AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

PROTECCIÓN DE DATOS Y PREVENCIÓN DE DELITOS

Sexting

1. ¿Qué es el sexting?

El sexting consiste en hacerse fotografías, grabarse en un vídeo o audio, o dejar que lo hagan otros, en una situación comprometida o íntima (por ejemplo, desnudo, o parcialmente desnudo, o en posición insinuante), que no te gustaría que conociera todo el mundo y se las envías voluntariamente a alguien que puede que luego las reenvíe o difunda sin tu consentimiento.

2. ¿Es malo el sexting?

Enviar fotos, videos o audio, de esta forma es muy arriesgado. Cuando envías una fotografía tuya, un vídeo o un audio a otra persona puede ser reenviada sin ningún límite. Además, puede terminar publicada en Internet y no podrás controlar quién accede a ella. Pierdes el control de las imágenes.

Las consecuencias del sexting van desde sentirse mal y avergonzarse delante de la familia, amigos, compañeros… al saber que te han visto y oido en esa foto, vídeo o audio, hasta que otra persona te acose, te humille, te amenace o te coaccione.

Incluso si no te importa que ahora te puedan ver u oír en esa foto, vídeo o audio, tal vez llegue un día en que sí te moleste que los demás tengan esas grabaciones tuyas.

3. ¿Qué hacer si recibes una fotografía o un vídeo de este tipo?

Nunca reenvíes las imágenes y/o grabaciones que recibas. La imagen y la voz de una persona es un dato personal y no puedes decidir sobre los datos personales de otra persona sin su permiso. Además, el reenvío de grabaciones de sexting sin la autorización del afectado es un delito, aunque se hayan realizado con el consentimiento de la persona.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Grooming

1. ¿Qué es el grooming?

Cuando un adulto, a través de las redes sociales u otros servicios de Internet, oculta su identidad, generalmente haciéndose pasar por un menor, con el objetivo de ganarse la confianza de otro menor.

En ocasiones, el adulto accede a la información personal del menor sobre sus gustos, hábitos y aficiones, que utiliza para ganarse su amistad y confianza.

Cuando ya se ha ganado su confianza consigue que le cuente cosas o que le envíe fotos o vídeos de actos o comportamientos comprometidos y de contenido sexual.

Una vez obtenida esta información, le pide más fotografías o vídeos o tener encuentros con fines sexuales y, si no se los da o acepta, es cuando le amenaza con contar lo que le ha dicho o con publicar las fotos y vídeos que le envió.

2. ¿Qué hacer si estás sufriendo grooming?

El grooming es un delito. Si lo sufres o si sabes de algún caso de grooming debes ponerlo en conocimiento de tus padres, de la Policía o de la Guardia Civil. También puedes llamar al teléfono de ANAR, 900 20 20 10, que es una asociación que ayuda a los niños y adolescentes, y es anónimo, gratuito y confidencial.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Ciberacoso

1. ¿Qué es el ciberacoso?

Amenazas, hostigamiento, humillación, control u otro tipo de molestias realizadas por un adulto contra otra persona por medio de las tecnologías de la información y comunicación (Internet). Cuando se produce entre menores se conoce como ciberbullying.

El acoso a través de Internet, a diferencia del acoso físico, supera las barreras del espacio y del tiempo. Se puede producir a cualquier hora del día y con independencia del lugar donde se encuentre el acosado.

Cuando alguien acosa a otra persona a través de Internet posiblemente esté cometiendo un delito de acoso.

2. ¿Qué consecuencias tiene?

Puede causar graves consecuencias a la persona acosada, desde hacerle sentir mal hasta llegar al suicidio.

Al acosador le puede suponer una pena y unos antecedentes penales que tienen consecuencias en el futuro.

Si eres objeto de acoso o sabes de alguien que lo está sufriendo, debes ponerlo en conocimiento de la Policía o de la Guardia Civil. Si eres menor de edad también puedes llamar al teléfono de ANAR, 900 20 20 10, que es una asociación que ayuda a los niños y adolescentes, y es anónimo, gratuito y confidencial; y al teléfono 900 018 018 si se produce en el entorno escolar.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Violencia de género

1. Definición

Violencia física y psicológica que, como manifestación de la discriminación, la situación de desigualdad y las relaciones de poder de los hombres sobre las mujeres, se ejerce sobre éstas por parte de quienes sean o hayan sido sus cónyuges o de quienes estén o hayan estado ligados a ellas por relaciones similares de afectividad, aun sin convivencia.

2. Manifestaciones de violencia contra las mujeres en el mundo digital

- El acoso online, que constituye una de las formas más visibles de la violencia contra las mujeres relacionada con la tecnología.
- La violencia en el ámbito de la pareja utiliza también la tecnología como medio para acosar, insultar y amenazar a la mujer, para controlarla o extorsionarla y chantajearla con divulgar imágenes intimas o comunicaciones privadas por parte de su pareja para impedir que abandone la relación.
- La geolocalización para rastrear los movimientos de una mujer por su pareja o expareja con fines de abuso o agresión sexual, o para proporcionar información sobre su ubicación y agredirla.
- También se pueden utilizar las nuevas tecnologías para contactar con mujeres para atraerlas a encuentros donde pueden ser agredidas.
- La tecnología puede jugar un papel en la creación de una cultura de la violencia contra las mujeres o en su justificación. Puede variar desde algo tan aparentemente banal como la difusión de una broma sexista que apoya la idea de que las mujeres son menos valiosas que los hombres, hasta la creación de grupos en redes sociales que promuevan diferentes formas de abuso contra las mujeres, por ejemplo grabando y difundiendo imágenes de una agresión sexual.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Phishing

1. ¿Qué es el phishing?

Es uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima, con la finalidad de causarle pérdidas económicas.

El estafador (phisher) utiliza técnicas de ingeniería social que consiste en obtener información esencial a través de la manipulación de los usuarios legítimos de Internet o de un servicio o de una aplicación.

2. ¿Cómo se produce?

El cibercriminal se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea, redes sociales, SMS/MMS, o incluso utilizando también llamadas telefónicas.

Los correos electrónicos fraudulentos, suelen incluir un enlace que, al ser pulsado, lleva a páginas web falsificadas. De esta manera, el usuario, creyendo estar en un sitio de toda confianza, introduce la información solicitada que, en realidad, va a parar a manos del estafador.

El ataque de phishing a través de SMS, es conocido como smishing, el usuario recibe un mensaje de texto intentando convencerle de que visite un enlace fraudulento.

El de telefonía es conocido como vishing (uso del teléfono con fines delictivos). El usuario recibe una llamada telefónica que simula proceder de una entidad bancaria solicitándole que verifique una serie de datos.

3. Consejos para protegerse del phishing

No contestes automáticamente a ningún correo que solicite información personal o financiera. Las empresas financieras o bancos no solicitan sus datos confidenciales o de tarjetas a través de correos.

No hagas clic en el enlace proporcionado en el correo electrónico.

Comprueba que la página web en la que has entrado es una dirección segura. Para ello, ha de empezar con https:// y un pequeño candado cerrado debe aparecer en la barra de estado de nuestro navegador.

Si recibes un email sospechoso, ignóralo y no respondas.

Si sospechas que has sido víctima de phishing cambia tus contraseñas y ponte en contacto inmediatamente con la entidad financiera para informarles.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Carding

1. ¿Qué es el carding?

Es el uso (o generación) ilegítimo de las tarjetas de crédito (o sus números), pertenecientes a otras personas con el fin de obtener bienes realizando fraude con ellas. Se relaciona mucho con malas prácticas del hacking y el cracking, mediante los cuales se consiguen los números de las tarjetas.

Su objetivo es hacerse con los datos numéricos de la tarjeta, incluido el de verificación.

Puede realizarse a través del teléfono, esto es, un operador te convence para que le des tú número de tarjeta de crédito, o a través de Internet recibiendo un correo electrónico fraudulento en el que nos solicitan estos datos.

Los importes de las compras serán pequeños y secuenciales, para evitar levantar sospechas y que sea difícil darse cuenta de que la estafa está sucediendo.

2. ¿Cómo evitarlo?

Hay que evitar abrir correos en los que nos piden nuestros datos personales o financieros.

En ningún caso dar nuestros datos bancarios por teléfono.

Por ello, las empresas emisoras de tarjetas de crédito hacen hincapié en que jamás enviarán un email o mensajes por móvil solicitando el número de tarjeta del cliente, la fecha de expiración, etc.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Trashing

1. ¿Qué es el trashing?

Consiste en obtener información privada a partir de la recuperación de archivos, documentos, directorios e, incluso, contraseñas que el usuario ha enviado a la papelera de reciclaje de su equipo.

Si la información se recolecta de «las papeleras» (papeles, discos duros) se habla de trashing físico. Cuando el atacante procura conseguir información revisando los archivos que puedan estar en el ordenador (papelera de reciclaje, historial de navegación, o los archivos que almacenan cookies), se denomina trashing lógico.

2. ¿Qué se debe hacer para evitarlo?

Utiliza técnicas adecuadas de destrucción de la documentación, bien a través de destructoras de papel o bien a través de depósitos de papel que garantizan que no se puede acceder a ellos y, posteriormente, se destruirá su contenido por empresas especializadas.

Tener en cuenta, en las políticas de seguridad, el trashing, formando a los usuarios adecuadamente.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Pharming

1. ¿Qué es el pharming?

Es el método utilizado normalmente para realizar ataques de phishing, redirigiendo el nombre de dominio (DNS) de una entidad de confianza a una página web, en apariencia idéntica, pero que en realidad ha sido creada por el atacante para obtener los datos privados del usuario, generalmente datos bancarios.

2. ¿Cómo se produce?

Cuando un usuario teclea una dirección en su navegador, ésta debe ser convertida a una dirección IP numérica. Este proceso es lo que se llama resolución de nombres, y de ello se encargan los servidores DNS. Sin embargo, existen ejemplares de malware diseñados para modificar el sistema de resolución de nombres local, ubicado en un fichero denominado HOSTS que permite almacenar de forma local esa resolución de nombres asociadas a direcciones IP.

Los ataques mediante pharming pueden realizarse de dos formas: directamente a los servidores DNS, con lo que todos los usuarios se verían afectados, o bien atacando a ordenadores concretos, mediante la modificación del fichero HOSTS.

A diferencia del phishing, el pharming no se lleva a cabo en un momento concreto, ya que la modificación del fichero HOSTS permanece en un ordenador a la espera de que el usuario acceda a su servicio bancario.

3. ¿Cómo protegernos?

Evita sitios web sospechosos y no hagas clic en enlaces de correos electrónicos que parezcan sospechosos.

Instala antimalware y antivirus potentes.

Verifica que los sitios webs que visitas, sobre todo aquellos que contienen información personal o financiera, tengan el icono de candado.

Evita páginas web que parezcan extrañas, o con una dirección IP extraña.

No des datos personales si empiezan a solicitártelos cuando, normalmente, no lo hacen.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Oversharing

1. ¿Qué es el oversharing?

Es la sobreexposición de información personal en Internet, en particular en las redes sociales a través de los perfiles de los usuarios.

2. ¿Qué consecuencias puede tener?

El exceso de información facilitada en Internet, así como el comportamiento de los usuarios en las propias redes sociales a través de sus identidades virtuales, suponen una información fácil de aprovechar por usuarios malintencionados que facilita la comisión de determinadas conductas que nos pueden ocasionar daños materiales, inmateriales y físicos. Cuanta más información se comparta en la red, más riesgo hay de robo y suplantación de identidad.

3. ¿Cómo evitar las consecuencias del oversharing?

Configura la privacidad de la red social para determinar quién puede acceder a tu información e imágenes.

Utiliza contraseñas robustas para proteger el acceso a los perfiles en las redes sociales.

Reflexiona antes de publicar información o imágenes.

Evita compartir información personal sensible.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Geolocalización

1. ¿Qué es la geolocalización?

Es la capacidad para obtener la ubicación geográfica real de un objeto, como un teléfono móvil o un ordenador conectado a Internet y proporciona el sitio en el que se encuentra el usuario. La geolocalización puede utilizarse de forma deductiva, o bien para la consulta real de la ubicación.

2. Beneficios y riesgos

Nos podemos beneficiar como usuarios de las aplicaciones móviles que nos permiten saber cómo llegar a un lugar, cómo indicar dónde nos encontramos y obtener información útil de nuestro entorno.

Pero tenemos que ser conscientes de que existen aplicaciones que utilizan la geolocalización y que terceros pueden aprovecharse de esas aplicaciones para fines lucrativos o maliciosos, sin que nosotros lo sepamos, por ejemplo, para saber que no hay nadie en casa y entrar a robar, o para acosar a una persona. Se tiene que ser precavido a la hora de facilitar a alguien nuestra ubicación.

3. Consejos para hacer un buen uso de la geolocalización

Desactiva los servicios basados en la localización geográfica cuando no los estés usando.

No des tu localización si no es a personas de confianza que ya conoces fuera de la red.

No envíes fotos de dónde te encuentras ni información sobre si estás o no en casa.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Busca ayuda

1. Agencia Española de Protección de Datos

Sede electrónica

2. Policía y Guardia Civil

ALERTCOPS

3. Violencia de género

Teléfono de Información a la Mujer: 016
www.violenciagenero.msssi.gob.es

4. Ministerio de Educación, Cultura y Deporte

Atención a casos de acosos en centros educativos: **900 018 018 – 600 909 073**

5. INCIBE

- is4K-Internet segura para FORKIDS: 900 116 117
www.is4k.es

6. Otros recursos

ANAR: 900 20 20 10
www.anar.org

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS