Taller de Huellas en la Red

“Ciberespacio Seguro : Educar para proteger”

Grooming , Ciberbullying ,Sexting , Sharenting y Ludopatía

Marco teórico

Grooming:

El grooming es el acoso sexual virtual dirigido hacia los niños, niñas y adolescentes a traves del uso de internet. Consiste en una serie de conductas preparatorias ejecutadas de manera virtual por un acosador, conocido como groomer, con el objetivo de alcanzar su propia satisfacción sexual. Para ello , a menudo utiliza una identidad virtual falsa para ganarse la confianza de la víctima, aprovechándose del anonimato que ofrecen las plataformas digitales. Estos agresores buscan intercambiar material de contenido sexual (imágenes, videos, mensajes, entre otros) para luego utilizarlo con fines de extorsión, y en algunos casos, pueden llegar a concretar un encuentro real que termine en abuso sexual.

El acoso en línea es más rápido y anónimo; en muchos casos, los niños y adolescentes confían más rápidamente en “sus amigos” en línea que personas que conocen cara a cara. La interacción a través de una pantalla puede disminuir las inhibiciones, colocándolos en una situación de mayor vulnerabilidad.

Hoy en día; las redes sociales como Instagram, Snapchat y TikTok son los medios más comunes que los groomers utilizan para llevar a cabo estas prácticas. Si bien el acoso y el abuso sobre niños y adolescentes han existido históricamente, la particularidad del grooming radica en el uso de dispositivos electrónicos, lo cual se adapta a las circunstancias sociales actuales, caracterizadas por una alta presencia de espacios virtuales en la vida cotidiana. El grooming, por tanto, es una nueva forma de ejecutar un antiguo delito que vulnera la integridad y los derechos de los menores.

Generalmente, el grooming se desarrolla en una serie de fases, aunque estas no

siempre se presentan de manera secuencial o exacta. Las fases suelen ser: acercamiento, establecimiento del vínculo de confianza, acoso, extorsión, y finalmente, ataque sexual.

Fase de acercamiento: El groomer busca generar un lazo de amistad con el niño, niña o adolescente, frecuentemente fingiendo ser alguien de la misma edad y mostrando intereses comunes. Para esto, investiga los gustos e intereses de la víctima para crear un perfil con el cual pueda empatizar.

Fase de establecimiento del vínculo de confianza: El groomer intenta fortalecer el lazo de confianza, posicionándose como un confidente y apoyo, con el objetivo de persuadir a la víctima a intercambiar material de connotación sexual. La confianza generada se utiliza para explotar la intimidad de la víctima.

Fase de acoso y extorsión: El groomer busca mantener el intercambio de material o incluso concretar un encuentro offline, utilizando la extorsión como herramienta, amenazando con hacer público el material ya enviado o con informar a los adultos responsables sobre las acciones de la víctima. Esto genera un estado de culpa y pudor en la víctima, atrapándola en una espiral de silencio y sometimiento creciente.

El grooming puede derivar en otros graves delitos como:

- Pornografia infantil
- Trata de personas
- Abuso sexual
- Homicidio

Prevención y detección del grooming: Es crucial entender que el mundo digital forma parte integral de la vida de los jóvenes y que, aunque existen riesgos asociados a su uso, prohibirlo no es la solución. Para hablar de prevención, es primordial construir un diálogo sobre estos temas. Los adultos deben comprender la cultura digital para acompañar a los jóvenes en su crecimiento. Es importante que las familias y referentes de adultos tengan herramientas para intervenir y apoyar en la vida digital de los jóvenes.

Para prevenir el grooming, no se trata de prohibir que los chicos hablen con desconocidos en las redes sociales, sino brindarles herramientas para que comprendan los riesgos de compartir información personal en espacios públicos como las redes sociales o internet y conozcan las formas de prevenirlo.

En Misiones, existe una ley de prevención de acoso escolar, grooming y bullying, que incluye la creación del Plan integral para el Abordaje, Prevención y Erradicación del acoso contra niñas, niños y adolescentes, el Programa Educativo para el uso consciente y responsable de las redes sociales e Internet, y la adhesión a la Ley Nacional N° 27.458 que declara el 13 de noviembre como el Dia de la lucha contra el grooming.

Para la prevención y el uso consciente de internet, es importante:

- No promocionar ni hacer accesible a extraños imágenes o información personal.
- Preservar la seguridad y confidencialidad de cuentas de usuario y contraseñas.
- No ceder ante el chantaje.
- Promover el pedido de ayuda en situaciones de estrés emocional.
- Recopilar pruebas de la actividad delictiva.
- Formular una denuncia con un adecuado análisis de la situación.

Además, los adultos deben:

- Controlar y supervisar el acceso de los menores a internet.
- Concientizar a los jóvenes sobre los peligros de la red.
- Mantener un diálogo abierto y crear un ambiente de confianza.
- Instalar antivirus o software de control parental en los dispositivos utilizados por los menores para protegerlos ante situaciones no previstas.

Sexting:

El término "sexting" proviene de la combinación en inglés de las palabras "sex"

(sexo) y "texting" (envío de mensajes de texto). Esta práctica ha surgido con el auge de las tecnologías digitales y consiste en el intercambio de contenido sexual a través de dispositivos móviles, como teléfonos celulares y tabletas. A menudo, se realiza mediante diversas aplicaciones populares como WhatsApp, Facebook, Instagram y Snapchat. Una vez que se envía una imagen o un video a uno o varios contactos, estos pueden reenviarlos , lo que puede llevar a la viralización del contenido. Este tipo de información está intrínsecamente ligado a la identidad digital de la persona que aparece en ella, lo que hace aún más crucial que se comprendan y utilicen adecuadamente las herramientas digitales para manejar este tipo de situaciones de manera responsable.

Las consecuencias del sexting son variadas y pueden ser devastadoras. Aunque las imágenes enviadas en el contexto del sexting suelen ser tomadas de manera consensuada y en un ambiente privado, su divulgación en internet puede generar resultados inesperados y perjudiciales para las personas involucradas. Algunas de las principales consecuencias incluyen:

- Descontextualización de la situación: Las imágenes o videos tienen un sentido específico en el contexto en el que fueron creados. Sin embargo, al ser compartidos públicamente, pueden ser malinterpretados o utilizados de manera inapropiada, lo que lleva a que los protagonistas se sientan incómodos e invadidos por la exposición.

- Exposición: Cuando una imagen se vuelve viral, puede ser vista por personas que no son los destinatarios originales. Cuantos más contactos visualicen el contenido, mayor será la exposición de la persona involucrada, lo que puede llevar a situaciones de acoso o bullying.

- Daño a la identidad o huella digital: Un video o una foto privada que se expone públicamente puede causar un daño significativo a la reputación en línea de la persona afectada. En internet, es muy difícil eliminar la información una vez que se ha compartido, lo que significa que el material puede persistir indefinidamente. Esto puede resultar en consecuencias negativas a largo plazo, ya que el

contenido relacionado con el sexting puede aparecer en búsquedas futuras y estar asociado de manera permanente con la identidad de la persona.

En caso de enfrentarse a una situación de sexting, es fundamental tomar acciones adecuadas:

-Reportar las imágenes: Siempre se debe denunciar las imágenes sexuales de niños, niñas y adolescentes en la web. Esto es crucial para detener su circulación. Las redes sociales y los sitios web ofrecen opciones para denunciar y bloquear contenido inapropiado, y es importante que tanto adultos como jóvenes conozcan y utilicen estas herramientas como parte de su responsabilidad digital.

-Denunciar ante las autoridades: En situaciones donde se involucra a menores, es vital realizar una denuncia en comisarías o fiscalías cercanas. También, es recomendable buscar asesoría legal para manejar la publicación del material de manera adecuada.

En suma, el sexting es una práctica que puede tener consecuencias graves si no se maneja con la debida responsabilidad y precaución. Educar a los jóvenes sobre los riesgos asociados y promover un uso consciente de las tecnologías digitales es esencial para prevenir situaciones perjudiciales.

Ciberbullying:

El ciberbullying se define como la intimidación psicológica o el hostigamiento que ocurre entre pares, tanto en el ámbito escolar como fuera de él. Una de sus principales características, que lo distingue de otros tipos de maltrato, es que se manifiesta de manera sostenida en el tiempo y con cierta regularidad, utilizando las nuevas tecnologías de la información y la comunicación como medio para perpetrar estos actos. Este fenómeno de ciberacoso presenta características particulares, como la viralidad de los contenidos y el sentimiento de anonimato que experimentan los agresores, lo que puede incrementar su comportamiento hostil.

Entre los principales motivos de discriminación, en línea, se encuentran las creencias religiosas, el racismo y el aspecto físico. Los tipos de ciberbullying pueden incluir diversas formas de hostigamiento, como la persecución en redes sociales, que abarca amenazas, insultos, grabaciones realizadas con dispositivos móviles, publicación de datos personales, así como el uso de software espía y virus. Además, se presenta la exclusión social mediante mensajes denigrantes que humillan y menosprecian a la víctima. La manipulación también es una táctica común, que implica la modificación y difusión de contenido en línea, incluyendo material alterado, conversaciones manipuladas y comunicaciones distorsionadas.

Es fundamental que tanto víctimas como espectadores sepan cómo actuar ante situaciones de ciberbullying. Si soy víctima, por un lado, puedo tomar las siguientes medidas: no responder a los agresores, bloquear a la persona que me hostiga y denunciar al acosador. Es importante comunicar la situación a una persona de confianza y utilizar las herramientas que ofrecen las plataformas o aplicaciones para denunciar publicaciones, comentarios o imágenes agresivas. Por otro lado, si me encuentro en el rol de espectador, tengo el poder de intervenir y denunciar el comportamiento cruel.

Los espectadores que intentan frenar el hostigamiento o ayudar a la víctima se convierten en defensores. Elegir ser un defensor implica rechazar comportamientos agresivos y fomentar actitudes amables y positivas, ya que una actitud constructiva puede tener un gran impacto y ayudar a evitar que la negatividad se convierta en crueldad y hostilidad.

Como espectador, puedo asumir un papel activo de defensa de la siguiente manera : encontrar formas de demostrar amabilidad y ofrecer apoyo a la víctima ; señalar el comportamiento agresivo en un comentario o respuesta recordando que debe señalarse el comportamiento y no a la persona; y evitar adoptar actitudes que agraven la situación o incentiven al agresor, como unirse al hostigamiento o compartir publicaciones o comentarios agresivos en línea. La clave está en promover un entorno digital más seguro y solidario para todos.

¿Quiénes participan del ciberbullying?

En el ciberbullying participan :

- La persona acosadora menor de edad, que ejerce su poder para humillar a otra persona menor de edad;
- La víctima , que es la persona menor de edad que sufre el maltrato ;
- Los espectadores que son quienes ven la agresión desde afuera, por lo general ,no se animan a denunciar y, a veces se suman a la agresión produciendo un efecto contagio.

¿Por qué medios se realiza el ciberbullying?

El ciberbullying puede realizarse a través de distintos medios electrónicos, como telefonía móvil , correo electrónico, mensajería instantánea, redes sociales o juegos online.

¿Cuándo un chico es víctima de ciberbullying?

Es víctima de ciberbullying cuando por ejemplo :

- Se lo denigra mediante las redes sociales a través de textos, videos o fotos
- Se le niega la entrada a foros , chats o plataformas sociales
- Se modifica y difunde información en las redes sociales que lo perjudican

Sharenting:

La terminología “sharenting” proviene del inglés de la unión de dos vocablos “share” y “parenting” los que se traducen como compartir y parentalidad. Se refiere a la práctica de compartir fotos de niños en Internet y las redes sociales en situaciones cotidianas (momentos de baños de bebes, juegos en la piscina, etc.) lo que puede ser tomado de manera morbosa por adultos con parafilia de fantasías de actividad sexual con niños. También estas imágenes pueden ser utilizadas con el fines de grooming, ciberbullying, robo de identidad y/o robo de datos personales.

En castellano hablamos de “sobreexposición” de los niños en las redes sociales donde muchos progenitores y tutores comparten fotos de sus niños, niñas y adolescentes porque quieren que sus familiares y amigos sean partícipes de la cotidianeidad de sus vidas. Sin embargo, existe el peligro de que estas fotos se reutilicen de una forma ilícita o malintencionada que pueda perjudicarles en un futuro.

Como fue mencionado anteriormente, cuando una imagen se sube a la red puede ser vista por personas que no son los destinatarios originales. Muchas veces los padres o adultos responsables pueden subir una foto a las redes sociales, publicar una imagen sobre el niño o la niña, o enviar un video con la intención de compartir momentos diarios de crecimiento, pero debemos tener en cuenta que esto puede conllevar a que personajes malintencionados utilicen estas imágenes con otra finalidad.

Stacey Steinberg se refiere a dos puntos a tener en cuenta antes de compartir imágenes de niños en internet. Por un lado, la experta se refiere a los daños materiales reales que los niños y niñas podrían sufrir debido a la información compartida en línea, lo que deja indefectiblemente una huella digital, lo que implica un rastro de información que dejamos cada vez que navegamos en línea. Por otro lado, la autora del libro sobre crianza “Growing up shared”, se refiere a que cuando compartimos información sobre los niños en internet sin consultarlos, desaprovechamos la oportunidad de enseñarles con el ejemplo sobre la noción de consentimiento, además de poder mostrarles que la privacidad es un aspecto importante en la vida.

El sharenting ha suscitado un debate entre padres, expertos en privacidad y defensores de los derechos infantiles. Se discuten cuestiones relacionadas con la falta de voz de los niños en las decisiones sobre lo que se comparte, así como la responsabilidad de los padres de proteger la privacidad de sus hijos. También , se considera si deberían establecer regulaciones sobre esta práctica.

Para manejar la sobreexposición de manera responsable, se recomienda que los padres piensen cuidadosamente antes de compartir contenido, configuren

adecuadamente la privacidad en sus redes sociales, eviten publicar información identificable y conversen con sus hijos sobre lo que se comparte acerca de ellos a medida que crecen.

GAMING

Estilos de ocio

El ocio es una parte muy importante de nuestras vidas. El tipo de ocio que realizamos durante nuestra juventud influye directamente en la adquisición y fortalecimiento de hábitos de vida saludable. Es interesante conocer el tipo de ocio que actualmente disfrutan las personas jóvenes y analizar el impacto que esto provoca en sus vidas. Asimismo, es importante dar a conocer las alternativas de ocio existentes, que no incluyan o fomenten las adicciones. El ocio, en sí mismo, es un espacio educativo fundamental para el desarrollo integral de la juventud. Por ello, debemos fomentar y promover un ocio saludable accesible.

Habilidades sociales:

Desarrollar unas correctas habilidades sociales en los y las jóvenes no sólo les ayudará a construir relaciones más positivas o a interaccionar mucho mejor con los demás, sino que pone a su alcance el núcleo del aprendizaje social y emocional. Sin duda, el autoconocimiento y la empatía tienen un papel protagonista en nuestras actividades porque consideramos que el hecho de manejarlas empodera a los jóvenes y les hace capaces de tomar decisiones responsables.

Si bien la Ludopatía ha sido siempre un problema socialmente histórico, en la actualidad se ha visto un incremento en el consumo compulsivo de juegos de azar en personas jóvenes. En la actualidad cada vez más jóvenes y adolescentes se ven involucrados en apuestas y juegos de azar a través de sus dispositivos digitales, pero jugar y apostar son cosas diferentes.

Aquí surge el interrogante: ¿Qué es la ludopatía? La ludopatía es definida como la adicción a los juegos de azar. La Organización Mundial de la Salud (OMS) define a

la ludopatía como un trastorno caracterizado por la presencia de frecuentes y reiterados episodios de participación en juegos de apuestas, los cuales dominan la vida del enfermo en perjuicio de sus valores y obligaciones sociales, laborales, materiales y familiares.

Pereyra (2009) define el juego compulsivo como: una enfermedad que se caracteriza por el impulso incontrolable por jugar. Se puede decir que alguien es un jugador compulsivo cuando éste juega, no sólo ya por el hecho de ganar, sino por el mismo placer de jugar y no es capaz de parar, ocasionando así problemas tanto emocionales, como familiares, legales, financieros, etc.; esta adicción suele estar acompañada de otras como el alcohol y las drogas... Es una enfermedad que, en resumidas cuentas, destruye tanto al jugador como a las personas que lo rodean. Además, el jugador patológico disminuye sus interacciones sociales con personas no relacionadas con el juego; es decir, sólo socializa con amigos en bares, casinos, etc.

Información sobre la ludopatía:

Se considera imprescindible proporcionar, tanto a jóvenes como a mediadores, información actualizada y veraz para, de este modo, poder desmitificar ideas erróneas sobre la ludopatía. Estas ideas están muy extendidas en nuestra sociedad y pueden llegar a crear mucha confusión. Por tanto, es necesario resolver dudas e inquietudes de los destinatarios fomentando un clima de confianza.

En los últimos años, y mayormente desde la pandemia, se ha visto un crecimiento desproporcionado en el consumo de juegos de azar en línea, lo que ha sido alimentado globalmente por el fácil acceso a internet. Si bien hoy en día están muy extendidas, algunas sociedades anteriormente tenían una experiencia limitada de juegos de azar y aún hoy siguen estando legalmente prohibidos en muchas partes del mundo. Aunque, otras sociedades han pasado por ciclos de liberalización y restricción que se remontan a cientos de años. En diferentes contextos se ha encontrado que la mayor vulnerabilidad, las desventajas económicas y sociales y la alta exposición al juego juegan un papel importante en

el desarrollo de problemas de ludopatía. Aún así, Domínguez (2009) señala que la ludopatía ha venido aumentado y afectando de forma importante a la población en general, sin importar si quiera la cultura, el sexo, la raza o nivel socioeconómico.

Adolescencia y Ludopatía:

Hoy en día es muy fácil acceder a una gran variedad de juegos. Existen de todo tipo: juegos de aventura, arcade, de deportes, puzzles, etc, los que son pensados para entretener tanto a grandes como jóvenes y niños.

Además, estos pueden accederse desde muchas plataformas diferentes. Hay una variedad de dispositivos tecnológicos desde los que se puede jugar. Cada vez es más común acceder desde una tablet o desde el móvil a miles de juegos online y todo gracias a Internet y a la gran cantidad de posibilidades que nos ofrecen las nuevas tecnologías.

En el caso de los niños y adolescentes, el uso desmedido y sin supervisión de los juegos en línea puede generar una dependencia y/o adicción tan extremas hasta hacerlos víctimas de ludopatía. Este trastorno se ha vuelto una problemática preocupante en nuestros tiempos ya que cada vez más niños/adolescentes, de diversas condiciones sociales, se ven inmersos en el juego con el fin de llenar vacíos emocionales, lo que puede verse agravado sin la adecuada dedicación y/o presencia de sus familias.

Si bien los juegos en línea son creados con el fin de entretener, muchas veces el juego se transforma en una necesidad de escapar del aburrimiento, de los miedos, o la necesidad de afecto, lo que indefectiblemente lleva a los jóvenes a generar adicción al juego.

Como menciona Tomás Calamardo, la ludopatía en los jóvenes es una problemática emergente cuyo primer síntoma es el absentismo escolar. El tallerista también menciona que “lo peor que le puede pasar cuando juega o apuesta por primera vez es que gane”. De aquí podemos concluir que los juegos generan una dependencia que se incrementa y se perpetúa, constituyendo los

denominados círculos viciosos de la dependencia, tanto psicológica como socialmente, transformándose en un trastorno que consume cada vez más de su tiempo, energía y recursos emocionales y materiales.

Pautas que podrían indicar que un adolescente abusa de los juegos de azar *online*

- Cambios significativos en el comportamiento o estado de ánimo como ansiedad, irritabilidad, cambios de humor repentinos, aislamiento social.
- Pérdida de interés repentina en otras actividades que antes disfrutaba como deportes, estudios o relaciones sociales y que ahora reemplazar por el juego *online*.
- Preocupación constante por el juego como hablar constantemente sobre apuestas, consultar resultados de manera compulsiva o buscar en forma reiterada oportunidades para jugar.
- Problemas financieros como dificultades para pagar deudas o rápido agotamiento de sus recursos económicos sin una explicación clara.
- Aumento del tiempo que dedica al juego.
- Negación o minimización del problema como justificar su comportamiento o mentir sobre la cantidad de tiempo o dinero que dedica al juego.

Phishing:

La palabra phishing quiere decir suplantación de identidad. Es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta. Lo que se extrae puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria.

El estafador, conocido como phisher, 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 o incluso utilizando

también llamadas telefónicas.

Al recibir un email o un mensaje a través de un chat en el cual se nos solicite información personal financiera o de cualquier índole, es importante que jamás respondamos, pero además tampoco debemos clickear en los enlaces que puedan aparecer en el mensaje.

¿Qué son los correos electrónicos falsos?

Son correos electrónicos que contienen información falsa y enlaces que redirigen tus respuestas hacia páginas de internet falsas con formularios y preguntas para obtener tus datos personales.

Estos correos electrónicos pueden aparecer como comunicaciones de bancos, servicios de pago, mercados de compra en línea o proveedores de servicios públicos. En general estos correos solicitan:

- Rellenar formularios o hacer clic en un enlace para obtener alguna información o archivo clave;
- Hacer clic en un enlace que redirige a una página de registro falsa;
- Descargar un archivo adjunto importante.

¿Cómo puedo saber si los mensajes o correos son un intento de *phishing*?

Es necesario prestar atención a los detalles como, por ejemplo:

- Correos o mensajes de WhatsApp enviados por remitentes desconocidos;
- El uso de remitentes parecidos a los de las páginas oficiales y legales;
- Faltas de ortografía: errores gramaticales y ortográficos, la falta de acentos o diéresis o la presencia de caracteres en otros idiomas;
- La presencia de enlaces y links dudosos;
- El tono del correo electrónico: las empresas se dirigen a sus clientes en tono cálido y personal, en general te llaman por tu nombre porque tus datos ya figuran en sus bases de datos;
- El objetivo del correo: ningún proveedor de servicios en línea le pide a sus

clientes la introducción de datos por medio del correo electrónico;
- Faltan o sobran letras en las direcciones URL: no es lo mismo “argentina.gob.ar” que “argentina.io”, esta última dirección URL es falsa;
- La página no tiene el candadito verde o gris con su certificado de seguridad.

¿Cómo puedo prevenir el *phishing*?

- Chequea el remitente: antes de abrir cualquier correo electrónico es importante chequear que no sea falso. Observa cuál es la dirección completa del remitente.
- Compara el remitente con los mensajes anteriores de tu banco o servicio.
- Comprobá si la dirección de internet (URL) que se muestra en la parte inferior izquierda en la ventana del navegador es igual a la de la empresa que te escribe. Podes hacer una búsqueda en internet de la empresa y comparar las URLs.
- Verifica el certificado de seguridad de la página de internet: es importante verificar que tenga el candado gris o verde y que sea una dirección HTTPS.
- Si tenés dudas comunícate con los servicios de atención al cliente antes de contestar cualquier comunicación por correo electrónico.
- No contestes formularios en línea enviados por destinatarios desconocidos.
- No respondas a ningún correo electrónico, mensaje o llamado telefónico que te solicite divulgar información personal.
- No envíes ni compartas ningún código de seguridad como el código PIN por teléfono o por correo electrónico.
- Desconfía de los archivos adjuntos: pueden causar la descarga de la clave de registro o software *"spyware"* en tu computadora.
- Utiliza un antivirus actualizado.

¿Qué es el Malware?

El malware es un programa malicioso que busca dañar a las computadoras y dispositivos móviles. Malware también se usa para nombrar distintos softwares hostiles, intrusivos o molestos que abren ventanas con publicidad.

Hay diferentes tipos de malware, y cada uno infecta o corrompe dispositivos de forma distinta, pero todas las variantes de malware están diseñadas para poner en peligro la seguridad y privacidad de los sistemas informáticos.

Tienen como objetivo:

- Robar información personal
- Robar tarjetas de créditos y contraseñas
- Espiar.
- Cobrar rescate en criptomonedas (monedas digitales como el Bitcoin).
- Bloquear equipos.
- Destruir información.
- Utilizar tu computadora o celular para minería de criptomonedas.
- Usar tu computadora para impedir el acceso a sitios web.
- Mostrar publicidad no deseada.

¿Cómo funciona el malware?

Todos los tipos de malware siguen el mismo patrón básico: Su dispositivo se infecta después de descargar o instalar software malicioso involuntariamente, por lo general al hacer clic en un enlace infectado o al visitar un sitio web infectado.

La mayoría de las infecciones se producen cuando se realiza sin saberlo una acción que provoca la descarga del malware. Esta acción podría ser un clic en el enlace infectado de un correo electrónico o la visita a un sitio web malicioso.

En otros casos, los hackers extienden el malware mediante servicios entre

iguales de compartición de archivos y paquetes de descarga de software gratuitos. Incrustar código informático malicioso en un torrent o una descarga popular es una manera efectiva de extenderlo por una base de usuarios más amplia.

Los dispositivos móviles también pueden infectarse mediante mensajes de texto.

¿Cómo circula el malware?

- Computadoras y dispositivos móviles
- Correo electrónico
- Redes sociales

Legislación sobre ciberdelitos en Argentina

¿Qué se considera ciberdelito? En el portal oficial argentino, Argentina.gob, se describe al ciberdelito como conductas realizadas en detrimento de una persona. Las mismas se producen en el ciberespacio a través del uso de dispositivos electrónicos y redes informáticas.

Con el fin de brindar normativa a los delitos informáticos, y regular las nuevas tecnologías como medios para cometer delitos, en Junio del 2008 se incorpora al Código Penal Nacional la Ley N° 26.388 de Delitos Informáticos. Dentro de esta ley de carácter nacional podemos encontrar las distintas normativas legales que conciernen a las nuevas tecnologías, y que cuyos contenidos marcan una guía relevante para el desarrollo de las tareas y funciones de los profesionales informáticos que investigan este tipo de delitos.

A partir del Decreto 577/2017 se crea en Argentina el *Comité de Ciberseguridad* con el fin de determinar la responsabilidad en casos de ciberseguridad y protección de infraestructuras de información y comunidades digitales.

Los ciberdelincuentes utilizan diversas técnicas de manipulación para obtener engaños, hacerse de datos personales, acosar sexualmente o hacerse pasar por la víctima. En cualquier caso es indispensable buscar ayuda, por lo que en el año

2222 fue necesario ampliar el *Programa Las Víctimas Contra las Violencias* (Línea telefónica 137) para brindar contención, orientación y acompañamiento a víctimas de violencia familiar, sexual, grooming, sexting, explotación sexual en las redes, y otros.

Bibliografía:

ARGENTINA, H. C. D. L. N. (n.d.). *Argentina.gob.ar*. Recuperado de https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto
Argentina.gob.ar. (n.d.). ¿Qué es el Malware? Recuperado de https://www.argentina.gob.ar/guia-practica-para-adultos-amenazas-en-internet/que-es-el-malware

Argentina.gob.ar. (n.d.). ¿Qué es el phishing? Recuperado de

https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/phishin

Argentina.gob.ar. (n.d.). Pautas para evitar que los adolescentes apuesten online Recuperado de https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/pautas-para-evitar-que-los-adolescentes-apuesten-online

Claves para entender y abordar el bullying. (n.d.). Aula Abierta. https://aulaabierta.info/claves-para-entender-y-abordar-el-bullying/

Confederación Don Bosco. (2023). Recursos didácticos para la prevención de la ludopatía. Pasaporte00. Recuperado de https://pasaporte00.confedonbosco.org/wp-content/uploads/2023/07/CASTELLANO-recursos-didacticos-para-la-prevencion-ludopatia.pdf

De Ley, P. (n.d.). https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2023/PDF2023/TP2023/4336-D-2023.pdf

De Salud, M., Sobre, M., Patológico, J., De Prevención P., Asistencia, Y.,

Compulsivo, A. (n.d.). *MANUAL SOBRE JUEGO PATOLÓGICO UNA EXPERIENCIA EN LA PROVINCIA DE BUENOS AIRES PROGRAMA DE PREVENCIÓN Y ASISTENCIA AL JUEGO COMPULSIVO; Ministerio de Salud*. https://www.loteria.gba.gov.ar/images/docs/manual_sobre_juego_patologico.pdf

Domínguez, M (2009). Epidemiología y factores implicados en el juego patológico, Guía clínica. Actuar ante el juego patológico, 27 (1), 3-20. Doi: 0213-3334.

"EDUCACIÓN 3.0." *EDUCACIÓN 3.0*, 14 Mar. 2019, www.educaciontrespuntocero.com/entrevistas/ludopatia-absentismo-escolar/.Recuperado 3 Aug. 2024.

HONORABLE CONGRESO DE LA NACIÓN ARGENTINA. "Argentina.gob.ar." *Argentina. gob.ar*, 2020, www.argentina.gob.ar/normativa/nacional/ley-27590-345231/texto. Accessed on 4 Aug. 2024.·

Pautas para evitar que los adolescentes apuesten online. (2024, March 11). Argentina.gob.ar. https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/pautas-para-evitar-que-los-adolescentes-apuesten-online

Pereyra, J. (2009). Que es la ludopatía. Revista infotigre, recuperado de: http://www.revistainfotigre.com.ar/2009/01/13/que-es-la-ludopatia/

¿Qué es la Huella Digital En Internet?" *Argentina.gob.ar*, 17 Apr. 2020, www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-la-huella-digital-en-internet.