CIBERLAND

Fundación MAPFRE

POLICÍA NACIONAL

¿TÚ CONTROLAS?

DESCUBRE LO QUE ESCONDEN LAS REDES

Ciberland es una exposición itinerante de Fundación MAPFRE y Policía Nacional que nos ayuda a comprender cómo funcionan las tecnologías de la información y comunicación en las RRSS.

Para ello es importante estar concienciados y saber identificar y prevenir situaciones de peligro.

¿SABES CÓMO PROTEGERTE EN LOS JUEGOS *ONLINE*?

Los juegos irrumpieron con fuerza en el mundo digital y han transformado el ocio de muchas generaciones. Para evitar los riesgos de los juegos *online:*

- Evita dar datos personales y configura tus perfiles privados.
- Limita las horas de juego y haz descansos (si tienes hijos revisa a qué juegan los menores y cuánto tiempo)
- Ten especial cuidado con los sistemas de micropagos porque, aunque parezcan pequeñas cantidades de dinero, pueden terminar siendo un gran gasto a largo plazo. Existen dos tipos de juegos: los llamados *"Free to Play"* (F2P), que son inicialmente gratuitos, y los "juegos premium" que son aquellos que cuestan dinero. Tanto en los de acceso gratuito como en los de pago existen las siguientes mecánicas conocidas como:

PAY TO WIN (P2W), PAY TO FAST (P2F) O PAY TO PROGRESS (P2PRO):	**Te permiten una serie de beneficios y ventajas con respecto al resto de los jugadores, pero para conseguirlas tienes que realizar unos pagos.**
LOOT BOXES: (CAJAS DE BOTÍN)	**Son una especie de cajas sorpresa que contienen premios al azar que pueden conseguirse o bien jugando muchísimas horas o directamente comprándolas. Uno de los mayores problemas de estas cajas es que, al no saber qué se esconde detrás, puede tratarse de lo que no estás buscando, de manera que incita a seguir adquiriéndolas.**

- Desconfía de la gente que te regala cosas.

¿SABÍAS QUÉ?

Algunas señales que indican una posible adicción a los videojuegos son:

- Ansiedad constante por jugar en todo momento.
- Aislamiento, mentiras a familiares y amigos sobre el tiempo jugado y el dinero invertido.
- Depresión, agresividad y ansia o fobia ante la prohibición de jugar.
- Trastornos del sueño. El *Vamping* es el término que utilizado para definir el uso de la tecnología hasta altas horas de la madrugada reduciendo las horas de sueño.
- Cambio de hábitos en la comida y/o problemas posturales, dolores musculares y lesiones físicas especialmente en espalda y manos.

Si te sientes identificado, acude a un profesional.

El Pan European Game Information (PEGI) es el sistema de clasificación por edades europeo que informa sobre la edad recomendada de un videojuego en términos de protección de los menores, sin tener en cuenta el nivel de dificultad ni las habilidades necesarias para jugar. Establece 5 categorías de edad: PEGI 3, 7, 12, 16 y 18

¡VIVE, DUERME, PASA TIEMPO CON AMIGOS Y FAMILIA...
NO DEJES QUE EL JUEGO CONTROLE TU VIDA!

APUESTAS *ONLINE*

Desde la Fundación de Ayuda contra la Drogradicción (FAD) alertan que más de 500.000 menores apuestan cada año en España, tanto *online* como de manera presencial, una cifra que ha ido en aumento en los últimos años, a pesar de ser ilegal. Recuerda que tienes que ser mayor de edad para realizar apuestas *online*.

Apostar no es un juego, sus consecuencias pueden ser muy variadas: ansiedad, insomnio, mala alimentación, endeudamiento, hacer uso de las mentiras, empeoramiento de las relaciones familiares y sociales, hurtos en casa, problemas de rendimiento escolar o absentismo laboral, etc. Si cuando no apuestas te sientes nervioso, has empezado a mentir, a robar o a pedir dinero, solicita ayuda.

¿SABÍAS QUÉ?

LUDOPATÍA (conocido como *Gambling* en inglés) es el impulso incontrolable de jugar apostando dinero sin tener en cuenta las consecuencias negativas.

CHALLENGES/ RETOS VIRALES

Uno de cada 10 adolescentes españoles reconoce haber realizado retos virales peligrosos, según un estudio del grupo de investigación Ciberpsicología de la Universidad Internacional de La Rioja (UNIR). Entre los retos positivos existen otros muy peligrosos que pueden ocasionar serios daños a quien los realiza, llegando incluso a costarle la vida, a él o a otras personas.

No te pongas ni a ti, ni a otras personas en peligro por conseguir un "me gusta".

Utiliza el sentido común; aunque lo hagan "todos", tú no tienes por qué hacerlo.

Si tienes hijos, supervisa a quién siguen y ayúdales a desarrollar la su capacidad crítica.

Evita la difusión de los retos que sean nocivos o peligrosos.

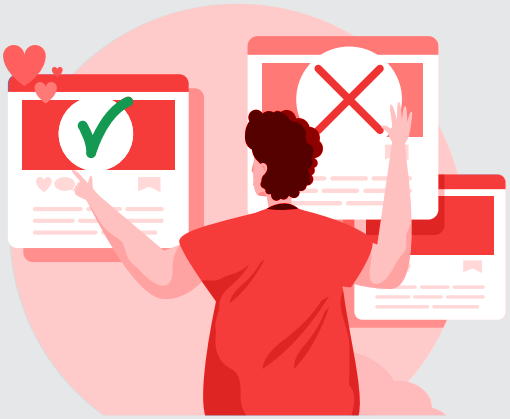
DESINFORMACIÓN. NO TE DEJES ENGAÑAR

Con Internet, las noticias falsas, también conocidas como *"Fake News"*, viven su momento más álgido, ya que pueden replicarse en segundos provocando un peligroso círculo de desinformación entre las personas que les dan credibilidad.

CÓMO DETECTAR NOTICIAS FALSAS

Mantén una actitud crítica cuando leas un titular, lee la noticia entera, y si no estás seguro de su veracidad, no la compartas.

- **Lee más allá del título y desconfía de los titulares sensacionalistas.**
- **Fíjate en la fuente de la noticia y en la procedencia del portal.**
- **Examina siempre la URL y presta atención al formato.**
- **Fíjate en la fecha de la noticia y consulta si otras fuentes fiables hablan de ella**



CONTENIDO INAPROPIADO

El contenido inapropiado es todo aquel material que percibido por un menor de edad puede causarle un perjuicio psíquico o físico.

Existen comunidades *online* que son grupos que comparten intereses comunes en Internet.
Muchas comunidades tienen buenas intenciones, como por ejemplo compartir aficiones de ocio, intereses culturales o educativos, conocimientos, etc.
Pero muchas otras comunidades tratan temas inapropiados o peligrosos.
Por ejemplo: comunidades que promueven el extremismo, el odio o la violencia. Comunidades «*hate-speech*» que promueven el odio racial, la xenofobia, el antisemitismo y la homofobia.

¿SABÍAS QUÉ?

En Internet hay contenidos nocivos e ilícitos y acceder a estos últimos es delito.

Contenidos ilícitos:
Son aquellos que no están permitidos legalmente.

Pornografía infantil
Difamación en Internet
Apología del terrorismo, racismo y xenofobia
Incitación a la Bulimia y/o anorexia

Contenidos nocivos:
Son legales pero pueden ser muy dañinos para el desarrollo personal y/o social.

Pornografía entre adultos
Violencia
Retos virales
Publicidad engañosa

RECUERDA: La Ley Orgánica de Protección de Datos establece multas económicas por manejar información/imágenes de otras personas sin su autorización.

RIESGOS DERIVADOS DEL USO DE LAS TIC

GROOMING

Cuando un adulto se gana la confianza de un menor a través del engaño, con el propósito de obtener de él un beneficio de naturaleza sexual. El adulto se suele hacer pasar por un menor, para generar un vínculo de confianza que pasa por diferentes fases. Unos de los medios favoritos para cometer grooming son los videojuegos. A través de los chats, los adultos *groomers* interaccionan con los menores con el propósito de alcanzar su objetivo.

SEXTING

Conducta de riesgo consistente en el envío de imágenes (fotografías y/o vídeos) de contenido sexual o erótico, creadas por el propio remitente de forma voluntaria, usando las tecnologías de la información y comunicación.
Sin embargo, la difusión, revelación o cesión de este tipo de contenidos, sin consentimiento, vulneraría los derechos de imagen y derecho a la intimidad de esa persona pudiendo convertir esta conducta en un delito del Código Penal.

- No te hagas ni envíes fotos comprometidas, pueden hacer una captura, manipularlas y distribuirlas por la Red. Si eres menor y alguien te pide que le envíes este tipo de contenido no lo hagas y avisa a tus padres.
- Nunca accedas a un chantaje.
- Denuncia cualquier situación de acoso.
- Cuando recibas imágenes comprometidas de otros, bórralas y no las reenvies. Si en las imágenes sexuales aparecen menores, eso es pornografía infantil y es un delito recogido en el Código Penal.

SEXTORSIÓN

Es el chantaje promovido por el envío de fotos o vídeos comprometidas de carácter sexual realizados en el Sexting.

CIBERACOSO ESCOLAR

Conducta delictiva en la que un menor humilla, amenaza, coacciona, insulta, aísla o chantajea a otro menor de forma intencionada y repetida en el tiempo a través de las TIC. El anonimato ni te exime de ese comportamiento que está penado por la ley, ni evita que seas descubierto, pues es muy sencillo detectar quién hay detrás de esos actos.

DENUNCIA

- Si eres víctima, habla con un adulto de confianza (padres, tutores, profesores, policía ...) y guarda las pruebas que tengas.
- Si eres testigo, no te calles, avisa a un adulto de confianza. No participes bajo ningún concepto en la agresión, te convertirías en cómplice.

CIBERCONTROL EN UNA RELACIÓN

En una relación de pareja también existe un tipo de acoso que se produce en redes sociales o a través de mensajería instantánea y que es considerada violencia digital.

- Protege tu intimidad y privacidad.
- No toleres ningún tipo de amenaza, chantaje o cualquier otro tipo de violencia
- No dejes que controlen tu ubicación, mensajes o actividad en redes sociales.

HAPPY SLAPPING

Grabación de una agresión física, verbal o sexual y su difusión *online*.

VIOLENCIA DIGITAL

Se presenta por una persona o grupo de personas hacia otra u otros, en el que se ejerce violencia a través de insultos, acoso, control, ataques, chantaje. En el caso de violencia de un hombre a una mujer estando o habiendo estado en una relación de afectividad se denomina "violencia digital de género" o si es dentro de la pareja (incluye mismo género), "violencia digital en pareja".

REDES SOCIALES

Las redes sociales son plataformas digitales que conectan entre sí a personas con intereses, actividades o relaciones en común.

Todos los datos e información que se publican en las redes sociales acaban construyendo tu identidad y tu reputación digital.

No facilites información personal y configura el perfil privado en las redes sociales.

Cuida tus publicaciones en la Red y decide con sentido común a quién agregamos como seguidor o amigo.

Antes de abrirte una red social nueva, lee las condiciones de uso y averigua cómo y para qué se utiliza.

Crea contraseñas fuertes y seguras.

¡Desconfía! Evita participar en sorteos o encuestas por RRSS que soliciten datos personales. Pueden ser falsos.

APRENDE A PROTEGERTE

¿CÓMO PUEDO PROTEGER MI PRIVACIDAD?

Configuración
Configura desde tu dispositivo los accesos de las apps, permisos, desbloqueos...

Contraseña
Crea contraseñas seguras, robustas y secretas, usando mayúsculas, minúsculas, números y símbolos. Cámbialas cada cierto tiempo.

Huella dactilar
Usa tu huella dactilar, es única e inmutable y aumenta la seguridad en tus aplicaciones y cuentas.

Descarga de Apps
Hazlo siempre en sitios oficiales y revisa los permisos que solicitan y valora si tienen sentido o no. Desconfía de versiones gratuitas. Mantén las actualizaciones al día.

Cámara frontal y *webcam*
Existe un virus que activa la *webcam* sin que la persona se dé cuenta. Utilízala únicamente con personas que conozcas personalmente y mantenla tapada cuando no se esté utilizando.

Antivirus
Todo dispositivo que tenga conexión a Internet (móvil, ordenador, tableta...) puede sufrir ataques de virus. Instala un software antivirus de calidad.

Geolocalización
Muchos sitios web y aplicaciones recopilan información de sus usuarios, entre ellos su ubicación - desactiva el GPS.

Menores en las TIC
Los navegadores Chrome o Firefox incluyen «*Safe Search*» en sus opciones de configuración para filtrar contenido explícito (imágenes, vídeos o sitios web). También existen aplicaciones de control parental que evitan que los menores tengan acceso a contenido no deseado y que evitan compras de productos *online* sin autorización.

¿QUÉ HAY QUE MIRAR ANTES DE BAJARTE UNA APP O JUGAR A UN JUEGO *ONLINE*?

- **Lee las condiciones de uso** de las diferentes aplicaciones o juegos que descargas.
- **Razona sobre la información que compartes** con los demás y la que das cuando te la piden. Evita dar datos personales a alguien desconocido.
- **Crea contraseñas seguras con más de 8 caracteres** con letras, mayúsculas, minúsculas, números y símbolos.
- **Usa diferentes contraseñas para cada perfil y cámbialas cada cierto tiempo.** Usa trucos para poder gestionar esas contraseñas, como reglas mnemotécnicas.
- **Denuncia por medio de sitios web o servidores cuando te percates de posibles estafas.** En el caso de que el problema persista o seas víctima de un delito, acude a las Fuerzas y Cuerpos de Seguridad para denunciar los hechos, guardando siempre toda la información que tengas (capturas de pantalla, correos, mensajes, números de teléfono, perfiles...)

CONSEJOS PARA DETECTAR POSIBLES ESTAFAS

Desconfía de los mensajes y de las llamadas de remitentes desconocidos.

Si te ofrecen premios, desconfía.

No pinches en enlaces ni descargues archivos adjuntos de correos, páginas o en mensajes que sean desconocidos o resulten sospechosos.

Evita guardar claves o información bancaria sin cifrar en tu teléfono.

Recuerda que el banco nunca te pedirá por sms o llamada que le facilites tus claves de acceso al completo ni tampoco los datos de tu tarjeta.

Evita facilitar información a personas desconocidas, especialmente cuando se trata de datos personales o bancarios.

Bloquea los mensajes de texto que consideres spam.

Verifica el remitente si tienes dudas del mensaje, busca en internet o escribe a tu contacto por otro canal.

Personaliza las opciones de seguridad, con contraseñas seguras y sistemas de doble verificación.

Presta especial atención a la ortografía y al lenguaje usado en los correos electrónicos que recibas.

FORMAS MÁS HABITUALES DE INTENTO DE ESTAFA

PISHING

Es una técnica que consiste en el envío de un correo electrónico, por parte de un ciberdelincuente, simulando ser una entidad legítima (tu banco, una institución pública...) para conseguir información personal del usuario y hacer un uso fraudulento de ella. (Robo de identidad, robo de cuenta, cargos económicos, etc.)

VISHING

Se trata de una llamada de teléfono, donde el supuesto operador, que se identifica como un trabajador de un banco, identidad pública etc., nos solicita datos personales o incluso acceso remoto a alguno de nuestros dispositivos para robarnos los datos, para conseguir información personal del usuario y hacer un uso fraudulento de ella.

SMISHING

Es una técnica que consiste en el uso de servicios de mensajería instantánea simulando ser una entidad legítima (red social, banco, institución pública, etc.) para conseguir información personal del usuario y robar tu identidad, hacerte un cargo económico, etc.

ESTAFAS CON PAGO INSTANTÁNEO

Las **aplicaciones de pago instantáneo** se encuentran entre las más utilizadas por la gente. A través de plataformas de envío de dinero instantáneo hay que ser muy cauteloso y se debe siempre comprobar que se recibe una notificación de "ingreso" y no una "solicitud de envío" de dinero. Las estafas más comunes a través de este tipo de aplicaciones de pago instantáneo son las siguientes:

Compras de segunda mano: esta es una estafa bastante habitual. El estafador se hace pasar por un comprador interesado en algún producto de segunda mano que tengamos en venta, en páginas conocidas dedicadas a este tipo de productos. El estafador dirá que nos va a hacer el pago instantáneo por aplicación, solicitándonos el número de teléfono para ello. Sin embargo, en vez de enviarnos el pago, lo que nos enviará será una solicitud de envío de dinero. El mensaje específica que es una solicitud de dinero, pero si por las prisas o desconocimiento de cómo funcionan estas aplicaciones, pulsamos en aceptar, estaremos enviando nosotros el dinero al estafador.

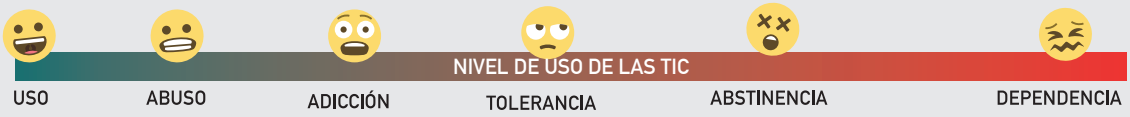
Pedir pagos por adelantado: otro de los casos es el fraude del falso vendedor. Aquí el estafador se hace pasar por un vendedor y ofrece artículos en páginas de venta en Internet por precios bastante atractivos e inferiores a lo normal. Una vez captado el interés de un comprador potencial, el estafador le pide que le adelante una parte del importe o el precio completo del producto para proceder a enviarlo. Sin embargo, una vez hecho el pago, la víctima no recibirá nunca el producto. Los estafadores que emplean este método se aprovechan de que no se puede anular un pago por este tipo de aplicaciones (a diferencia de una transferencia bancaria normal), ya que el envío de dinero es instantáneo e irrevocable.

Supuestos abonos de la Seguridad Social: se trata de un falso abono de la Seguridad Social por alguna prestación o por ERTE. En este caso, el estafador envía un SMS a la víctima potencial o recurre a una llamada telefónica *(vishing)* en la que se hace pasar por la Seguridad Social y comunica a la víctima que le van a hacer un abono de una prestación pendiente. Dicho abono lo harán por la aplicación, por lo que solicitan el número de teléfono y, como en el caso del falso comprador, lo que envían es una solicitud de envío de dinero. A veces, en el mensaje aparece el nombre «TGSS» para tratar de darle veracidad.

El aviso de pago por error a través de aplicaciones de mensajería instantánea: otras de las estafas que se han empezado a ver con aplicaciones de pago es la del aviso de pago por error a través de aplicaciones de mensajería instantánea. Aquí, el estafador le envía un mensaje por la aplicación de mensajería a la víctima, en el que se le comunica que por error le ha enviado un pago por aplicación de pago instantánteo de X cantidad de euros (lo más habitual son 50 €); aparentemente, quien envía el mensaje es alguien de la lista de contactos de la víctima, pero en realidad es un ciberdelincuente, que pide a la víctima que le devuelva ese dinero. Si picamos, porque no nos paramos a comprobar que el supuesto ingreso es real, perderemos esos 50 euros.

CONSECUENCIAS FÍSICAS Y PSICOLÓGICAS DEL USO DE LAS TIC

Hay que tener claro que las TIC son una herramienta o una alternativa de ocio, pero no sustituyen las posibilidades que ofrece la vida "real". Hay que valorar la vida ***offline***: hacer deporte, quedar con amigos, familiares, disfrutar de la vida fuera de Internet… Hay miles de experiencias que solo pueden vivirse en el mundo "real".



MIEDOS Y FOBIAS

NOMOFOBIA

Miedo irracional, intranquilidad, ansiedad y gran malestar que siente una persona por no disponer del teléfono móvil y la incapacidad de apagar el móvil incluso en lugares donde su uso está prohibido.

FOMO

Temor a quedar desconectado, perdiendo mensajes o *whatsapps*, o el contacto con las redes sociales.

CRACKBERRY

(adicción a las notificaciones)

Imposible continuar cualquier tarea si salta un aviso, apareciendo la necesidad imperiosa de ver su contenido, o la necesidad de revisar continuamente la cuenta de correo electrónico, entre otras aplicaciones.

PHUBBING

En una reunión social, ignorar a alguien al estar prestando atención al teléfono móvil en lugar de hablar con esa persona cara a cara.

- PROBLEMAS EN LOS LIGAMENTOS
- PROBLEMAS NERVIOSOS
- PROBLEMAS VISUALES
- PROBLEMAS AUDITIVOS
- PROBLEMAS OSTEOMUSCULARES
- PROBLEMAS VASCULARES
- PROBLEMAS METABÓLICOS Y CARDIACOS
- TRASTORNOS DEL SUEÑO

CIBER LAND

Fundación MAPFRE

POLICÍA NACIONAL