GUÍA DE CIBERSEGURIDAD PARA MUJERES EN EL MEDIO RURAL DE CANTABRIA

GOBIERNO DE ESPAÑA
MINISTERIO DE DERECHOS SOCIALES Y AGENDA 2030
POR SOLIDARIDAD
OTROS FINES DE INTERÉS SOCIAL

Colectivos Acción Solidaria

ASOCIACIÓN La Columbeta

GOBIERNO DE ESPAÑA
MINISTERIO DE DERECHOS SOCIALES Y AGENDA 2030
POR SOLIDARIDAD
OTROS FINES DE INTERÉS SOCIAL

colectivos acción solidaria

ASOCIACIÓN La Columbeta

INTRODUCCIÓN

La falta de prevención es la madre de todos los problemas informáticos. Muchos de los riesgos de seguridad informática que asumimos se deben a la falta de conocimientos en esta materia. Ignoramos lo que son capaces de hacer los ciberdelincuentes y, como consecuencia, realizamos conductas que pueden convertirnos fácilmente en víctimas.

A veces los ciberdelincuentes se aprovechan de las vulnerabilidades de los sistemas informáticos (por ejemplo, de los sistemas operativos) para poder entrar en los mismos y realizar actividades ilegales, robar información sensible o interrumpir su funcionamiento.

Es recomendable actualizar a las últimas versiones, las aplicaciones informáticas, sistemas de protección y sistemas operativos, pues esas actualizaciones contienen muchas correcciones sobre vulnerabilidades descubiertas.

Amenazas informáticas

Es toda aquella acción que aprovecha una vulnerabilidad para atacar o invadir un sistema informático.

¿Qué es la ciberseguridad y para qué sirve?

La ciberseguridad es el conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos

PISHING

NO MUERDAS EL ANZUELO

¿Qué es el pishing?

Es una estafa que tiene como objetivo obtener a través de internet datos privados de los/as usuarios/as, especialmente para acceder a sus cuentas o datos bancarios.

Como evitarlo:

¡PRECAUCIÓN! Ante correos que aparentan ser de entidades bancarias o servicios conocidos (Dropbox, Facebook, Google Drive, Apple ID, Correos y Telégrafos, Agencia Tributaria, etc.) con mensajes que no esperabas, que son alarmistas o extraños.

¡ERRORES GRAMATICALES! Pueden haber utilizado un traductor automático para la redacción del mensaje trampa. Ningún servicio con cierta reputación enviará mensajes mal redactados.

¡COMUNICACIÓN ANÓNIMA! Como por ejemplo: "Estimado cliente", "Notificación a usuario" o "Querido amigo", es un indicio que te debe poner en alerta.

¡NO DISPONER DE TIEMPO! Si el mensaje te obliga a tomar una decisión de manera inminente o en unas pocas horas, es mala señal. Contrasta directamente si la urgencia es real o no directamente con el servicio o consultando otras fuentes de información de confianza: la OSI, Policía, Guardia Civil, etc.

¡USO DEL DOMINIO! Un servicio con cierto prestigio utilizará sus propios dominios para las direcciones de email corporativas. Si recibes la comunicación desde un buzón de correo tipo @gmail.com, @outlook.com o cualquier otro similar, sospecha.

SOLICITUD DE DATOS BANCARIOS + DATOS PERSONALES = FRAUDE.

Cómo actuar si detectas un phishing:

- No facilites la información que te solicitan ni contestes en ningún caso a estos mensajes.
- En caso de duda consulta directamente a la empresa o servicio que supuestamente representan a través de sus canales oficiales.
- No accedas a los enlaces facilitados en el mensaje ni descargues ningún documento adjunto que puede contener, podría tratarse de malware.
- Elimínalo y si puedes, alerta a tus contactos sobre este fraude para que ellos no caigan tampoco en la trampa.

Qué hacer si has caído en la trampa

Recopila toda la información que te sea posible: correos, capturas de conversaciones mediante mensajería electrónica, documentación enviada, etc. Puedes apoyarte en testigos online para la recopilación de evidencias.

⇒ Para los casos de phishing bancario, **contacta con tu oficina bancaria para informarles de lo sucedido** con tu cuenta online. Adicionalmente, modifica la contraseña de todos aquellos servicios en los que utilizases la misma clave de acceso que para el servicio de banca online.

Recuerda: no uses la misma contraseña en varios servicios, es muy importante gestionar de forma segura las contraseñas para evitar problemas.

⇒ Presenta una **denuncia** ante las Fuerzas y Cuerpos de Seguridad del Estado (FCSE).

HISTORIETA:

"El día que María estuvo a punto de morder el anzuelo".

Aquel sábado, Carmen había quedado con sus amigos/as. Bajó hasta el comedor donde estaba su madre, María, para pedirle un poco de dinero, pero lo que vio le dejó de piedra:

¡su madre estaba siendo engañado por un correo falso!

Comencemos por el principio. María estaba revisando su correo electrónico. En ese momento le llegó un correo de su banco, el Banco Rural Cántabro, en el que le comunicaban que "habían incorporado a sus sistemas un servicio antifraude que eliminaría la posibilidad de accesos fraudulentos a su cuenta". También le especificaban que debería activar ese servicio antes de 48 horas o su cuenta quedaría bloqueada.

A primera vista le pareció perfecto, ya que todo sistema que aumentara la seguridad de su cuenta era bienvenido. Además, desde la entidad habían sido muy considerados y facilitaban un enlace para que de forma sencilla pudiera activar dicha funcionalidad. Pero al pulsar en el enlace, se llegaba a una página web en la que le solicitaban datos tales como la clave de seguridad, tarjeta de coordenadas (primeros 24 números), datos personales, número de tarjeta, fecha de vencimiento, csc, pin, usuario, clave y firma electrónica, todos datos de carácter confidencial y necesarios para realizar operaciones con la cuenta.

Fue en ese momento cuando llegó Carmen, ¡y menos mal que llegó!, ya que su madre se encontraba cumplimentando dichos campos. María no se había dado cuenta que se encontraba en una web fraudulenta y que si hubiera pulsado el botón completar, sus datos bancarios hubieran llegado a manos de ciberdelincuentes, que podrían haber operado con su cuenta bancaria.

Carmen instó a su madre a que siguiera una serie de trucos a fin de poder detectar si un correo es legítimo o se trata de un intento de phishing.

¿Qué es pentesting?

Es un ataque a un sistema informático con la intención de encontrar las debilidades de seguridad y todo lo que podría tener acceso a ella, su funcionalidad y datos. El proceso consiste en identificar el o los sistemas del objetivo.

De esta forma, se puede determinar:

- Si el sistema informático es vulnerable o no.
- Evaluar si las defensas con las que cuenta, son suficientes y eficaces.
- Valorar la repercusión de los fallos de seguridad que se detecten.

Tipos de pruebas de pentesting:

- **De caja blanca:** disponen de toda la información sobre los sistemas, aplicaciones e infraestructura, pudiendo simular que el ataque se realiza por alguien que conoce la empresa y sus sistemas.
- **De caja gris:** dispone de algo de información pero no de toda.
- **De caja negra:** no dispone de información sobre nuestros sistemas; en este caso, se simula lo que haría un ciberdelincuente ajeno.

Pentest: test de seguridad para prevenir ciberataques

Es un método para evaluar los sistemas de información y la red de una organización simulando un ataque para encontrar vulnerabilidades que permitirían a potenciales atacantes robar información o afectar los activos de la misma (malware, ataques DoS, etc.). Las medidas y controles de seguridad son analizados para encontrar debilidades, fallos técnicos y vulnerabilidades.

Estas pruebas se realizan utilizando técnicas y herramientas similares y en muchos casos las mismas que utilizan los atacantes, pero sin perjudicar a la organización ni realizar actividades ilícitas.

Beneficios de los pentests

–Descubrir las debilidades en la seguridad de las TIC de la organización antes que los atacantes.

–Definir planes de acción correctivos y preventivos de ciberseguridad y justificar a la alta dirección las inversiones requeridas.

Los pentests son básicos para la seguridad, previene ataques virtuales y sabe responder en caso de incidentes.

ADWARE

PUBLICIDAD NO DESEADA

¿Qué es el adware?

Es cualquier programa que automáticamente muestra u ofrece publicidad, ya sea incrustada en una página web mediante gráficos, carteles, ventanas flotantes, o durante la instalación de algún programa al usuario, con el fin de generar lucro a sus autores.

¿Cómo se cuela?

- **Tiendas de aplicaciones de terceros** o aplicaciones consideradas por nuestro dispositivo como poco seguras, descargadas directamente de alguna página en internet.
- **Navegación por determinados sitios web** no seguros o de dudosa reputación que hacen uso de vulnerabilidades en los navegadores (llamadas exploits) para descargar sin consentimiento y sigilosamente el adware.
- Una vez que el adware 'secuestra' el dispositivo, puede analizar la ubicación y los sitios web que visita y mostrar anuncios acordes a su ubicación e intereses.

¿Cómo saber si se está infectado?

- Iconos misteriosos que aparecen de golpe en la pantalla de inicio.
- Anuncios de forma masiva que empiezan a bloquear la pantalla del dispositivo.
- Algunos ejemplos de ventanas emergentes, son los anuncios con programas para perder peso milagrosamente, ofertas con secretos para hacerse rico y falsas advertencias sobre virus que invitan a hacer clic sobre ellas.
- Enlaces que redirigen a sitios web diferentes de los que deberían.
- Navegador web muy lento.
- Instalación automática de aplicaciones de software no deseadas.
- El navegador se bloquea.

Ranking de software malicioso lo ostentan los siguientes:

- **Helper-** Se utiliza para descargar otras aplicaciones maliciosas y mostrar anuncios. La aplicación es capaz de evadir los programas antivirus móviles, así como reinstalarse por sí misma en caso de que el usuario la elimine.
- **AndroidBauts –** Adware dirigido a usuarios/as de Android que extrae IMEI, IMSI, localización GPS y otra información de dispositivos y permite la instalación de aplicaciones y accesos directos de terceros en dispositivos móviles.

• **Lotoor–** Herramienta de hacking que explota vulnerabilidades en el sistema operativo Android para obtener privilegios de root.

Medidas de protección

• La mejor forma de bloquear los anuncios emergentes es utilizar uno distinto, **desactivar JavaScript, o instalar un bloqueador de anuncios.**

• Con la tecla 'Atrás' de Android. También podemos **limpiar el historial y la caché**, lo que evitará que los anuncios vuelvan.

• **Descargar un programa de seguridad informática** legítimo, ya que están diseñados para buscar y destruir adware y cualquier tipo de malware o virus que pueda estar infiltrándose.

• Realizar un **análisis cada cierto tiempo** y si en nuestro móvil se esconde alguno de estos programas, lo identificará y eliminará.

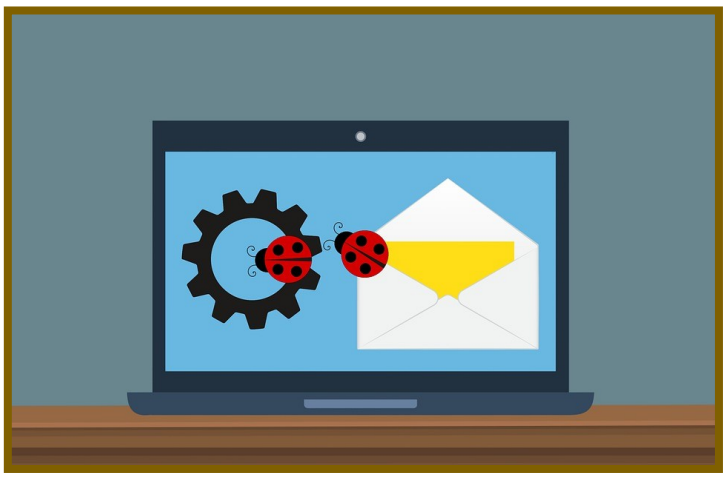
• **Cambiar las contraseñas**, tanto de la cuenta asociada al dispositivo, como la del correo electrónico, redes sociales, páginas web favoritas de compra en línea y de los centros de banca online que utilicemos.

Algunas recomendaciones:

• Utilizar una red **wifi segura.**

• **Supervisar el correo electrónico**. No hacer clic en enlaces de correo electrónico, ni en otros mensajes, ya que estos pueden llevar a sitios web de robo de datos o suplantación de identidad (phishing).

• **SMS y mensajería instantánea.** Algunos mensajes fraudulentos tratan de hacer que el/la usuario/a haga clic en un enlace o facilite cierta información, por lo que debemos permanecer atentos y eliminar estos mensajes, bloqueando también si es posible al remitente.



¿Qué es Man in the Middle?

Es un ataque en el que se adquiere la capacidad de leer, insertar y modificar a voluntad. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas y procurar que ninguna de las víctimas conozca que el enlace entre ellos ha sido violado.

Cómo protegernos de ataques Man in the Middle

Evitar las redes públicas y abiertas

Debemos asegurarnos de que las redes a las que accedemos son reales, seguras y que no van a ser un problema para nuestra seguridad. Así podremos proteger la información a la hora de navegar. **Hablamos por ejemplo de un Wi-Fi que nos encontremos en un aeropuerto o centro comercial**. No sabemos realmente quién puede estar detrás y de qué manera podría interceptar la conexión y afectarnos.

Usar herramientas para navegar en HTTPS

Si navegamos por páginas HTTP nuestra información puede ser interceptada. Esto hace que algo básico para evitar ser víctimas de este tipo de ataques sea navegar solo a través de páginas HTTPS, que son aquellos sitios cifrados.

Ahora bien, podemos hacer uso de herramientas que nos ayudan a ello. Hay extensiones que nos permiten navegar únicamente por sitios HTTPS y de esta forma no comprometer nuestros datos. También, los navegadores más modernos suelen lanzar un aviso cuando intentamos entrar en una web que no es segura. Esto puede servirnos de ayuda para no entrar en páginas que puedan ser un peligro.

Utilizar servicios VPN

El uso de servicios VPN puede ayudar a prevenir los ataques Man in the Middle cuando navegamos por páginas que no estén cifradas o desde redes Wi-Fi públicas. Hay muchas opciones tanto gratuitas como de pago y tienen como objetivo cifrar nuestras conexiones. Es un tipo de herramientas que debemos considerar.

Las podemos usar tanto en ordenadores como también en móviles. Así podemos navegar con mayores garantías y no tener problemas. Incluso nos permiten acceder a determinados sitios que puedan estar restringidos según la ubicación geográfica que tengamos, como sería por ejemplo si estamos de viaje y queremos ver contenido de España que pueda estar limitado.

Proteger nuestras cuentas

Con esto nos referimos a utilizar contraseñas que sean fuertes y complejas, pero también el uso de métodos como la autenticación en dos pasos para evitar que alguien pudiera acceder.

Es importante que nuestras cuentas en Internet estén perfectamente protegidas.

Cuidado con los correos electrónicos

Debemos tomar precauciones a la hora de abrir, leer o responder correos que recibimos. Siempre hay que asegurarse de que el emisor es realmente quien dice ser y no es un impostor que pueda recopilar nuestra información. Es un medio muy usado por los/as piratas informáticos para lanzar sus ataques, robar claves de acceso o afectar a la seguridad de alguna manera.

Mantener los sistemas actualizados

Por supuesto algo que no puede faltar es tener los sistemas y aplicaciones actualizados. Con esto nos referimos al sistema operativo, al navegador, así como a cualquier otro tipo de herramientas que utilicemos. Hay que tener en cuenta que en ocasiones surgen vulnerabilidades que pueden ser aprovechadas por los piratas informáticos para llevar a cabo sus ataques.

¿Qué es el malvertising?

Es más que otra técnica para intentar infectar nuestros equipos. El nombre de esta práctica viene de las palabras "malicious advertising" (publicidad maliciosa) y lo que hace es esconder malware para infectar nuestros dispositivos en los espacios de publicidad de otras páginas webs.

Pero para entender bien que es el malvertising debemos saber qué es el adware, que es su hermano mayor. (pág 4)

¿Cómo protegernos?

- Mantener nuestros sistemas siempre actualizados.
- Instalar y habilitar sólo los complementos de los navegadores necesarios para el día a día.
- Leer los permisos que nos solicitan los complementos o plugins antes de instalarlos.
- Debemos tener nuestro software de seguridad actualizado: antivirus, antimalware y antispyware.
- Instalar siempre la última versión de nuestro navegador.
- Actualizar siempre programas como Java o Adobe, desde sus sitios oficiales.
- Habilitar la función "click-to-play" disponible en todos los navegadores, de manera que antes de ejecutar cualquier plugin el usuario debe permitir dicha ejecución.

Enciende el botón del menú de Chrome y haz clic en la opción Configuración. Haga clic en Mostrar configuración avanzada y, a continuación, en Configuración de contenido en Privacidad. Desplácese hacia abajo hasta que aparezca una opción que diga «**Click to Play**».

PRETEXTING

VERIFICA CON QUIEN HABLAS POR TELÉFONO

¿Qué es el pretexting?

Es un tipo de ataque de ingeniería social que involucra una situación, o pretexto, creado por un atacante con el fin de atraer a una víctima a una situación vulnerable y engañarla para que brinde información privada, específicamente información que la víctima normalmente no daría fuera de la red.

¿Cómo sucede?

Los/as pretexters usualmente se hacen pasar por compañeros/as de trabajo, autoridades, bancos, investigadores de seguros u otras instituciones o negocios oficiales. Esencialmente cualquier persona que pueda tener algún tipo de autoridad o un derecho a saber sobre el objetivo. El atacante solo necesita preparar respuestas a las preguntas que su víctima pueda hacerle. Por lo general, todo lo que necesitan es el tono correcto y algunas habilidades de improvisación para engañar a la mayoría de las personas.

Los ataques de texto previo a menudo se utilizan para obtener datos confidenciales y no confidenciales.

> El año pasado, por ejemplo, un grupo de estafadores se hizo pasar por representantes de agencias de modelos y servicios de acompañantes. Fabricaron fondos falsos y preguntas de entrevistas para convencer a las mujeres y las adolescentes de que les enviaran fotos de ellas desnudas. Luego, vendieron esas fotos a negocios pornográficos por dinero.

El ingrediente clave de la ingeniería social es la confianza.

Los/as estafadores/as deben inspirar confianza en sus víctimas, de lo contrario, probablemente fracasarán. Un buen pretexto es una parte fundamental para generar confianza. Si el alias, la historia o la identidad del atacante tienen agujeros o carecen de credibilidad o incluso de la percepción de credibilidad, lo más probable es que la víctima lo descubra.

Cómo defenderte contra el pretexto.

Como cualquier otra buena defensa, debe ser proactivo en lugar de reactivo. Si, por ejemplo, recibe un correo electrónico de alguien que dice que un/a trabajador/a de mantenimiento se presentará en su lugar, comuníquese con la compañía del remitente, no con el remitente.

Llámalos y asegúrate de que realmente están enviando a alguien. Si está en casa cuando se presenten, exija hablar con su superior, en lugar de simplemente tomar su palabra. Pídales el número corporativo de la compañía y el nombre de su supervisor, para que pueda llamarlos para confirmar la identidad de la persona en su hogar.

¿Qué es la sextorsión?

Es una forma de explotación sexual, en la cual una persona es inducida o chantajeada generalmente por aplicaciones de mensajería por Internet con una imagen o vídeo de sí misma desnuda o realizando actos sexuales, mediante sexting.

¿Cómo evitar el sexting?

Los padres y madres deben procurar dar a sus hijos/as una buena educación digital donde se hable abiertamente de este tema y sus consecuencias.

Es su responsabilidad generar un clima de confianza suficiente para que su hijo/a, ante una situación de este tipo, no dude en pedir ayuda cuanto antes porque el miedo y la vergüenza son el peor enemigo y el arma que los chantajistas utilizan para que la situación no cese y vaya siempre a mas.

Todos cometemos errores, pero detectarlos y frenarlos a tiempo es la mejor solución para prevenir problemas mayores.

Para ello, hay dos grandes frentes para proteger a los menores de esta práctica:

1. Educación y responsabilidad digital: La concienciación sobre los peligros que acarrea esta práctica, explicar las consecuencias que tiene sí lo practican , y saber qué hacer si los menores se encuentran ante un extorsionador sexual es imprescindible.

2. Acompañamiento y supervisión digital: Utilizar un app control parental, configurar correctamente los dispositivos, y usar un filtro de contenido además de configurar correctamente la privacidad de las aplicaciones y redes sociales que utilicen es primordial para mantener seguro el contenido almacenado y evitar contactos peligrosos.

También es importante revisar la seguridad de la red Wifi del hogar para evitar hackers y ciber delincuentes que accedan a nuestros dispositivos y roben contenido.

¿Cuáles son los riesgos de Sextear?

Son innumerables los casos de jóvenes han compartido fotografías o videos con alguien que creían de confianza y, tras perder el control de ese contenido, han acabado sufriendo sus consecuencias al ver que sus imágenes han viralizado en la red, o caído en manos de alguien

que ahora le chantajea pidiendo dinero a cambio de no difundirlo, solicitando más contenido sexual, o incluso obligando a mantener relaciones sexuales.

Los principales riesgos de esta práctica son los siguientes:

1. Las imágenes son usadas para acosar sexualmente a la víctima: Existen muchos casos de exparejas que se han chantajeado con fotos sexuales, videos de contenido sexual que compartieron en el pasado y han acabado siendo utilizadas para conseguir encuentros sexuales o siendo filtradas en diferentes redes y grupos de Whatsapp.

2. Las imágenes acaban en manos de terceros y son usadas sin el consentimiento de la persona para crear perfiles falsos, webs de fotos, o incluso para convertirse en anuncios pornográficos.

3. Las imágenes caen en manos de Groomers y pederastas ya sea por engaño, suplantación de identidad, o porque hackean el teléfono de la víctima. Este es uno de los riesgos más peligrosos porque generalmente son utilizadas para extorsionar al menor pidiendo dinero o más contenido sexual. Esto es lo que se denomina Grooming, extorsión sexual, y en casi la totalidad de los casos acaba causando problemas graves en el menor.

4. Campañas de sextorsión dirigidas a adolescentes orquestadas por grupos de ciberdelincuentes organizados. Este probablemente sea el mayor de los riesgos de 'sextear' por el gran alcance que tienen, ya que existen bandas organizadas que han encontrado un modelo de negocio a través de esta práctica.

El abuso y explotación sexual contra menores a través de Internet es una realidad. Puede resultar difícil de asumir, pero cualquier persona menor de edad puede convertirse en víctima de alguna de sus múltiples variantes. Por ese motivo la implicación de la familia, la escuela y la sociedad en su conjunto es esencial para conocer, prevenir, reducir y afrontar este tipo de riesgos.

SPEAR PISHING

DETRÁS DE UN CONOCIDO PUEDE ESCONDERSE UN CIBERDELINCUENTE

¿Qué es el Spear Pishing?

Consiste en una modalidad phishing dirigida contra un objetivo específico, en el que los atacantes intentan, mediante un correo electrónico, conseguir información confidencial de la víctima.

¿Cómo podemos evitar ser víctima de un ataque de Spear Phishing?

Como usuarios/as, estamos más prevenidos sobre los ataques de phishing, hemos aprendido a reconocerlos con el tiempo y cada vez es menos probable que mucha gente caiga víctima de estos ataques. Sin embargo, estamos mucho menos atentos a detectar ataques de spear phishing, que son mucho más sofisticados y están mucho más trabajados. Pero esto no quiere decir que no sean evitables.

Lo primero que se debe hacer, es formarnos y capacitarnos en materia de ciberseguridad. **Es recomendable** instalar soluciones de seguridad que eviten que los emails fraudulentos lleguen a la bandeja de entrada. Muchos servidores de correo electrónico detectan ya emails falsos, se trata de ir un paso más allá e instalar una capa extra de seguridad.

Tener cuidado con la información personal que compartimos en redes sociales u otras plataformas de Internet. Los phishers que llevan a cabo este tipo de ataques recopilan toda la información posible para personalizarlos y hacernos creer que son auténticos, así que procuremos no publicar información relativa a nuestro trabajo, por ejemplo.

Hemos dicho que los/as ciberdelicuentes emplean direcciones de email muy similares a las auténticas en este ataque, por ello, siempre debemos **comprobar la dirección del remitente**, especialmente si el correo que hemos recibido no lo esperábamos, resulta mínimamente sospechoso o contiene instrucciones que nos indiquen que pulsemos en un enlace, facilitemos datos personales o cuentas de usuario o nos descarguemos algún archivo adjunto. Si nos fijamos en la dirección de correo del remitente y la comparamos con otro legítimo, podremos ver que son diferentes.

Si aún te quedan dudas ante un posible correo fraudulento, lo más recomendable es preguntar directamente a la persona o entidad que te lo ha enviado, pero ojo, no respondiendo al email que crees que puede ser falso, sino desde un nuevo email, introduciendo tú la dirección de correo del supuesto remitente o incluso llamándole por teléfono. Así podrás asegurarte de si realmente te ha escrito ese email.

En definitiva, como con cualquier ciberamenaza, la mejor defensa en este caso es la precaución y la desconfianza.

Spear phishing vs. phishing: Diferencias y similitudes

- Mientras en el primero, se envían unos pocos correos concretos personalizados con datos reales de la víctima y sus circunstancias, en el segundo se envían correos masivos, muchas veces traducidos literalmente de otro idioma y con un contenido genérico. Es la diferencia entre «Estimado cliente» y «Estimado (nombre de la víctima).
- Ambos ataques emplean el correo electrónico como medio para llegar a sus víctimas, pero a diferencia del ataque de phishing, que está mucho menos elaborado, en el spear phishing el phisher dedica bastante tiempo a reunir información de su objetivo y elaborar un contenido cuidado y realista basado en ella.
- Los intentos de phishing se dirigen a todo tipo de personas, mientras que el spear phishing está más dirigido a empresas u organizaciones, siendo los objetivos empleados de las mismas.
- Finalmente, en ambos casos, la intención del ataque es, generalmente, conseguir dinero de las víctimas (aunque también hay casos de hackers que llevan a cabo ataques sobre empresas y organizaciones para mostrar las vulnerabilidades de sus sistemas y no por un motivo económico). Si bien, algunos ataques de spear phishing tienen como objetivos organismos e instituciones públicas, a las que pueden bloquear mediante ransomware.

¿Qué es el ciberbullyng?

El ciberacoso, también denominado acoso virtual, es el uso de medios digitales para molestar o acosar a una persona o grupo de personas mediante ataques personales, divulgación de información personal o falsa entre otros medios.

- A menudo **los/as menores hablan abiertamente de su vida en Internet**, y podemos percibir posibles usos poco respetuosos o saludables que nos permitan anticiparnos al problema y reaccionar a tiempo.
- **No dejes pasar conductas llamativas**, como el aislamiento social, bajadas de rendimiento o cambio de círculos de amistades. Confía en tu intuición en estas situaciones, porque es posible que haya un problema de acoso detrás de estos comportamientos. Valora también actitudes agresivas u ofensivas, un repentino incremento de popularidad o cambios sociales entre el alumnado, que puedan señalar la presencia de un posible acosador/a.
- Ante los primeros **indicios o rumores**, investiga sobre la realidad de los hechos. Si llegan a tus oídos noticias sobre posibles conflictos o ataques a un menor, seguramente ya son suficientemente graves como para tomar medidas.
- **Conversa de forma independiente con las personas afectadas** por un posible caso de ciberacoso. Si consideras que existe un problema, habla con cada implicado/a por separado, ya sea el acosador/a, la víctima o potenciales observadores. Así será más fácil crear un clima de confianza y averiguar qué está ocurriendo.
- **No toleres ningún tipo de humillación, burla o ataque.** Debes mostrar una postura coherente y firme, que les haga entender que no habrá excepciones. Ninguna conducta que dañe emocionalmente a un menor, por inocente que pueda parecer, se debe pasar por alto. Así evitaremos que se normalice ciertos niveles de violencia o maltrato, y que puedan incrementarse.

Juego interactivo:

https://www.is4k.es/oca

HACKER VS CIBERDELINCUENTES

PARECE LO MISMO, PERO NO LO ES

"Hacker" y "ciberdelincuente" son dos términos que habitualmente se confunden.

- Un **hacker** es aquella persona que trata de solventar, paliar o informar sobre los problemas de seguridad encontrados en programas, servicios, plataformas o herramientas.
- El **ciberdelincuente** es la persona que buscará sacar beneficio de estos problemas o fallos de seguridad utilizando para ello distintas técnicas como es la ingeniería social o el malware.

¿Qué información pueden robarnos?

Por medio de esta técnica, el/la ciberdelincuente es capaz de hacerse con las credenciales de acceso de la red social de nuestro protagonista, lo que a su vez le da acceso a todo tipo de información tanto del usuario/a como de sus contactos. Sin embargo, esta técnica puede permitirle robar mucha información valiosa, como:

- Datos personales: o correos electrónicos, datos de localización y contacto o incluso números de documentos de identidad.

- Información bancaria y financiera: Número de tarjetas de crédito o de cuentas bancarias.

- Credenciales de acceso a redes sociales y cuentas de correo electrónico.

¿Qué es la mediación parental?

Ess el conjunto de estrategias para acompañar, orientar y supervisar a los hijos e hijas por un buen uso de la Internet y la tecnología, previniendo riesgos y solucionando problemas en línea.

En general, hablar de mediación parental es hablar de dos tipos de estrategias, que son complementarias y deben ponerse en práctica simultáneamente:

- **Mediación activa:** supervisión, acompañamiento y orientación. Supone una implicación de los/as adultos/as, antes, durante y después de que los menores utilicen las tecnologías digitales. Dar ejemplo al utilizar las nuevas tecnologías, hablarles sobre los riesgos reales de Internet e interesarnos sobre su comportamiento online son actitudes educativas que requieren ser parte activa de su desarrollo.

- **Mediación restrictiva:** establecer reglas y límites. Para que los/as menores aprendan progresivamente a navegar con seguridad, sin la compañía de un adulto, es necesario establecer unas normas que irán adaptándose a su edad y madurez. A la hora de poner en práctica estas normas, pueden ser de ayuda las herramientas de control parental, las cuentas de usuario limitado para los/as menores y las aplicaciones diseñadas específicamente para ellos como los buscadores infantiles.

Cómo reaccionar en caso de conflicto

- **Escuchar y dialogar.** Es necesario preguntar a los menores de forma calmada qué ha ocurrido, para poder reunir toda la información y conocer la situación sin juzgarle.

- **Reforzar su autoestima y aconsejarle.** Debe saber que cuenta con ayuda y comprensión, y que no se trata de buscar culpables, sino soluciones. Ya cuando la situación se haya calmado, podremos analizar juntos las causas y prevenir que vuelva a repetirse.

- **Trazar un plan.** Los problemas no van a resolverse solos, es necesario actuar. Evitaremos improvisar, trazando un plan de acción y contando con el/la menor para que comprenda por qué se da cada paso y cómo debe actuar.

- **Buscar ayuda especializada.** Existen líneas de ayuda en las que se puede contactar con psicólogos/as, abogados/as y expertos/as en seguridad y educación. También pueden asesorarnos en el centro educativo o nuestro centro de salud, que tendrán un papel importante en la resolución del problema, ya sea porque el incidente tenga que ver con otros/as alumnos/as o simplemente por ser el lugar donde el/la menor pasa más tiempo y donde más apoyo puede recibir.

En situaciones graves: denuncia.

En los casos más complejos, debemos acudir a los departamentos correspondientes de las Fuerzas y Cuerpos de seguridad o la Fiscalía de Menores.

Cada herramienta de control parental es diferente.

Pueden tener su propia selección de funciones, y su propia manera de gestionarlas para adaptarse a diferentes necesidades familiares. Sin embargo, independientemente de cómo lo lleven a cabo, las funcionalidades de supervisión.

Permite revisar los términos buscados en el dispositivo del menor. En caso de haber alguna búsqueda llamativa, nos daría pie a poder hablar sobre ese tema.

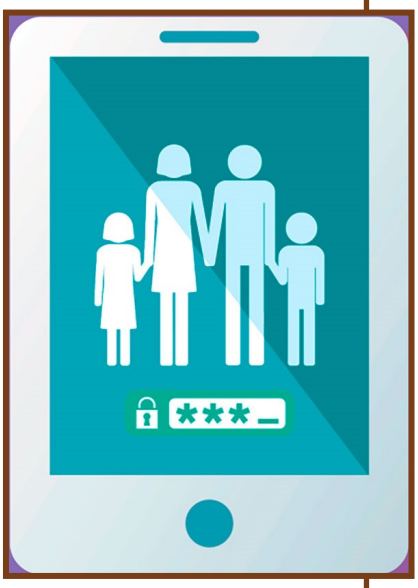
Muestra el conjunto de páginas web visitadas en el dispositivo. Es posible revisarlo aun cuando se hubiera limpiado el historial en el navegador.

Control de tiempos

Monitoriza el tiempo de uso general del dispositivo, y el empleado en cada aplicación, pudiendo obtener resúmenes diarios, semanales, etc.

Configuración de alertas

Establece el envío de alertas y notificaciones a los dispositivos de los padres y madres cuando se detecten ciertas condiciones en el dispositivo del menor. Por ejemplo, cuando se supera el límite de tiempo de uso o se intenta acceder a una aplicación restringida.



¿Qué es?

Una práctica fraudulenta que consiste en el uso de la línea telefónica convencional y de la ingeniería social para engañar personas y obtener información delicada como puede ser información financiera o información útil para el robo de identidad. El término es una combinación del inglés "voice" y phishing.

Ataques de vishing más comunes

- Reembolso por servicio informático. Con el argumento de realizar un reembolso por un servicio que se ha dejado de prestar, los/as ciberdelincuentes persuaden a sus víctimas para que instalen un software en su equipo y accedan a su cuenta bancaria. A continuación, simulan una transferencia al interesado por un valor superior. Y después solicitan que la víctima devuelva la diferencia. Ahí es donde se produce la estafa.
- Soporte técnico y falsa infección con malware. Simulando ser un experto de una empresa especializada en seguridad informática, el atacante convence a la víctima para que le permita acceder a su equipo a través de herramientas de acceso remoto. Una vez permitido el acceso, le informa de una supuesta infección. Y le invita a gastarse una importante suma de dinero para solucionar el problema.
- Problemas financieros o legales. Otro ataque habitual de vishing es la suplantación de la policía, un banco o una firma legal para informar de la existencia de algún problema. El objetivo es obtener información personal de la víctima o acceder a sus dispositivos.
- Conocido en problemas. Por último, simulando ser algún conocido que se encuentra en apuros, los/as atacantes solicitan que se les entregue dinero, físicamente o por transferencia, de manera urgente.

¿Cómo evitar ser víctima del vishing?

Con el fin de que los/as ciudadanos/as no sean víctimas de este tipo de ataque de ingeniería social, la Oficina de Seguridad del Internauta (OSI) de España recomienda poner en práctica los siguientes consejos:

- Evitar compartir información personal.

- Desconfiar de llamadas de números desconocidos o con una numeración sospechosa.
- Comprobar la autenticidad de la llamada
- Utilizar apps de rastreo de llamadas.
- Contactar siempre con los teléfonos oficiales de las entidades.
- Evitar las herramientas de acceso remoto.

Finalmente, es lógico pensar que los/as ciberdelincuentes nos investiguen y conozcan nuestro nombre, dirección, número de teléfono y dirección de correo electrónico. Por ello, es fundamental ser precavido a la hora de compartir, facilitar o publicar datos sensibles en Internet que puedan serles de utilidad.

¿Qué es el Botnet?

Los dispositivos infectados que forman parte de una *botnet* también se conocen como *bots* o zombis. Cualquier equipo que tenga conexión a Internet como ordenadores, servidores, *routers*, etc., puede infectarse y llegar a formar parte de una *botnet*.

¿Cómo se infectan los dispositivos?

• **Troyanos.** Este método suele afectar a dispositivos de usuarios/as como ordenadores, smartphones o tablets. El ciberdelincuente, utilizando técnicas de ingeniería social consigue que la víctima descargue y ejecute un archivo malicioso infectado con malware. El troyano puede esconderse en diferentes sitios, como documentos adjuntos en correos electrónicos, ficheros enviados en servicios de mensajería instantánea o redes sociales, sitios web comprometidos, webs de descarga no oficiales, etc.

• **Vulnerabilidades no parcheadas.** Este vector de ataque puede afectar a cualquier dispositivo, ya que todos ellos pueden contar con vulnerabilidades no parcheadas que pueden llegar a ser explotadas por los/as ciberdelincuentes.

• **Configuraciones inseguras.** Algunos dispositivos como routers suelen contar con configuraciones por defecto poco seguras, así como, con contraseñas débiles. Estas configuraciones débiles son usadas por los/as ciberdelincuentes para obtener acceso al dispositivo y convertirlo en parte de la botnet.

¿Cuál es el objetivo de una botnet?

Este tipo de red generalmente tiene como último fin el beneficio económico de los/as ciberdelincuentes que la han creado. Para lograrlo pueden utilizar la botnet de diferentes maneras:

- **Ataques de denegación de servicio distribuido o DDoS**. En este tipo de ataques, el objetivo de los/as ciberdelincuentes es impedir el correcto funcionamiento de un servicio, como puede ser la página web de una organización con el consiguiente daño de su imagen y reputación. Para conseguirlo ordenan a un gran número de dispositivos zombis que accedan a la vez al mismo servicio, haciendo que este se sature llegando incluso a bloquearse e impidiendo que los/as usuarios puedan utilizarlo. El funcionamiento es similar al de una autopista, cuando el tráfico es el habitual, los vehículos pueden desplazarse con normalidad, pero cuando el trafico aumenta excesivamente se producen retenciones, llegando incluso a tener que detener el vehículo.

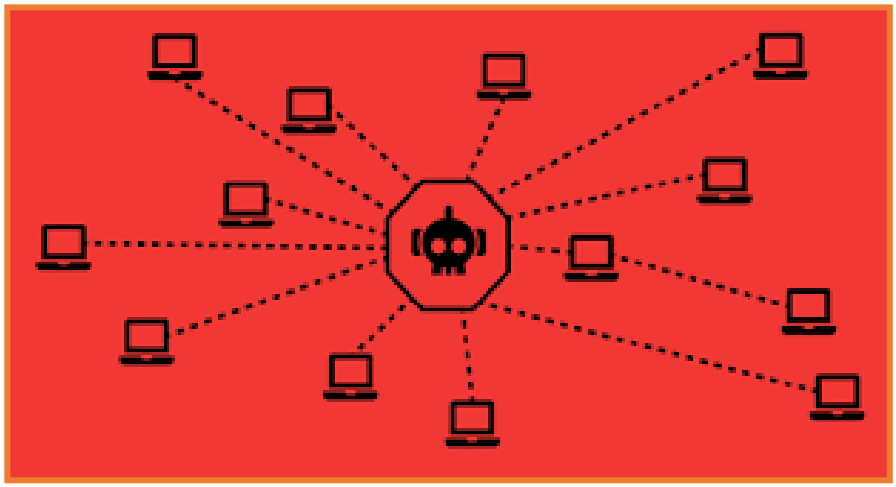
• **Envío de spam**. Los/as ciberdelincuentes utilizan los equipos infectados para enviar correos electrónicos fraudulentos de forma masiva, que en muchos casos incluyen estafas como enlaces a páginas web de tipo *phishing* o *malware*.

• **Fraudes publicitarios**. Normalmente, los servicios de anuncios en Internet pagan a los/as administradores/as de las webs donde figuran en función de varios factores, entre los que se incluye la visualización del anuncio y el hacer clic en el mismo. Los/as ciberdelincuentes ordenan a los *bots* que visiten sus propios sitios web y hagan clic en los anuncios para generar beneficios económicos de manera fraudulenta.

•**Venta y alquiler de la botnet**. Las botnet en algunos casos son alquiladas por usuarios/as que desean realizar algún tipo de actividad delictiva, como perpetrar ataques de denegación de servicio. También pueden ser vendidas en porciones para que los nuevos administradores/as hagan con ella a través de los dispositivos infectados, cualquier tipo de actividad fraudulenta.

• **Minado de criptomonedas**. Las criptomonedas se han convertido en un activo de gran valor, los/as ciberdelincuentes pueden utilizar la capacidad de cómputo conjunta de la botnet para minar criptomonedas sin que los recursos utilizados para ello sean suyos, aumentando de esta forma los beneficios.

•**Robo de información**. La información personal como pueden ser las credenciales de acceso o datos bancarios, es valiosa en sí misma, por ello los/as ciberdelincuentes intentan conseguirla mediante campañas de *phishing* lanzadas desde botnets para posteriormente venderla al mejor postor.



¿Qué es el grooming?

Es una práctica en la que un adulto se hace pasar por un menor en Internet o intenta establecer un contacto con niños/as y adolescentes que dé pie a una relación de confianza, pasando después al control emocional y, finalmente al chantaje con fines sexuales.

Prevención

Establecer unos hábitos de navegación seguros. Acordar unas normas de uso de Internet en casa favorecerá su responsabilidad y su seguridad al conectarse. Debemos establecer unos horarios de uso y cuál será el lugar para usar esos dispositivos, procurando que sean espacios comunes.
Extremar la precaución al conversar online. Para los/as menores, un desconocido puede dejar de serlo si ya han hablado un par de veces por Internet. Puede incluso que el atacante sea una persona que sí conocen en persona. Por ello, en cualquier conversación online debemos ser cautos a la hora de compartir nuestra información personal y mantenernos alerta: no todo es lo que parece.

Evitar prácticas de riesgo. En Internet es bastante fácil que alguien se haga pasar por quien no es. Por ello, es recomendable evitar prácticas como el sexting, así como no contactar o quedar con personas a las que no conocemos en persona. Siempre que alguien proponga un encuentro, comunicárselo a un adulto de confianza.

Ser conscientes del uso que hacen de la cámara del móvil o WebCam. Es necesario plantearnos si son suficientemente maduros/as para tener su propio móvil o dispositivo, con la responsabilidad que eso conlleva. Enviar fotos o realizar videollamadas es un riesgo sobre el que no siempre reflexionan, pueden producir un contenido comprometedor o íntimo sin que ellos/as sean conscientes de ello. Mientras no se estén usando, las cámaras deben estar tapadas, y sólo utilizarse de forma meditada y con precaución.

Comunicación y sensibilización. Hablar con naturalidad del amor y la sexualidad les ayudará a diferenciar las relaciones saludables de las que no lo son. Deben conocer con claridad cómo ocurre una situación de grooming y sus consecuencias para saber cómo protegerse. Además, una buena comunicación nos permitirá conocer sus hábitos en Internet y sus amistades online. Frente a un problema, podrán acudir a nosotros/as o a un adulto de referencia con el que se sientan cómodos.

Acompañamiento y supervisión. El acceso de los/as menores a Internet debe ser progresivo y contar con el respaldo de un adulto, para que aprendan poco a poco cómo utilizar las nuevas tecnologías de forma segura y responsable. Para los/as más pequeños/as, podemos además

instalar sistemas de control parental en los dispositivos, para limitar su uso y supervisar su actividad.

Cómo reaccionar en caso de problemas

Red de apoyo. Deben saber que pueden acudir a los adultos de su confianza en busca de ayuda, ya que se trata de un problema de gravedad. Es el momento de transmitir al menor una actitud de seguridad y madurez para que se sienta protegido.

Ser prudentes y mantener la calma. Si el/la menor ha decidido dar el paso de contarnos lo que está sucediendo, debemos valorar el esfuerzo que eso supone y no dudar o cuestionar sus palabras. No culpabilizar a la víctima y reafirmar nuestro apoyo incondicional.

Recoger información. No debemos dejarnos llevar por la situación o actuar irreflexivamente. Contactar con el acosador o borrar información (contenidos enviados, conversaciones, perfiles en redes sociales, etc.) puede dificultar la resolución del problema o incluso agravarlo.

Nunca aceptar un chantaje. Si nos encontramos ante un/a agresor/aque tiene (o dice tener) alguna información sensible en su poder, nunca debemos ceder a la manipulación, ya que empeorará la situación.

Denuncia. Ante una situación de grooming es imprescindible contactar con las Fuerzas y Cuerpos de seguridad.

Ayuda psicológica. Las consecuencias pueden ser difíciles de afrontar, tanto para el/la menor como para su familia. El centro de salud y su centro educativo pueden ofrecer apoyo emocional y seguimiento si es necesario.

¿Cómo se detectan perfiles falsos?

Suelen centrarse en una temática en concreto, como por ejemplo política, religión, deporte, etc., y no realizan comentarios sobre algún amigo, actividad o contenido que puede demostrar una mínima interacción.

Su contenido en cuanto a imágenes, suele ser además llamativo. En ocasiones utilizarán fotos con poses atractivas de las personas suplantadas que servirán como gancho de atención.

Utilizan datos personales poco fiables, incompletos o con descripciones copiadas.

No suele tener amigos/as en común contigo. Las redes sociales basan sus relaciones en conocimientos previos que te unirán con personas afines a una serie de datos, lo que hace muy extraño peticiones de amistad basadas únicamente en tu foto de perfil, sin conexiones de ningún tipo.

Con los mecanismos de verificación de perfiles que proporcionan las redes sociales se evitan muchos problemas de suplantación

TYPOSQUATTING

CUIDADO CON LO QUE ESCRIBES

¿Qué es el typosquatting?

Es un fenómeno por el cual un/a usuario/a acaba en una página web que no es la que estaba buscando por el hecho de teclear mal por error la URL en su navegador.

Diferentes métodos de cybersquatting

- **Adición.** Consiste en añadir un carácter al final del nombre de dominio "columbetas.es".
- **Sustitución.** Se cambia un carácter del nombre de dominio por otro "columveta.es"
- **Homográfico.** Se sustituye un carácter por otro que a simple vista resulta similar "coLumbeta.es". En esta técnica también se pueden utilizar diferentes alfabetizaciones cuyos caracteres son similares al alfabeto latino "incíbe.es", cuando en realidad pueden pertenecer a otro como por ejemplo al cirílico.
- **Separación.** Consiste en añadir un guion en alguna parte del nombre de dominio "colum-beta.es".
- **Inserción.** Se añade un carácter entre el primero y el último del nombre de dominio "columbeta.es".
- **Omisión.** Se elimina un carácter "colmbeta.es".
- **Subdominio.** Radica en registrar un nombre de dominio con el nombre parcial del legítimo y añadir los caracteres restantes por medio de un subdominio "colum.beta.es".
- **Trasposición.** Alternación del orden de los caracteres del nombre de dominio "oclumbeta.es".
- **Cambio de dominio.** Se utiliza un dominio libre pero utilizando el mismo nombre de dominio "columbeta.eu".
- **Otros.** Algunas otras técnicas utilizadas consisten en añadir "w" al comienzo del nombre o "com" al final, "wwwcolumbeta.es" "columbetacom.es".

Qué hacer ante un caso de cybersquatting

- **Vía judicial.** Puedes acudir a la vía judicial ya que tanto la Ley de Marcas como la Ley de Competencia Desleal te amparan.
- En el caso de dominios .es se establece un sistema de resolución extrajudicial de conflictos previsto en el Plan Nacional de Nombres de Dominio el cual otorga a la Entidad Pública Red.es la función de autoridad de asignación.

Trivial de la Ciberseguridad

https://www.osi.es/es/campana/trivial-de-la-ciberseguridad

¿Qué es el deepfake?

Son vídeos manipulados para hacer creer a los/as usuarios/as que los ven que una determinada persona, tanto si es anónima como si es personaje público, realiza declaraciones o acciones que nunca ocurrieron. Para la creación de dichos vídeos, se utilizan herramientas o programas dotados de tecnología de inteligencia artificial que permiten el intercambio de rostros en imágenes y la modificación de la voz.

Podemos identificar dos tipos de deepfakes:

- **Deepface:** en este caso, se trata de superponer el rostro de una persona en la de otra y falsificar sus gestos. En algunos casos, el resultado es tan realista que resulta muy difícil identificar el engaño o fraude.
- **Deepvoice:** en este otro caso se trataría de unir frases y palabras sueltas utilizadas por una persona para crear un discurso. Incluso, es capaz de clonar la voz original a partir de estos fragmentos

¿Son una amenaza?

Al ritmo al que avanza esta tecnología, en poco tiempo será casi imposible identificar si se trata de una falsificación o no, llegando a crear verdaderos estragos en la credibilidad o reputación de una persona. Si las noticias falsas ya influyen en temas tan importantes como en la crisis sanitaria que estamos viviendo actualmente debido al coronavirus, imaginemos lo que podría conseguirse con las deepfakes.

¿Te imaginas a un personaje conocido con cierta reputación dando unas declaraciones en las que dijera que el COVID-19 es un virus de laboratorio cuyo principal objetivo es reducir el número de habitantes de la Tierra? Aunque parezca mentira, con esta tecnología sería posible manipular imágenes y voz de dicho personaje para poner en circulación un discurso de estas características y crear alama y confusión en la sociedad, además de manchar su imagen personal.

Otro ejemplo, recibes por WhatsApp un vídeo de tu vecina en el que aparece haciendo un baile erótico en una tarima, ¿estás seguro de que ella ha hecho ese baile? ¿O alguien ha creado un deepfake que utiliza su imagen para hacerle daño?

Como puedes ver, las deepfakes pueden resultar una amenaza para la sociedad al tener implicaciones sociales, morales y políticas.

Afortunadamente, grandes compañías como Facebook, Twitter y Google (mediante la herramienta Assembler) están tomando cartas en el asunto para poner freno a este tipo de contenidos multimedia falsos.

¿Cómo se pueden detectar las deepfakes?

Del mismo modo que cada vez hay más y mejores herramientas para crear deepfakes, también la industria está trabajando para desarrollar programas que sean capaces de detectar si una imagen ha sido manipulada, lo cual será de gran ayuda de cara a identificarlos rápidamente.

Busca aquello que no tenga sentido. Si un detective busca pistas que no encajen en la escena del crimen, podemos hacer lo mismo con estos montajes. Busca fondos o formas distorsionadas o sombras que no cuadren con el tipo de iluminación. Cualquier despiste o detalle que demuestre signos de manipulación.

Revisa detenidamente la imagen. Si el rostro, los gestos, el tono de piel o alguna postura no encaja con el resto del cuerpo es posible que nos encontremos ante un montaje. La mayoría de los deepfakes se centran en sustituciones faciales, por lo que los cambios en el resto del cuerpo no se aplican y pueden darnos pistas. Un detalle interesante reside en los tiempos de parpadeo. Un ser humano parpadea, de promedio, en intervalos de 2 a 8 segundos. En este tipo de falsificaciones los personajes suelen parpadear poco y en períodos relativamente largos.

Afina el oído. El audio del vídeo puede delatar a la falsificación. Si el sonido no coincide con la imagen, detectas algún tono fuera de lugar en la voz del protagonista o una falta de sincronización, posiblemente se tratará de una falsificación.

¿Tiene coherencia? En muchas ocasiones se utilizan los deepfakes para degradar la reputación de alguien, crear discordia entre dos bandos o para exagerar algunas declaraciones. Si el contenido del vídeo es muy alarmante, llamativo e incendia las redes en poco tiempo, mantente alerta y desconfía.

Atento/a a la duración del vídeo. Debido al trabajo de edición, estos vídeos suelen ser cortos.

Al final, como cualquier intento de desinformar, las recomendaciones son siempre muy parecidas: revisar la fuente y contrastar la información. No nos cansaremos de repetirlo, pues es fundamental para luchar en esta era de la desinformación.

¡No te creas todo lo que lees y aplica una mentalidad crítica! Es trabajo de todos hacer de Internet un lugar mejor. Los deepfakes así como otros contenidos falsos circulan por la Red a gran velocidad a través de redes sociales, aplicaciones de mensajería o comunidades virtuales y por eso es muy importante aprender a distinguirlos, desarrollando la capacidad crítica en cada uno/a de nosotros/as,

Ataques a contraseñas

Los/as ciberdelincuentes se sirven de diversas técnicas y herramientas con las que atacar a nuestras credenciales. Los/as usuarios/as no siempre les dificultamos esta tarea, y solemos caer en malas prácticas que ponen en peligro nuestra seguridad:

- Utilizar la misma contraseña para distintos servicios.
- Utilizar contraseñas débiles, fáciles de recordar y de atacar
- Utilizar información personal a modo de contraseñas, como la fecha de nacimiento.
- Apuntarlas en notas o archivos sin cifrar.
- Guardar las contraseñas en webs o en el navegador.
- Y, finalmente, hacer uso de patrones sencillos, como utilizar la primera letra en mayúscula, seguida de 4 o 5 en minúscula y añadir 1 o 2 números o un carácter especial. Estos patrones acaban por popularizarse, facilitando aún más la tarea a los ciberdelincuentes

Ataques por ingeniería social Los ataques por ingeniería social se basan en un conjunto de técnicas dirigidas a nosotros/as, los/as usuarios/as, con el objetivo de conseguir que revelemos información personal o permita al atacante tomar control de nuestros dispositivos. Existen distintos tipos de ataques basados en el engaño y la manipulación, aunque sus consecuencias pueden variar mucho, ya que suelen utilizarse como paso previo a un ataque por malware.

Ataques a las conexiones Los ataques a las conexiones inalámbricas son muy comunes, y los/as ciberdelincuentes se sirven de diversos software y herramientas con las que saltarse las medidas de seguridad e infectar o tomar control de nuestros dispositivos. Generalmente, este tipo de bataques se basan en interponerse en el intercambio de información entre nosotros y el servicio web, para monitorizar y robar datos personales, bancarios, contraseñas, etc.

Ataques por malware Los ataques por malware se sirven de programas maliciosos cuya funcionalidad consiste en llevar a cabo acciones dañinas en un sistema informático y contra nuestra privacidad. Generalmente, buscan robar información, causar daños en el equipo, obtener un beneficio económico a nuestra costa o tomar el control de su equipo. Dependiendo del modus operandi, y de la forma de infección, existen distintas categorías de malware. Las medidas de protección, por el contrario, son muy similares para todos ellos y se basan en mantener activas y actualizadas las herramientas de protección antimalware.

GLOSARIO

Amenaza: Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los/as activos/as provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.

Antivirus: Es un programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso (virus, troyanos, gusanos, etc.), así como proteger los equipos de otros programas peligrosos conocidos genéricamente como malware. La forma de actuar del antivirus parte de una base de datos que contiene parte de los códigos utilizados en la creación de virus conocidos. El programa antivirus compara el código binario de cada archivo ejecutable con esta base de datos. Además de esta técnica, se valen también de procesos de monitorización de los programas para detectar si éstos se comportan como programas maliciosos

Análisis de riesgos: Es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo.

Aviso Legal: Un aviso legal es un documento, en una página web, donde se recogen las cuestiones legales que son exigidas por la normativa de aplicación. El aviso legal puede incluir:

1. Términos y condiciones de uso.
2. Política de privacidad y protección de datos si recogen datos de carácter personal según la LOPD (formularios, registro de usuarios/as,…).
3. Información general a la que se hace referencia en al artículo 10 de la LSSI-CE y otra información relativa al uso de cookies, contratación, etc. si aplicara.
4. Qué elementos están sujetos a los derechos de propiedad intelectual e industrial, entre otros: - la propia información de la web - el diseño gráfico - las imágenes - el código fuente - las marcas - los nombres comerciales - el diseño del sitio web

GLOSARIO

Biometría: La biometría es un método de reconocimiento de personas basado en sus características fisiológicas (huellas dactilares, retinas, iris, cara, etc.) o de comportamiento (firma, forma de andar, tecleo, etc.). Se trata de un proceso similar al que habitualmente realiza el ser humano reconociendo e identificando a sus congéneres por su aspecto físico, su voz, su forma de andar, etc. Para la identificación del individuo es necesario que los rasgos o características analizadas sean de carácter universal, ser lo suficientemente distintas a las de otra persona, permanecer de forma constante e invariante en el individuo y además, poder ser medida.

Bluetooth: Es una tecnología inalámbrica de radio de corto alcance, cuyo objetivo es eliminar los cables en las conexiones entre dispositivos electrónicos, simplificando así las comunicaciones entre teléfonos móviles, ordenadores, cámaras digitales y otros dispositivos informáticos operando bajo la banda de radio de 2.4 GHz de frecuencia. Este protocolo ofrece a los dispositivos la posibilidad de comunicarse cuando se encuentran a una distancia de hasta 10 metros, incluso a pesar de que pueda existir algún obstáculo físico o a pesar de que los usuarios de los dispositivos se encuentren en distintas habitaciones de un mismo emplazamiento. Algunas aplicaciones de los dispositivos Bluetooth son:

- Intercambio de ficheros, fichas de contacto, recordatorios.
- Comunicación sin cables entre ordenadores y dispositivos de entrada y salida (impresoras, teclado, ratón).
- Conexión a determinados contenidos en áreas públicas.

Bulo: También llamados hoax, son noticias falsas creadas para su reenvío masivo ya sea a través de redes sociales, mensajería instantánea o correo electrónico, con el fin de hacer creer al destinatario que algo es falso. Pueden ser varias las motivaciones para crear este tipo de noticias, como difundir información falsa en perjuicio de terceras personas u organismos o incitar al receptor del mensaje a causar daños en su propio ordenador.

Cesión de datos: La cesión de datos es la comunicación de datos de carácter personal a una tercera persona sin el consentimiento del interesado. La comunicación de este tipo de datos está regulada en el artículo 11 de la LOPD.

Clave pública: Los sistemas de criptografía asimétrica, se basan en la generación, mediante una «infraestructura de clave pública», de un par de claves, denominadas clave pública y clave privada, que tienen la peculiaridad de que los mensajes cifrados con una de ellas sólo pueden ser descifrados utilizando la otra. Así, se conoce como clave pública a una de estas claves, que puede ponerse en conocimiento de todo el mundo y que utilizará un remitente para cifrar el mensaje o documento que quiere enviar, garantizando de esta forma que tan solo pueda descifrarlo el destinatario con su clave privada.

Clave privada: Los sistemas de criptografía asimétrica, se basan en la generación de un par de claves, denominadas clave pública y clave privada, que tienen la peculiaridad de que los mensajes cifrados con una de ellas sólo pueden ser descifrados utilizando la otra. En este tipo de sistemas, la clave privada sólo debe ser conocida por el usuario para el cifrado y descifrado de mensajes. El hecho de que la clave privada sólo sea conocida por su propietario/a persigue dos objetivos:

• Cualquier documento generado a partir de esta clave necesariamente tiene que haber sido generado por el propietario/a de la clave (firma electrónica).

• Un documento al que se aplica la clave pública sólo podrá ser abierto por el propietario/a de la correspondiente clave privada (cifrado electrónico). Estos sistemas de criptografía constituyen un elemento esencial para la propia seguridad del tráfico jurídico y el desarrollo de transacciones económicas o el comercio on-line.

Cloud computing: El término cloud computing o computación en la nube se refiere a un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es Internet. Esta tendencia permite a los usuarios almacenar información, ficheros y datos en servidores de terceros, de forma que puedan ser accesibles desde cualquier terminal con acceso a la nube o a la red, resultando de esta manera innecesaria la instalación de software adicional (al que facilita el acceso a la red) en el equipo local del usuario. Importantes plataformas ofrecen herramientas y funcionalidades de este tipo y aunque conlleva una importante dinamización y libertad, se debe prestar especial atención a la seguridad de la información, particularmente desde el punto de vista de la protección de la intimidad y de los datos personales, ya que la información, documentos y datos se encuentran almacenados en servidores de terceros sobre los que generalmente no se tiene control.

Confidencialidad: Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad de la información constituye la piedra angular de la seguridad de la información. Junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información.

Control parental: Conjunto de herramientas o medidas que se pueden tomar para evitar que los/as menores de edad hagan un uso indebido del ordenador, accedan a contenidos inapropiados o se expongan a riesgos a través de Internet. Estas herramientas tienen la capacidad de bloquear, restringir o filtrar el acceso a determinados contenidos o programas, accesibles a través de un ordenador o de la red, y de dotar de un control sobre el equipo y las actividades que se realizan con él, a la persona que sea el/la administrador/a del mismo, que normalmente deberá ser el padre, madre o tutor del menor.

Cookie: Es un pequeño fichero que almacena información enviada por un sitio web y que se almacena en el equipo del usuario, de manera que el sitio web puede consultar la actividad previa del usuario/a.

Sus principales funciones son:

- Llevar el control de usuarios: cuando un usuario introduce su nombre de usuario y contraseña, se almacena una cookie para que no tenga que estar introduciéndolas para cada página del servidor.
- Recabar información sobre los hábitos de navegación del usuario. Esto puede significar una ataque contra la privacidad de los usuarios y es por lo que hay que tener cuidado con ellas.

Cortafuegos: Sistema de seguridad compuesto o bien de programas (software) o de dispositivos hardware situados en los puntos limítrofes de una red que tienen el objetivo de permitir y limitar, el flujo de tráfico entre los diferentes ámbitos que protege sobre la base de un conjunto de normas y otros criterios. La funcionalidad básica de un cortafuego es asegurar que todas las comunicaciones entre la red e Internet se realicen conforme a las políticas de seguridad de la organización o corporación. Estos sistemas suelen poseer características de privacidad y autentificación.

GLOSARIO

HTTP: Son las siglas en inglés de Protocolo de Transferencia de Hipertexto. Se trata del protocolo más utilizado para la navegación web. Se trata de un protocolo que sigue un esquema peticiónrespuesta. El navegador realiza peticiones de los recursos que necesita (la web, las imágenes, los videos…) y el servidor se los envía si dispone de ellos. A cada pieza de información transmitida se la identifica mediante un identificador llamado URL (del inglés Uniform Resource Locator). La información enviada mediante HTTP se envía en texto claro, lo que quiere decir que cualquiera que intercepte el tráfico de red puede leer lo que se está enviando y recibiendo. Por esta razón se desarrolló el protocolo HTTPS, en el que la información es cifrada antes de ser enviada por la red.

LAN: Una LAN (del inglés Local Area Network) o Red de Área Local es una red informática de pequeña amplitud geográfica, que suele limitarse a espacios como una oficina, una vivienda o un edificio. Una Red de Área Local permite interconectar distintos dispositivos todo tipo, ordenadores, impresoras, servidores, discos duros externos, etc. Las Redes de Área Local pueden ser cableadas o no cableadas, también conocidas como redes inalámbricas. Por término general las redes cableadas son más rápidas y seguras, pero impiden la movilidad de los dispositivas.

Malware: Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario/a en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: malicious software. Dentro de esta definición tiene cabida un amplio elenco de programas maliciosos: virus, gusanos, troyanos, backdoors, spyware, etc. La nota común a todos estos programas es su carácter dañino o lesivo.

Política de seguridad: Son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riegos a los que están expuestos. Este término también se refiere al documento de nivel ejecutivo mediante el cual una empresa establece sus directrices de seguridad de la información.

Protocolo: Es un sistema de reglas que permiten que dos o más entidades se comuniquen entre ellas para transmitir información por medio de cualquier tipo de medio físico.

Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como también los posibles métodos de recuperación de errores. Los protocolos pueden ser implementados por hardware, por software, o por una combinación de ambos.

Proxy: El proxy es tanto el equipo, como el software encargado de dar el servicio, que hacen de intermediario en las peticiones de los equipos de la redes LAN hacia Internet. Su cometido es de centralizar el tráfico entre Internet y una red privada, de forma que se evita que cada una de las máquinas de la red privada tenga que disponer necesariamente de una conexión directa a Internet y una dirección IP pública. A mismo tiempo un proxy puede proporcionar algunos mecanismos de seguridad (firewal o cortafuegos) que impiden accesos no autorizados desde el exterior hacia la red privada.

Router: Es un dispositivo que distribuye tráfico de red entre dos o más diferentes redes. Un router está conectado al menos a dos redes, generalmente LAN o WAN y el tráfico que recibe procedente de una red lo redirige hacia la(s) otra(s) red(es). En términos domésticos un router es el dispositivo que proporciona el proveedor de servicios de telefonía (o ISP) y que permite conectar nuestra LAN doméstica con la red del IS. El router comprueba las direcciones de destino de los paquetes de información y decide por qué ruta serán enviados, para determinar el mejor camino emplean cabeceras y tablas de comparación.

Suplantación de identidad: Es la actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude, acoso (cyberbulling). Un ejemplo es, en las redes sociales, crear un perfil de otra persona e interactuar con otros usuarios haciéndose pasar por ella

Troyano: Se trata de un tipo de malware o software malicioso que se caracteriza por carecer de capacidad de autoreplicación. Generalmente, este tipo de malware requiere del uso de la ingeniería social para su propagación. Una de las características de los troyanos es que al ejecutarse no se evidencian señales de un mal funcionamiento; sin embargo, mientras el usuario realiza tareas habituales en su ordenador, el programa puede abrir diversos canales de comunicación con un equipo malicioso remoto que permitirán al atacante controlar nuestro sistema de una forma absoluta.

GOBIERNO DE ESPAÑA
MINISTERIO DE DERECHOS SOCIALES Y AGENDA 2030
POR SOLIDARIDAD
OTROS FINES DE INTERÉS SOCIAL
Colectivos Acción Solidaria
ASOCIACIÓN La Columbeta