándolo para obtener la mayor cantidad de información posible para su fin, con el objetivo de lograr la con-

fianza del menor. En esta fase, el acosador puede utilizar diferentes métodos para acceder inicialmente a la víctima hasta conseguir su confianza, como pueden ser regalos, premios, pagos o incluso engaños.

En una segunda fase, denominada de «relación», el acosador profundiza en el menor, perfeccionando el conocimiento de este (gustos, aficiones, problemáticas, etc.) y mejorando la presunta amistad conseguida en la primera fase. Intenta consolidar así la confianza obtenida del menor. En esta fase, el acosador suele introducir el componente sexual en el menor, incitándole o animándole a participar de actividades de carácter sexual.

En la tercera frase, o fase del «inicio del abuso», el acosador o *groomer*, aprovechando la curiosidad del menor por el contenido sexual tratado en la fase anterior, ahondará aún más en dichas prácticas, siempre que el menor siga mostrando interés en ellas.

En este punto, es frecuente que el menor empiece a tener dudas respecto a las actividades de carácter sexual llevadas a cabo, por lo que suele renunciar a continuar con tales actividades, momento que utiliza el *groomer* para realizar el chantaje, pieza clave de todo *grooming*, que consistirá en amenazar al menor con hacer públicas las imágenes o vídeos proporcionados anteriormente por dicho menor, ya sea en redes sociales, por correo electrónico a su círculo de amistades, etc. Es importante tener presente que el acosador, en un momento u otro, puede haber infectado el ordenador del menor con un software malicioso que le ha permitido obtener las contraseñas de su correo electrónico, Facebook, etc., y disponer a su antojo de los contactos del menor acosado.

La última fase, denominada «de abuso y agresiones sexuales», aunque no suele ejecutarse siempre, es muy peligrosa, ya que consiste en contactar físicamente con el menor y abusar sexualmente de él.

El *grooming* puede llegar a ser más lesivo para el menor que el *ciberbullying*, si cabe, ya que en el caso de realizarse la última fase de contacto físico, las lesiones del menor son tanto psicológicas como físicas. Por este motivo, algunos de los síntomas que pueden presentar los menores son algo más severos que en el caso del *ciberbullying*; entre estos destacamos las conductas autodestructivas, las automutilaciones o las lesiones físicas, las conductas suicidas o las fugas, o incluso trastornos de la identidad sexual.

Tal y como apuntábamos al principio de este módulo, los menores que pasan mucho tiempo solos conectados a Internet sin una supervisión adulta y sin unas instrucciones claras de cómo utilizar las TIC presentan una mayor probabilidad de sufrir este tipo de situaciones de riesgo.

Educar al menor en el uso seguro de Internet, sus herramientas, servicios y redes sociales permitirá que este, de forma gradual, sea capaz de gestionar por sí mismo este tipo de situaciones y entornos. Debemos educar en aspectos tan

sencillos como el de no aceptar a desconocidos en las redes sociales, juegos en línea o servicios de mensajería, utilizando la publicación de noticias sobre *grooming* como trampolín para hablar con los menores sobre los riesgos que pueden afectarlos.

Como en el caso del ciberacoso escolar, es básica la adopción de metodologías que faciliten la inserción y el abordaje desde el currículum escolar de la problemática del *grooming*, y tomar medidas dirigidas a su prevención.

El *sexting* consiste en la difusión o publicación de imágenes o vídeos de tipo sexual, producidos por el propio remitente, principalmente por medio del teléfono móvil o por otros dispositivos tecnológicos (tableta, portátiles, etc.).

Es importante destacar que, a diferencia de los casos anteriormente analizados, en el caso del *sexting*, el origen del vídeo es lícito, en el sentido de que el protagonista del vídeo, o bien facilita él mismo dicho vídeo o imagen, o bien presta su consentimiento para realizar la grabación de este.

Evidentemente, el problema surge en el momento en que el poseedor del vídeo pierde el control del material audiovisual correspondiente, sea de forma voluntaria o no, por una distribución a terceros.

El motivo por el que un menor suele iniciar el fenómeno del *sexting* suele ser como método de seducción o, simplemente, para captar el interés del receptor de las imágenes o vídeos.

Por otro lado, el motivo por el que las imágenes de carácter sexual o erótico terminan distribuidas, es decir, acaban teniendo difusión pública, con las consiguientes repercusiones sociales y emocionales para el protagonista, suele ser la broma, la burla, la extorsión o el chantaje. Atacar el *sexting* desde el punto de vista del momento sexual que vive el adolescente, teniendo presente los cambios hormonales, químicos y psicológicos que sufre, resulta una tarea difícil; aún más, si tenemos presente la sexualización precoz de la infancia que adelanta la adolescencia a edades cada vez más tempranas, resultará un cometido difícil de conseguir.

Así pues, la importancia de informar y educar a los menores y adolescentes sobre los riesgos y las consecuencias del uso inadecuado de los dispositivos tecnológicos que tienen a su alcance es fundamental para hacer frente a las amenazas TIC como el *sexting*.

La mayoría de los menores creen que controlan las nuevas tecnologías y que a ellos nunca les afectarán las amenazas que estas presentan. Son confiados, ingenuos y crédulos, lo que dificulta aún más la labor que deben desempeñar las instituciones escolares para mostrar los peligros de Internet.

Partiendo de la necesidad básica en formación en cultura de la seguridad, atacar también el problema enseñándoles a configurar adecuadamente el nivel de seguridad de los perfiles de las aplicaciones que usan (configuración de los niveles de privacidad), o recordándoles la posibilidad de que su terminal móvil pueda ser robado o su ordenador resulte infectado, pueden resultar técnicas *a priori* eficaces para prevenir la amenaza.

Es importante recordarles a los menores que no existe el *sexting* seguro: da igual el momento, el motivo, la persona o el lugar. Una vez distribuida la imagen o el vídeo se pierde el control de lo enviado y, en consecuencia, la posibilidad de borrarlo o destruirlo.

3. Comunidades en línea

Son muchos los beneficios que nos aporta Internet. De todos ellos, quizás el más destacado sea que representa la fuente de información más importante que existe. Y no solo eso, sino que además no deja de crecer. De hecho, es común oír aquella expresión que dice: «Si no está en Internet, es que no existe».

Pero no todo lo que está en Internet es cierto ni bueno. A diferencia de las clásicas bibliotecas, en Internet no se selecciona ni se evalúa la información en función de su calidad, ya que es un medio en el que cada uno publica libremente aquello que desea. En Internet, las personas publican de forma participativa, contribuyendo al interés general.

Es entonces cuando surge el problema. ¿Son todas las informaciones vertidas en Internet verídicas? ¿Están todas ellas contrastadas? ¿Son las comunidades y los sitios web seguros? ¿Se vierte en ellos información adecuada y saludable? Evidentemente, la respuesta es no.

> Las comunidades en línea se pueden definir como un grupo de personas que, careciendo de un espacio físico, disponen de una identidad en Internet, manteniendo relaciones a partir de unos intereses comunes.

Por lo tanto, por definición, las comunidades en línea no presentan peligro alguno. Son espacios virtuales donde un grupo de personas vierte opiniones, ideas e información diversa en función de un tema o interés compartido por todos ellos. El peligro radica entonces en la información vertida en ellas, o, dicho de otro modo, la temática de la comunidad.

Así podemos encontrar comunidades peligrosas que tratan temas como la incitación al odio racial o la xenofobia; comunidades que promueven la anorexia y la bulimia; o que incitan al consumo de drogas y alcohol en jóvenes y menores. En estos casos, no solo resulta peligroso el contenido vertido en ellas, sino también la simplicidad con la que Internet es capaz de crear nuevas comunidades y la facilidad de difundir sus valores y principios, así como el enorme poder de reclamo del que disponen a través de Internet.

Pero no solo podemos encontrar xenofobia, islamofobia, antisemitismo, homofobia y grupos proanorexia y probulimia en recónditas páginas web o comunidades en línea alojadas en espacios privados; hoy en día, es posible localizar dicha información, su promoción e incluso su distribución en redes sociales tan utilizadas como Facebook o Twitter.

Ana y Mia

Resulta sorprendente la facilidad con la que conseguir información respecto a la anorexia y la bulimia (conocidas como Ana y Mia). Probemos tan solo de introducir las palabras «Ana y Mia» en cualquier buscador de Internet.

TABLA DE PESO ANA Y MÍA ACORDE A TU ESTATURA

Estatura (m)	Peso (kg)	Estatura (m)	Peso (kg)
1.45	38	1.65	48
1.46	38	1.66	48
1.47	38	1.67	48
1.48	39	1.68	49
1.49	39	1.69	49
1.50	40	1.70	51
1.51	40	1.71	51
1.52	40	1.72	51
1.53	41	1.73	53
1.54	41	1.74	53
1.55	43	1.75	55
1.56	43	1.76	55
1.57	43	1.77	55
1.58	44	1.78	57
1.59	44	1.79	57
1.60	45	1.80	59
1.61	45	1.81	59
1.62	45	1.82	59
1.63	46	1.83	61
1.64	46	1.84	61

Por tal razón, su detección, tan precoz y temprana como sea posible, resulta de vital importancia. Los casos de comunidades en línea de carácter peligroso o inadecuado no dejan de exponer a quién participa en ellas, o simplemente las sigue por convicción de lo que en ellas se comulga, a un riesgo conductual, físico e incluso cognitivo.

Así pues, la observación (forma pasiva) o la conversación (forma activa) con el menor o adolescente nos retornará información fundamental. Por ejemplo, es el caso del menor que en un momento dado está navegando por Internet y que cuando un adulto se acerca cierra repentinamente el navegador para que no se vea aquello que estaba consultando; o el caso del menor que reacciona mal ante la pregunta del adulto sobre un tema específico relacionado con algún grupo o comunidad en línea peligroso. Ambas son técnicas básicas pero perfectamente válidas para detectar la relación con la comunidad o grupo en línea con el menor.

Los síntomas que guardan correspondencia con la exposición al riesgo que suponen las comunidades en línea suelen tener un carácter más bien cognitivo. Entre dichos síntomas o manifestaciones se pueden destacar los problemas de rendimiento escolar o de convivencia, los conflictos de identidad, o sencillamente cambios en el comportamiento que se darán en mayor o menor medida según el tipo de comunidad peligrosa en línea con la que hayan tenido relación.

En lo referente a la forma de hacer frente a este tipo de amenazas, en primer lugar, se debe destacar la necesidad de que los adultos, ya sean profesores, tutores, padres, etc., sean conscientes de la existencia y el peligro que representan dichas comunidades. La interacción con los menores, permitiéndoles exponer sus dudas y escuchando sus opiniones, así como la observación de sus conductas diarias, darán a aquellos adultos responsables de ellos la idea de si interaccionan o no con entornos peligrosos.

No se debe olvidar que el menor y el adolescente son un blanco perfecto para la estafa o el fraude. Por tal motivo, es bueno compartir tiempo con ellos informándolos de los peligros que pueden surgir en la Red; eso sí, sin llegar a prohibirles el acceso a Internet (lo que supondría un enorme error, pues se les negaría el acceso al mayor recurso informativo del mundo). Hablar con ellos es el mejor y más eficaz recurso al que se puede recurrir.

Concretamente, desde el punto de vista de la docencia, realizar cursos de formación al profesorado, dando a conocer los factores de riesgo y las consecuencias peligrosas de las comunidades en línea, o llevar a cabo campañas de sensibilización sobre el tema en cuestión es, como se ha comentado anteriormente, la manera más efectiva para hacer frente al problema.

4. Identidad digital, privacidad, suplantación de identidad e ingeniería social

Desde el nacimiento de Internet, la red de redes ha evolucionado enormemente. Repasando un poco su historia, descubriremos que lo que actualmente llamamos Internet empezó llamándose ARPANET (*Advanced Projects Agency Net*). Fue un proyecto de los años sesenta del Ministerio de Defensa de Estados Unidos mediante el cual quería establecer una red interestatal de tal manera que la defensa del país dependiera de esta red. A su vez, permitía compartir los recursos en línea.

Son muchos los servicios que ofrece Internet: el FTP o *File Transfer Protocol*, la WWW o *World Wide Web*, o el correo electrónico, entre otros. Pero, de todos ellos, el más utilizado y conocido es, sin duda, la WWW o, simplemente, web. Y es en este donde uno debe detenerse para entender la relación entre la identidad digital y la privacidad con la web.

La WWW nos permite la posibilidad de ir de un sitio a otro, gracias al hipertexto, sin conocer la dirección exacta. Así, por lo tanto, si accedemos a cualquier página de un periódico en línea, podemos clicar sobre una de sus noticias y automáticamente seremos redirigidos a esta sin tener que preocuparnos de escribir nada en la barra de dirección.

La primera web, llamada más tarde Web 1.0, simplemente mostraba información y permitía al usuario acceder a ella solo como lectura. El usuario en este caso no podía interactuar con la página. Su contenido era estático.

Más tarde llegó la versión 2.0. La Web 2.0 ya permitía a los usuarios interactuar con otros usuarios o cambiar el contenido del sitio web. Se suele decir que el diseño de la web 2.0 estaba centrado en el usuario, en el sentido de que estaba orientada a la interacción y a las redes sociales, donde los usuarios participan del contenido mostrado. De esta manera, el usuario que navega por Internet ya puede colaborar, compartir e interactuar con los demás usuarios formando parte de una comunidad virtual.

Los usuarios se relacionan en Internet compartiendo información con otras personas, publicando fotos o vídeos, comprando en línea o simplemente jugando con videojuegos. Y es en este punto donde entra en juego la privacidad, ya que el usuario debe controlar la información personal con la que interacciona en Internet.

Concretamente, por privacidad en Internet entenderemos el nivel de protección que reciben los datos e informaciones de una persona en el momento en que se encuentran alojados en sitios de Internet, como por ejemplo una red social, y, en consecuencia, el grado de accesibilidad que otros usuarios o internautas tienen sobre ellos.

Pero ¿qué datos debemos proteger? ¿Qué son los datos personales?

Según la Agencia Española de Protección de Datos, miembro de la Red Iberoamericana de Protección de Datos (RIPD), los datos de carácter personal son:

"cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables".

AEPD

La Agencia Española de Protección de Datos (AEPD) es la autoridad de control independiente que vela por el cumplimiento de la normativa sobre protección de datos y garantiza y tutela el derecho fundamental a la protección de datos personales en España.

Como ciudadanos, podemos consultar e informarnos sobre el ejercicio de los derechos de acceso, rectificación, cancelación y oposición cuando no han sido adecuadamente atendidos.

Así mismo, Argentina dispone de la Dirección Nacional de Protección de Datos Personales (PDP), como órgano de control para la efectiva protección de los datos personales.

Tiene a su cargo el Registro Nacional de Bases de Datos, medio que la ley confiere para conocer y controlar a quienes tratan datos personales.

Asesora y asiste a los titulares de datos personales, y recibe las denuncias y reclamos efectuados contra los responsables de los registros, archivos, bancos o bases de datos por violar los derechos de información, acceso, rectificación, actualización, supresión y confidencialidad en el tratamiento de los datos.

En este sentido, tiene por función investigar si la base de datos denunciada da cumplimiento o no a los principios que establece la ley y las disposiciones reglamentarias.

En este sentido, es importante destacar que no solo nuestro documento nacional de identidad, nuestros nombres y apellidos, o nuestra dirección postal, son considerados datos de carácter personal, sino también que lo pueden ser nuestros gustos e ideas.

Teniendo presente que toda persona tiene derecho a la protección de sus datos de carácter personal y a saber con qué objetivo una organización utilizará sus datos, es de vital importancia la protección de nuestra privacidad en la web, ya que, de lo contrario, podríamos ser víctimas de convertir nuestra vida privada en una fuente pública de información.

Aun siendo conscientes del problema, los menores y adolescentes suelen ofrecer su información privada fácilmente. Desde su punto de vista, sentir el reconocimiento social y la aceptación por parte del resto de las personas, o simplemente de un grupo, resulta clave para el desarrollo de su autoestima. Además

debemos tener presente que en su esfera de influencia suelen localizarse personajes públicos cuya vida personal carece de privacidad, ya que cualquier información relacionada con dicho personaje se hace pública rápidamente con el beneplácito de este. De ahí la importancia que recibe la identidad digital en el mundo virtual.

Según definió el Instituto Nacional de Tecnologías de la Información de España en el año 2012, actual Instituto Nacional de Ciberseguridad (INCIBE), «La identidad digital, por tanto, puede ser definida como el conjunto de la información sobre un individuo o una organización expuesta en Internet (datos personales, imágenes, registros, noticias, comentarios, etc.), que conforma una descripción de dicha persona en el plano digital».

En consecuencia, de la misma manera que en el mundo real disponemos de una reputación personal normalmente basada en aquellos hechos que hemos llevado a cabo en el espacio físico, en el mundo virtual disponemos también de reputación digital entendiéndola como «la opinión o consideración social que otros usuarios tienen de la vivencia en línea de una persona o de una organización», tal y como definía el Instituto Nacional de Tecnologías de la Información de España en el mismo año 2012.

Es deducible entonces que, mientras utilizamos una identidad digital para cada uno de nosotros en nuestra interacción en la red de redes, dejamos información en aquellos lugares por donde navegamos, en lo que se denomina «la huella digital». Dicha huella digital resultará información vertida por nosotros mismos o por terceros que definirá, juntamente con nuestra identidad digital, nuestra reputación digital. Es de vital importancia que menores y adolescentes sean capaces de interiorizar la necesidad de activar pautas de seguridad y privacidad, aprendiendo a aplicar sus bases en el entorno digital.

Los principales riesgos que los adolescentes o menores pueden encontrarse en relación con una incorrecta gestión de la privacidad son un uso perverso de su información privada por parte de terceros (ya hemos visto casos como el del *ciberbullying* o el *grooming*) o un uso no autorizado de la información personal por parte de organizaciones dedicadas al comercio y que puede influir inadecuadamente sobre el menor.

A tal efecto, tutores y educadores deben transmitir a los menores la importancia del concepto de privacidad y la necesidad de controlar a conciencia la información que vierten en Internet. Con este objetivo es vital que se traten temáticas que guarden relación con la privacidad de los datos personales, así como del uso del anonimato de la identidad digital. La importancia radicará en dos aspectos complementarios y sucesivos: en primer lugar, se debe tomar conciencia de los riesgos a los que los menores se encuentran expuestos en su

relación con las nuevas tecnologías; en segundo lugar, y entrando en la privacidad como tema central por tratar, una correcta configuración de la privacidad que permita la mitigación o la supresión del riesgo presentado.

El soporte legal que ofrecen las leyes toma especial relevancia en el caso que nos ocupa. En España, la Ley orgánica 15/1999 de 13 de diciembre, de Protección de datos de carácter personal (LOPD) y el Real decreto 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos, establecen, entre otros muchos aspectos, que los datos personales de los menores de catorce años solo pueden ser tratados por terceras personas con el consentimiento de los padres o del tutor legal.

Uno de los aspectos que más relevancia suele tomar cuando se tratan los riesgos y peligros que presenta el uso de la identidad digital es la suplantación de identidad.

La suplantación de identidad se entiende como el uso de información personal para hacerse pasar por otra persona para obtener un beneficio propio. En efecto, este beneficio suele generar un perjuicio a la persona afectada.

Aunque quede fuera del propósito de este módulo, la bibliografía suele distinguir entre suplantación de identidad y usurpación de identidad. Se suele entender que la diferencia recae en el hecho de que la usurpación de identidad consiste en que una vez suplantada la identidad se empiece a interactuar como si realmente se fuese propietario de esos derechos y facultades que le otorga la identidad suplantada.

Así, por ejemplo, registrar o entrar en un perfil de una red social con el nombre de otra persona, y su clave de acceso si corresponde, sin su consentimiento y utilizando sus datos sería un caso de suplantación de identidad. Si además, se accede a una cuenta ajena utilizando los datos personales de un tercero sin su previo consentimiento, y se hace pasar por el suplantado, sería un caso de usurpación de identidad.

Aclarados los dos conceptos, y quedándonos con la idea de la suplantación de identidad, debemos introducir el concepto de la ingeniería social.

La ingeniería social es el uso que hacen los ciberdelincuentes de la manipulación psicológica sobre las personas para conseguir sus fines, teniendo en cuenta la tendencia general de estas a la confianza.

Dicho de otra manera, todos tendemos en principio a confiar en los demás, de tal manera que un ciberdelincuente, partiendo de ese concepto, establecerá todo un entramado de acciones dirigidas a que el atacado realice una serie de acciones en beneficio del atacante.

Uno de los métodos más utilizados para llevar a cabo la suplantación de identidad es, sin lugar a dudas, la ingeniería social. Se utiliza ingeniería social, por ejemplo, en el caso de un atacante que desee obtener las credenciales que le permitan acceder de forma no autorizada a un sistema, usando técnicas como el *phishing*.

Ved también

El *phishing* se estudia en el módulo «Software malicioso» de esta asignatura.

En cuanto al contexto relacionado con menores, uno de los servicios más utilizados por los ciberdelincuentes para suplantar la identidad de estos son las redes sociales. Para ello suelen emplear una serie de excusas para engañar al usuario, tales como enviar un mensaje privado en el que se comunique que se han detectado conexiones extrañas en la cuenta, por lo que, para mantener la seguridad, se recomienda que se cambien las claves. En otras ocasiones, crean sitios web falsos con la apariencia de la página de inicio de sesión para que cuando se introduzca el nombre de usuario y la contraseña se grabe y conserve esta información. De una manera u otra, el objetivo en este caso es conseguir el acceso a la cuenta del menor para obtener sus datos privados y suplantar su identidad.

La gravedad de las posibles consecuencias derivadas de los casos de suplantación de identidad son diversas y de distinto grado de afectación en la víctima. En el caso de los menores, suelen ir desde casos basados en burlas e insultos normalmente iniciados por otros menores, hasta casos más graves, donde se suele atacar la reputación de la víctima falseando su información.

En el caso de la suplantación de identidad, la única forma de reducir la exposición de los menores a los peligros que presenta es la prevención y el uso de técnicas dirigidas a minimizar y reducir las posibilidades de padecerlo. Así, minimizar la exposición de los datos sensibles, llevar a cabo una adecuada gestión de contraseñas, utilizar adecuadamente el correo electrónico o las redes sociales permitirá establecer unos márgenes de protección mínimamente efectivos ante este tipo de peligros.

La evolución de las amenazas presentes en Internet hace pensar que la cultura de la seguridad desempeñará un papel mucho más importante que el uso de cualquier sistema, software o hardware destinado a la protección ante los peligros de la gran Red. En este sentido, en el ámbito educativo es altamente productivo la organización de cursos o seminarios de sensibilización y formación para menores y comunidad educativa en general.

5. El fraude en línea

Sin duda, y tal y como hemos visto hasta ahora, navegar por Internet presenta riesgos y peligros. En este apartado analizaremos como el fraude en Internet supone un riesgo para todos los que hacemos uso de la gran Red. Da igual si somos adultos o menores, si utilizamos Internet para buscar información o jugar en línea, incluso si somos profesionales de las TIC o neófitos en el tema.

En nuestro día a día, independientemente del motivo por el que lo hacemos, tomamos una serie de medidas básicas para protegernos, aunque sea mínimamente, de los peligros o riesgos que nos presenta nuestra vida en sociedad. No dudamos, por ejemplo, en cerrar con llave la casa o el coche cuando no estamos en su interior y nos alejamos, o en contratar servicios como los seguros (coche, vida, hogar…) para que, en caso necesario, poder protegernos de contingencias normalmente imprevistas.

Pero en Internet actuamos de distinta forma. Para la mayoría de las personas, el hecho de estar detrás de una pantalla genera una falsa sensación de seguridad; si no nos ven, si no pueden tocarnos, no pueden hacernos daño. Y, en el caso de los menores, esta sensación se incrementa drásticamente. Si ellos todavía no tienen formado un concepto formal de seguridad física (no suelen tener miedo a ciertos peligros físicos que desde un punto de vista adulto lo son sin ningún tipo de duda), menos todavía en Internet.

Pero, en la actualidad, el fraude en línea, orientado a obtener un beneficio económico ilícito, representa uno de los principales retos de seguridad mundial. Son muchos los nuevos casos de estafas, robos, etc., que surgen diariamente en cualquier país del mundo. Su metodología es cambiante, sus objetivos pueden variar. Además, con un arsenal de nuevas posibles víctimas dispuestas a caer en la trampa, puede resultar difícil entender que se pueda disminuir o minimizar el impacto derivado de los ilícitos actos del delincuente.

Para llevar a cabo el fraude en línea un atacante puede hacer uso de múltiples mecanismos con el objetivo de robar nuestros datos bancarios, nuestros números de tarjetas de crédito, nuestra información personal, nuestras contraseñas de acceso al correo electrónico, incluso hacer uso de nuestra webcam, obviamente sin nuestro permiso, con el fin de obtener la información anterior.

Son muchas las técnicas mediante las cuales un atacante puede hacerse con nuestra información. Mientras hace años los primeros virus tenían la simple intención de molestar, como, por ejemplo, el virus ping-pong, conocido por que su única función consistía en hacer rebotar lo que parecía ser una pelota de ping-pong en nuestra pantalla, en la actualidad podemos hablar de virus que, por el mero hecho de conectarse a una página web y sin que el usuario sea

Ved también

En el módulo de «Software malicioso» se estudian las diversas técnicas mediante las cuales un atacante puede hacerse con nuestra información.

consciente de ello (el usuario desconoce que a través de alguna vulnerabilidad de su sistema se ha instalado el *malware* correspondiente), permiten al atacante obtener el control remoto y total del ordenador atacado.

Vulnerabilidades del sistema operativo, fallos de seguridad en las aplicaciones del sistema o incluso de *plugins* del navegador, enlaces a páginas webs, etc., son algunas de las posibles entradas de virus en nuestros ordenadores. En la actualidad, los atacantes suelen ayudarse de ataques de ingeniería social para inyectar el *malware* en nuestros sistemas. A partir de la infección, el atacante podrá llevar a cabo aquellas acciones para las que fue diseñado el software malicioso.

Confiar en que disponemos de un antivirus instalado y actualizado no es suficiente. Aunque obviamente es necesario, ya que es una primera línea de defensa básica para proteger nuestros ordenadores y dispositivos electrónicos, el antivirus por desgracia siempre va detrás del *malware*, ya que debemos partir de la premisa que dicho *malware*, una vez es detectado por las compañías desarrolladoras de antivirus, es añadido a sus bases de datos, pero no antes. La pregunta que debemos hacernos entonces es: ¿y hasta que lo añaden?

El fraude en línea, como hemos visto, utiliza vulnerabilidades en los sistemas para actuar ilícitamente sobre ellos: un archivo adjunto a un correo electrónico, un enlace de WhatsApp, Twitter, Facebook… Cualquiera de ellos puede resultar una infección. Resulta difícil establecer una clasificación en los tipos de fraude en línea existentes; normalmente se establece en función del vector de origen de la infección. A continuación veremos algunos ejemplos de tipos de fraudes en línea.

Los *rogues* suelen resultar muy efectivos. Un *rogue* es una aplicación ilegítima de seguridad; es decir, una aplicación que contiene código malicioso, pero se ofrece como lo contrario, como una aplicación dirigida a proteger nuestro sistema como podría ser un antivirus.

En primer lugar, el *rogue* informa al destinatario del ataque o a la posible víctima con una serie de alertas de seguridad conforme su sistema está infectado. Entonces le ofrece, como no podía ser de otra manera, la solución: un antivirus o software de seguridad, previo pago, que lo único que acabará haciendo es eliminando los molestos e inquietantes mensajes de infección. Evidentemente, no había infección alguna.

El *spam* es otro tipo de fraude en línea. A partir de correos electrónicos de distribución masiva y contenido normalmente publicitario o malicioso que el usuario recibe sin haberlo solicitado, se anuncian productos y servicios que suelen ser de dudosa calidad; se persigue, claro, que el receptor los compre.

También se utiliza el *spam* con finalidades activistas o simplemente para molestar.

Cabe destacar que, aunque el objetivo del atacante se cumpla y, por lo tanto, la víctima compre el producto ofrecido por el primero, para la víctima no todo el problema termina ahí. Imaginemos los problemas de salud que puede conllevar para el inocente comprador el consumo de dicho producto si este debe ingerirse.

El *phishing* es otro de los posibles orígenes del fraude en línea. Consiste en el robo de información a un usuario suplantando/falseando una entidad legítima en la que este confía.

Ved también

El *phishing* se estudia en el módulo «Software malicioso» de esta asignatura.

Aunque aplicable a cualquier empresa u organización presente en Internet, es el sector de las entidades financieras el más perjudicado con este tipo de fraude. Para ejecutar el fraude, suele utilizarse la técnica de enviar un correo electrónico ilegítimo, pero «disfrazado de legítimo», con el objetivo de que la víctima siga las instrucciones incluidas en él terminando por facilitarle al delincuente las claves o credenciales de acceso a su entidad bancaria.

Aunque en desuso por el incremento del uso de la mensajería instantánea (WhatsApp, WeChat, Telegram,...), otro de los fraudes en línea más conocidos es el SMS Premium, el cual consiste básicamente en el cobro por el envío de mensajes SMS tipo *Premium*, previa suscripción involuntaria a servicios de información diversa.

Fundamentalmente, el SMS Premium se realiza cuando un usuario instala una aplicación en cuyo proceso de instalación viene camuflado, en el listado de condiciones, la aceptación del consentimiento para que dicha aplicación envíe mensajes del tipo SMS Premium, impactando enormemente en la factura de la víctima del fraude.

En lo que se refiere a fraudes en línea destinados especialmente al universo del menor, estos suelen ir asociados a los videojuegos, que, evidentemente, es un foco de interés de menores y adolescentes. Como en los casos vistos hasta ahora, se trata de videojuegos y aplicaciones gratuitas de interés para

el menor que suelen llevar consigo la suscripción oculta y con coste en los SMS Premium, incluso en algunos casos con robo de datos del afectado por proporcionar este sus datos de acceso a redes sociales.

Como podemos ver, sea cual sea el tipo de fraude en línea ejecutado, el objetivo siempre es el mismo: la obtención de un beneficio económico, sea directo o indirecto (robo de información por el que después el atacante solicitará el pago correspondiente). Veamos un ejemplo real de este tipo de amenazas de Internet.

El virus de la policía

En los años 2011 y siguientes, una famosa campaña de *ransomware* (software malicioso cuyo objetivo es lucrarse al atacante por medio de rescates económicos), bloqueó miles de ordenadores de usuarios bajo la premisa de que sus direcciones IP habían sido supuestamente registradas en páginas webs ilegales orientadas a la difusión de pornografía infantil, zoofilia e imágenes de violencia contra menores.

Una vez informado del hecho, se solicitaba al usuario el pago de unos cien euros en concepto de «multa», llegando incluso a mostrar una imagen tomada desde la webcam de dicho usuario unos minutos antes de la notificación.

Aviso de infección por el virus de la policía en España (Cuerpo Nacional de Policía) y Reino Unido (*Metropolitan Police*)

Como medidas para prevenir este tipo de peligros de Internet, es fundamental mantener actualizados todos los programas instalados, el sistema operativo, los navegadores de Internet y el antivirus. Recordemos que cualquier software que tengamos instalado es susceptible de presentar vulnerabilidades que pueden ser explotadas por un atacante.

La actualización de nuestros programas, como pilar de la seguridad de nuestros sistemas debe realizarse con las máximas garantías. En este sentido, no se debe instalar ninguna actualización que no proceda, sea la vía que sea, de los desarrolladores de dicho software. Tendremos especial cuidado con las páginas web que nos ofrecen actualizaciones de software de terceros.

Tendremos en cuenta también el hecho de que un programa utiliza, en un momento dado, los privilegios de los que dispone el usuario que lo está ejecutando. Este aspecto es muy importante en el sentido de que, si somos usuarios tipo administrador, el programa (que puede ser *malware*) tendrá los privilegios de un administrador, mientras que si somos usuarios con cuenta limitada los privilegios serán los de dicho usuario.

Cuenta de usuario

Una cuenta de usuario es una colección de información que indica al sistema operativo los archivos y las carpetas a los que puede tener acceso un determinado usuario del equipo, los cambios que puede realizar en él y sus preferencias personales.

Un usuario tipo administrador posee la mayor cantidad de permisos y accesos a un equipo, y están dirigidos a administrar el sistema operativo sin restricción alguna, pudiendo modificar aspectos importantes de la configuración, entre otros.

Por otro lado, los usuarios tipo estándar pueden visualizar información y realizar modificaciones y algunos cambios en el equipo, pero disponen de una menor cantidad de permisos.

La gestión de contraseñas (se recomienda siempre que sean secretas, robustas y no repetidas) y la realización de copias de seguridad de nuestros datos para que podamos recuperarlos en caso de accidente o incidente son otras de las dos medidas que debemos aplicar para proteger nuestros sistemas.

En lo que se refiere a procedimientos llevados a cabo desde los centros de enseñanza, es recomendable que dispongan de sistemas que permitan la supervisión de la actividad de los menores en su interacción con Internet, configurando adecuadamente los sistemas y estableciendo las restricciones necesarias en su acceso a las páginas web que puedan resultar potencialmente peligrosas.

Contrariamente a lo que se pueda creer, los centros de enseñanza no deben realizar estas acciones como una operación de control o de restricción en la navegación web de los alumnos. Lejos de esa idea, los centros han de presentar dichas acciones como parte de la cultura en seguridad TIC que los alumnos conviene que aprendan.

6. Recomendaciones de seguridad

En el ámbito de la seguridad informática existe una premisa básica que debemos tener siempre presente: la seguridad absoluta, con una probabilidad del cien por cien, no existe.

Entonces, si no podemos garantizar la seguridad completa de nuestros sistemas, ¿debemos hacer algo al respecto? Y, en caso afirmativo, ¿qué medidas debemos aplicar? Evidentemente, el hecho de que no podamos garantizar el cien por cien de la seguridad de nuestros dispositivos TIC no significa que no debamos protegerlos tanto como podamos. De hecho, la seguridad de nuestros hogares, vehículos, incluso nuestras vidas, no está nunca garantizada, pero aun así intentamos hacerlos tan seguros como nos es posible.

Aunque es cierto que la seguridad es proporcional al coste de las medidas de protección, también lo es el hecho de que la cultura de la seguridad no tiene coste y suele representar el pilar fundamental para protegerse ante los múltiples peligros de Internet.

Así, debemos aprender los distintos ámbitos desde donde tenemos que actuar en lo que se refiere a seguridad informática: la prevención, la detección, la respuesta y la recuperación.

A continuación valoraremos las recomendaciones de seguridad más importantes que debemos tener en cuenta para salvaguardar nuestros dispositivos. Haremos referencia a técnicas de prevención y detección, viendo cómo estas aumentan la seguridad de un sistema de información durante su funcionamiento normal, previniendo la ocurrencia de violaciones a la seguridad e incluyendo, si es necesario, medidas de disuasión. También veremos técnicas de respuesta y recuperación, que serán aquellas que se aplican en el momento que detectemos la violación a nuestra seguridad y que permiten recuperarnos de un ataque.

6.1. Técnicas de prevención, detección, respuesta y recuperación

Existen innumerables herramientas y sistemas de seguridad orientados a preservar la integridad, la confidencialidad y la disponibilidad de la información y los sistemas.

Como técnicas de prevención y detección, es esencial y básica la instalación de software antivirus con actualizaciones regulares de fabricantes reconocidos. Estos permiten llevar a cabo tareas de análisis, automatizadas algunas y otras a requerimiento del usuario, dirigidas a la eliminación de los virus y otro *malware* actual.

Entre las tareas más importantes de un antivirus, podemos encontrar el escaneo bajo demanda (planificado por el usuario), el escaneo de acceso (llevado a cabo automáticamente por el antivirus al abrir un archivo), el control de firmas (que consiste en la detección de cambios en ciertos archivos llevados a cabo ilícitamente), o el más conocido método heurístico (que busca virus «modelo» ya conocidos en el ordenador, a partir de una base de datos del antivirus). No hay que olvidar la importante función que llevan a cabo los antivirus, realizando análisis en el envío y recepción de correos electrónicos.

No solo disponer de antivirus es necesario para prevenir de *malware* nuestros sistemas. Es muy importante tener habilitada la actualización automática de software y aplicar las actualizaciones (tanto del sistema operativo como de las distintas aplicaciones de trabajo) siempre que surja una nueva versión (reiniciando el sistema lo antes posible en caso de ser solicitado). Por este motivo, cada vez más los antivirus amplían sus funcionalidades mediante la implementación efectiva de control de configuración y gestión de software, tratando de asegurar que los sistemas operativos y las aplicaciones sean actualizados de forma correcta tras la publicación de los parches preceptivos.

Obviamente, es fundamental la realización de copias de respaldo o *backups*, que serán almacenadas en un lugar seguro, para poder restaurar el sistema a un estado anterior pero idóneo. Las copias de respaldo están orientadas a garantizar la disponibilidad de los sistemas informáticos frente a cualquier contingencia o incidente.

Otro de los elementos de red que suele resultar muy efectivo es el cortafuegos. Cierto es que su uso profesional está mucho más extendido que en el ámbito personal; se emplean dispositivos tipo hardware que controlan las comunicaciones en la red, permitiendo y denegando estas, y asegurando que el tráfico de red es aquel que se ha autorizado. Aun así, en el ámbito doméstico, los cortafuegos tipo software como el que incluyen los sistemas operativos como Microsoft Windows resultan ser altamente efectivos para tratar de disminuir el número de accesos potenciales e ilícitos.

Pero, sin lugar a dudas, no debemos olvidar que el mejor método de prevención es la formación constante en materia de seguridad. Lo que hoy en día es válido en materia de seguridad lógica, es posible que, en un periodo de tiempo

más bien corto, deje de ser efectivo y deba ser necesario aplicar otras medidas. Estar formados en el ámbito de la seguridad es esencial como protección contra el software malicioso.

En lo que se refiere a acciones que deben ejecutarse una vez que el ataque o el incidente se han hecho efectivos, destacaremos la desconexión física de la red de los dispositivos afectados con el objetivo de proteger nuestros datos y evitar la propagación de la infección (puede incluir el aviso de nuestra infección a otras personas que creamos que pueden verse afectadas por el incidente), la eliminación del software malicioso origen de la infección de nuestro dispositivo, y, finalmente, el inicio del proceso de recuperación de nuestros datos a partir de una copia de respaldo o *backup* que previamente nos hemos asegurado que es íntegro.

6.2. Resumen de recomendaciones de seguridad

A título de recapitulación, veremos los principales puntos que debemos tener presentes para asegurar nuestros dispositivos de red:

- Modificar las opciones por defecto o de fábrica en la configuración de seguridad de los dispositivos electrónicos incrementando su nivel de seguridad. Normalmente, las opciones de seguridad vienen por defecto a niveles más bajos de los deseados, de tal manera que favorecen la conectividad pero perjudican gravemente la seguridad.

- No debemos mostrar información en nuestros dispositivos cuando estos están fuera de nuestro alcance, aun cuando se encuentren bloqueados. Dicha información puede ser utilizada para acceder a ellos y romper así la barrera de seguridad que supone el bloqueo.

- Asegurar que los sistemas de autenticación para el control de acceso de los usuarios funciona adecuadamente. No debemos prescindir en ningún momento del uso de credenciales de usuario y contraseña para proteger nuestros ordenadores y otros dispositivos que conectamos a Internet.

- Actualizar el software a la última versión suministrada por el fabricante. Los programas de gestión, sistemas operativos, antivirus, etc., utilizan un software llamado *firmware* que debemos actualizar constantemente para protegernos de los fallos de seguridad detectados y reparados por el fabricante de dicho software.

- Configurar adecuadamente nuestros navegadores web. Estos representan la puerta que comunica nuestros ordenadores, tabletas, móviles, etc., con Internet, motivo por el cual deben estar correctamente configurados, permitiendo o denegando ciertas opciones según nuestro interés. Así, por ejemplo, se recomienda permitir funcionalidades del navegador como la administración de las advertencias sobre sitios web inseguros, deshabilitar

la ejecución y uso de *plugins*, y denegar el almacenamiento automático de datos personales, cuentas y contraseñas de usuario en dicho navegador.

- Las conexiones inalámbricas tipo wifi o Bluetooth deben estar por defecto desactivadas. Debemos ser conscientes en todo momento del estado de las conexiones de nuestros dispositivos, activándolas o desactivándolas a nuestro parecer. En esta línea, no debemos conectarnos a redes wifi públicas, ya que desconocemos el control de la seguridad que se ejerce sobre ellas; nuestros datos podrían ser capturados y analizados sin que nosotros seamos conscientes de ello.

- Las copias de seguridad deben realizarse de forma regular comprobando su funcionalidad de vez en cuando. No debemos olvidar que los archivos de instalación del software como el sistema operativo o los programas son fácilmente recuperables reinstalándolos nuevamente. Por otro lado, nuestros documentos personales, fotografías, etc., no los recuperaremos a menos que dispongamos de una copia de seguridad correctamente realizada.

- Como norma general, no abriremos ninguna comunicación que no venga directa y explícitamente dirigida a nosotros. Esta recomendación hace referencia a correos electrónicos, pero es extensible a cualquier tipo de comunicación electrónica como un SMS o MMS, un WhatsApp, etc.

- Las redes sociales son un punto clave en lo que se refiere a la cultura de la seguridad. Concienciar a los usuarios respecto al buen uso que deben hacer de su información personal en Internet es fundamental para asegurar su privacidad y la protección de sus datos, y evitar así la filtración de estos. Debemos configurar adecuadamente las opciones de seguridad ofrecidas por la red social en cuestión, desactivando los servicios de localización, entre otros.

- Utilizar, siempre que sea posible, sistemas de protección de nuestros documentos y fotografías con el objetivo que aunque culmine con éxito el ataque, la información capturada por el atacante no sea visible por este. Es recomendable la utilización de programas de cifrado que ocultan los datos a proteger, mostrando únicamente la opción de introducir la clave o contraseña adecuada.

- Se recomienda la desincronización automática de los distintos soportes de almacenamiento digital y otros dispositivos que conectamos a nuestros ordenadores. La sincronización automática permite reconocer e incluso ejecutar el soporte conectado al ordenador. Pero este aporte de usabilidad otorga al soporte la capacidad de efectuar una acción determinada como ejecutar un archivo .exe al insertar un medio extraíble, como por ejemplo un dispositivo de almacenamiento masivo USB. Para evitar este tipo de

peligros, debemos desactivar la reproducción automática en todas las unidades extraíbles.

Resumen

En este módulo hemos visto, en primer lugar, cómo de vulnerables son los menores y jóvenes ante las nuevas tecnologías, motivo por el cual merecen una atención y protección especiales ante su visión TIC enormemente distinta de la de los adultos, fomentando el uso de un entorno digital seguro.

Se han estudiado las principales amenazas a las que menores y adolescentes están expuestos en su interacción con el mundo digital. Hemos analizado el ciberacoso, el *grooming*, el *sexting*, las comunidades en línea, la identidad digital, la privacidad, la suplantación de identidad, la ingeniería social y el fraude en línea.

En la segunda parte del módulo, se han dado las recomendaciones de seguridad consideradas fundamentales para guiar nuestra seguridad a través de Internet, partiendo de una premisa básica de la seguridad informática y que debemos tener siempre muy presente: no existe un sistema informático 100% seguro.

Partiendo de ese concepto, hemos analizado distintas técnicas de prevención, detección, respuesta y recuperación. Finalmente, se han dado una serie de puntos clave, a título de compendio, para hacer de nuestros sistemas informáticos un entorno TIC más seguro.

Actividades

1. En el módulo hemos visto comunidades en línea peligrosas que promueven la anorexia y la bulimia, o que incitan al consumo de drogas. Analizando otras comunidades peligrosas, ¿en qué consisten las comunidades *self-harm*? ¿y las *hate-speech*? Explica qué tipo de actitudes fomentan.

2. El ciberacoso, el *grooming*, el *sexting*, las comunidades y el fraude en línea han sido algunos de los riesgos TIC estudiados en este módulo. Ampliando conceptos ¿qué son las tecnoadicciones? ¿Cuáles son sus características principales?

Bibliografía

Asociación Protégeles (2010). *Estudio sobre la utilización de la web 2.0 por parte de los menores*.

Luengo, J. A. (2011). «Guía de recursos para centros educativos en casos de ciberacoso». Defensor del Menor en la Comunidad de Madrid.

Miranda de Larra, R. (2005). *Los menores en la Red: comportamiento y navegación segura*. Fundación Auna.

Mitchell, K. J.; Finkelhor, D.; Wolak, J. (2003). *The Exposure of Youth to Unwanted Sexual Material on the Internet: A National Survey of Risk, Impact, and Prevention*. Youth & Society.

UNICEF (1989). *Convención sobre los Derechos del Niño*.

Willard, N. (2005). *Educator's Guide to Cyberbullying, Cyberthreats & Sexting*. Center for Safe and Responsible Use of the Internet.

Enlaces de Internet

http://www.centrointernetsegura.es/noticias_interior.php?id=48

http://www.internetsociety.org/sites/default/files/bp-childrenandtheinternet-20129017-en_ES.pdf

http://mediasmarts.ca/digital-media-literacy/digital-issues/pornography/responding-online-pornography

http://www.injuve.es/sites/default/files/2013/22/eventosinfo/Informe%20Racismo%20Odio%20e%20Intolerancia%20%20en%20Internet.pdf

https://ink.niche.com/best-worst-media-habits-class-2014/

http://www.pantallasamigas.net/estudios-realizados/pdf/inteco-estudio-uso-seguro-tic-menores.pdf