#DigitSafe

Boosting Digital Safe Spaces and Resilience

Manual de resiliencia digital

CONEXX-EU
inova aspire
CESUR Tu Centro Oficial de FP
Co-funded by the Erasmus+ Programme of the European Union

Contenido

Introducción

El proyecto #DigitSafe, Boosting Digital Safe Spaces and Resilience, tiene como objetivo empoderar a los jóvenes para que se conviertan en ciudadanos digitales resilientes y seguros, permitiéndoles hacer frente a algunos de los desafíos e impactos negativos de la era digital. Esto está en línea con el Objetivo 6, "Información y diálogo constructivo", de la Estrategia de la UE para la Juventud 2019-2027.

El proyecto #DigitSafe persigue fomentar un conocimiento más amplio y profundo entre los jóvenes sobre los dos temas clave de la ciberseguridad y el discurso de odio, y la seguridad y la privacidad. El proyecto tiene como objetivo principal llegar a los grupos de jóvenes más vulnerables, mediante la creación de espacios y prácticas digitales más seguras, a la vez que se potencian sus capacidades en términos de resiliencia digital.

Este proyecto también quiere alcanzar los siguientes tres objetivos principales específicos:

1. Promover la ciudadanía digital entre los jóvenes de los países participantes, de acuerdo con la Estrategia de la UE para la Juventud 2019-2027, empoderándolos con información práctica y recopilada sobre Seguridad y Privacidad, y Discurso de Odio y Ciberacoso.

2. Proporcionar a los jóvenes, especialmente a los que tienen menos oportunidades y que a menudo carecen de conocimientos sobre información y datos, las competencias necesarias para mejorar su resiliencia digital.
3. Desarrollar una metodología innovadora que traduzca la información relevante recopilada en este manual en una campaña de concienciación pública multicanal, utilizando las prácticas de comunicación audiovisual, el lenguaje, las herramientas y las tendencias más comunes entre los jóvenes. Se tratará de una estrategia multimedia y multicanal que explote el gran número de posibilidades de creación de contenidos accesibles a todos los usuarios en el actual panorama de las redes sociales, con el objetivo de reforzar la capacidad de los jóvenes para tomar decisiones racionales y conocer sus derechos digitales.

Este Manual de Resiliencia Digital ofrecerá una orientación completa y unificada, que abarcará información y consejos prácticos (incluyendo recursos legales, psicológicos, de formación y de aprendizaje abierto), y hará recomendaciones clave para ayudar a los jóvenes a adquirir un conocimiento más profundo de sus derechos,

riesgos y amenazas digitales en el contexto de estos temas. Concienciará sobre las oportunidades y los recursos disponibles para desarrollar las habilidades necesarias para hacer frente a los problemas que surgen en la vida digital actual de los jóvenes. Capacitará a los jóvenes para que se conviertan en ciudadanos digitales comprometidos y fomenten un mundo digital más seguro. Recopilará una gran cantidad de información, unificándola de forma más útil y completa.

#DigitSafe
Boosting digital safe spaces and resilience

Co-funded by the
Erasmus+ Programme
of the European Union

1. Ciberacoso

1.1. ¿Qué es el ciberacoso?

A nivel europeo, se han encontrado múltiples definiciones de ciberacoso que incorporan diversos aspectos en función de las características específicas de los países en los que se ha realizado el estudio (Bélgica, Bulgaria, Países Bajos y España). Sin embargo, el estudio desarrollado en 2016 por el Departamento de Políticas de Derechos Ciudadanos y Asuntos Constitucionales perteneciente al Parlamento Europeo "El ciberacoso entre los jóvenes", ha elaborado una definición bastante precisa y homogénea que puede ser utilizada transnacionalmente en la Unión Europea:

- El ciberacoso describe aquellas situaciones en las que el acoso tiene lugar en Internet, principalmente a través de los teléfonos móviles y las redes sociales. El ciberacoso corresponde, por tanto, a un acto igualmente agresivo e intencionado, llevado a cabo mediante el uso de las tecnologías de la información y la comunicación (TIC)."

Al igual que el acoso fuera de línea, el ciberacoso suele contar con los siguientes tres participantes clave:

- El **agresor**: *la persona que lleva a cabo la agresión.*
- La **víctima**: *la persona que sufre la agresión.*
- Los **espectadores**: *aquellos que ven lo que ocurre entre el acosador y la víctima, pero no están directamente implicados en el acoso.*

La conducta debe producirse de forma intencionada y reiterada y debe existir un desequilibrio en las relaciones de poder entre el agresor y la víctima.
Hay características clave del ciberacoso que facilitan su identificación y comprensión:

- El ciberacoso es malicioso y nunca accidental. El ciberacoso tiene el objetivo claro y consciente de dañar a la víctima, causarle dolor, humillarla, hacerla sufrir física o mentalmente.
- Se realiza desde una posición de poder. El ciberacosador siempre tiene ventaja y ocupa una posición de superioridad. Dependiendo del entorno en el que se produzca el ciberacoso, puede tratarse de un ciberacoso en grupo contra una víctima que está sola.

Los agresores pueden aprovecharse de una víctima no agresiva o vulnerable, incapaz de defenderse.

- Es repetitivo y tiene como objetivo intimidar, enfadar o avergonzar a las víctimas. Una acción agresiva aislada no es todavía ciberacoso. Se convierte en ciberacoso cuando la agresión se repite una y otra vez contra la misma persona (o las mismas personas).

La digitalización ha multiplicado los canales por los que se puede perpetrar el acoso a través de Internet. Sin embargo, algunas de las formas más comunes de atacar a las víctimas del ciberacoso son las siguientes:

Redes sociales

Teléfonos móviles

Plataformas de comunicación

Plataformas de juego

Para aclarar qué acciones ilegales entrarían dentro del ciberacoso, he aquí algunos ejemplos:

- *Difundir mentiras o publicar fotos/vídeos vergonzosos de alguien en las redes sociales.*
- *Enviar mensajes ofensivos o amenazas a través de plataformas de comunicación.*
- *Enviar mensajes maliciosos bajo la identidad de otra persona.*

1.2 La importancia del ciberacoso y sus consecuencias: concienciación y cómo identificarlo

Identificación del ciberacoso

Una de las claves para hacer frente al ciberacoso es ser capaz de identificarlo y estar atento a las señales de alarma. No existe una definición universalmente aceptada de ciberacoso a nivel internacional o europeo.

Sin embargo, la Comisión Europea define el ciberacoso como "el acoso verbal o psicológico repetido llevado a cabo por un individuo o un grupo contra otros a través de los servicios en línea y los teléfonos móviles". (2) Según el Consejo de Europa, el ciberacoso se distingue de otros tipos de acoso

(2)'Cyberbullying among Young People', Directorate General for Internal Policies (European Parliament), 2016, p.8.

debido al riesgo de exposición pública, a las complejas funciones de los observadores y al tamaño de la audiencia que conllevan las tecnologías digitales y la comunicación.(3)

Para crear un mundo más tolerante y seguro en línea, el ciberacoso debe abordarse a mayor escala, tanto a nivel individual como organizativo.

Las consecuencias del ciberacoso no pueden tomarse a la ligera ni considerarse meras bromas, ya que no sólo se niegan las emociones y el sufrimiento de la víctima, sino que se normaliza este tipo de violencia en el entorno digital. Las consecuencias del ciberacoso pueden ser duraderas y afectar a las víctimas de muchas maneras.

Podríamos destacar como principales consecuencias del Ciberacoso:

- **Consecuencias mentales y emocionales**

Las víctimas pueden sentirse tristes, avergonzadas, tontas, deprimidas, enfadadas y ansiosas. Las víctimas suelen perder el interés por las cosas que antes les gustaban. Desarrollan una baja autoestima, o se sienten aislados, incapaces de comunicarse con sus compañeros. A veces, las víctimas del ciberacoso pueden convertirse en "víctimas-agresores", replicando el comportamiento y acosando a otros.(4)

(3) https://www.coe.int/en/web/campaign-free-to-speak-safe-to-learn/preventing-bullying-and-violence [accessed 27/05/2022)
(4) Joint Research Centre (2013). Social Networks and Cyberbullying among Teenagers

- **Consecuencias físicas** - El estrés y la ansiedad que sufre la víctima pueden provocar problemas físicos, como la sensación de cansancio por las alteraciones del sueño o la experimentación de verdaderos síntomas de salud, como dolores de estómago o de cabeza.
- **Consecuencias legales** - La sensación de estar siendo ridiculizado o acosado por otros suele impedir que las víctimas del ciberacoso denuncien o intenten solucionar el problema. Esto, unido a la lenta evolución en la tipificación legal del delito, hace que a menudo quede impune y fomenta la repetición de los ataques.

Para prevenir el ciberacoso, es fundamental concienciar a la población sobre su existencia. El primer paso para identificar el ciberacoso es tener una definición clara de lo que implica. En Europa se han tomado decisiones políticas y se han definido y aplicado numerosos programas para prevenir el ciberacoso.

El Centro de Investigación del Ciberacoso ha elaborado una serie de consejos estructurados sobre cómo proceder para prevenir el ciberacoso y asegurarnos como usuarios. La prevención es siempre la mejor opción para luchar contra este problema.

Dirigido a los jóvenes:

- Manténgase al día con la configuración de privacidad: los sitios y programas de las redes sociales modifican y actualizan su configuración de privacidad con frecuencia. Asegúrate de estar familiarizado con las nuevas opciones de perfil y mantén la mayor cantidad de información posible restringida a las personas en las que realmente confías.
- Restringe el acceso a tu información de contacto: no des tu correo electrónico ni tu número de teléfono a personas que no conoces. Además, mantén tu correo electrónico y tu número de teléfono fuera de las redes sociales.
- Aprende la etiqueta de Internet - Para evitar posibles problemas con otros internautas, aprende las convenciones sociales relacionadas con la interacción en el ciberespacio.
- No envíes fotos o vídeos inapropiados - Recuerda que el novio, novia o pareja de hoy puede ser el amante despechado de mañana. No quieres que alguien con fotos o vídeos inapropiados tuyos los publique en Internet y los comparta con el resto del mundo. No te pongas en la situación de tener que preocuparte por esto.

- Búscate a ti mismo en Google - Siempre debes saber lo que se dice de ti. A menudo es sorprendente encontrar información que pensabas que era privada que aparece en bases de datos públicas, nuevos artículos o en páginas de medios sociales que han sido indexadas por los motores de búsqueda.
- No aceptes solicitudes de amistad de extraños - Si no conoces a la persona que te envía una solicitud de amistad o de seguimiento, ignórala. La mayoría de las redes sociales y aplicaciones también te dan la opción de bloquear al usuario si quieres.
- Utiliza controles basados en el sitio - desactiva las opciones de búsqueda en determinados sitios de redes sociales para evitar que cualquier persona del público en general te busque o te envíe mensajes.
- Mantenga su información protegida - Si utiliza un ordenador público o una red inalámbrica, asegúrese de cerrar la sesión de cualquier sitio en el que esté cuando se aleje de ese ordenador, aunque sea por un minuto.

- Sé escéptico en las interacciones en línea - Incluso entre personas de confianza, es arriesgado revelar demasiada información porque nunca sabes con certeza si la persona con la que crees que te estás comunicando está realmente ahí, o si está sola.
- Protégete de la gente - Recuerda que algunas personas tienen mucho tiempo libre y lo único que quieren es hacer la vida imposible a los demás. No se lo permitas. Resístete a poner en línea demasiada información personal o privada que pueda ser utilizada para acosarte o humillarte y resístete a interactuar con ellos de cualquier manera.

Dirigido a profesores y padres:

Es importante que las organizaciones, las escuelas, los lugares de trabajo y los individuos se comprometan a hacer frente al ciberacoso debido al impacto que éste puede tener en las víctimas. La investigación desarrollada por el Centro de Investigación del Ciberacoso en 2021 "Cyberbullying: Identificación, prevención y respuesta" ofrecía una amplia explicación de cómo los profesores y los padres podían abordar el ciberacoso en términos de identificación y prevención.

Educar a la comunidad sobre un uso responsable de los dispositivos centrado en la ciudadanía digital es quizás el paso preventivo más importante en lo que respecta a las instituciones educativas y sus profesores/profesores.

En otras palabras, es importante no sólo confiar en la educación formal, sino utilizar actividades no formales e informales en las escuelas para combatir y prevenir el ciberacoso desde un punto de vista creativo.

Por otro lado, los padres "deben demostrar a sus hijos con palabras y acciones que ambos desean el mismo resultado final: que el ciberacoso cese y que la vida no se haga aún más difícil".

¿Cómo deben reaccionar los padres si descubren que su propio hijo es un ciberacosador? En primer lugar, deben explicarle cómo ese comportamiento está provocando e infligiendo daño y dolor en el mundo real. Después, los padres deben ser capaces de darle la oportunidad de seguir adelante y poner fin a ese comportamiento. Los niños deben saber que toda acción, aunque sea en línea, tiene consecuencias graves. Por parte de los padres, es esencial empezar a prestar más atención al comportamiento y las acciones de sus hijos en Internet.

1.3 Directrices: ¿Cómo tratar a las víctimas de ciberacoso?

(Procedimientos, empatía, la importancia de escuchar, apoyo emocional, apoyo psicológico)

Cuando tú mismo eres una víctima:

Si estás sufriendo ciberacoso, te aconsejamos que sigas esta serie de pasos:

- Busca ayuda En primer lugar, debes hablar con familiares o profesionales.
- Denuncia el contenido Si el ciberacoso se ha producido a través de una red social, denuncia el contenido a esa plataforma. Esto no siempre es efectivo, pero es importante que la red social sepa quién es el acusado para que pueda tomar medidas, a veces después de varias denuncias.
- Protégete Cambia tu contraseña, aumenta la privacidad de tus publicaciones, elimina información personal como tu dirección de correo electrónico, número de teléfono o enlaces a otras cuentas. Como medida temporal, **elimina tu cuenta o cambia tu nickname.**

- Póngase en contacto con el proveedor de servicios de Internet (ISP) Intente ponerse en contacto con el proveedor de servicios de Internet de la persona que le está acosando si ha sido identificada. El ISP puede entonces ponerse en contacto con la persona o quizás cerrar su cuenta de Internet directamente.
- Presenta una denuncia acudiendo a una comisaría de policía Lleva pruebas del ataque (por ejemplo, capturas de pantalla). La policía tomará nota de tu denuncia y de toda la información relacionada con ella y la incluirá en un reporte.
- Denuncia el ciberacoso públicamente Comparte las capturas de pantalla del acosador (asegúrate de ocultar el nombre de usuario y la foto de perfil del acosador para que no te acusen de difamación).

Como profesor:

Los profesores tienen que prestar atención a diferentes signos que pueden mostrar que un niño está siendo ciberacosado. Algunos de estos signos pueden ser un rápido aumento o disminución del uso del dispositivo o una respuesta emocional a lo que está sucediendo en su dispositivo. Si un niño esconde su pantalla o dispositivo cuando otros están cerca y evita la discusión, esto debe tenerse en cuenta.

Además, los profesores también tienen que ayudar a los niños a identificar, responder y evitar el ciberacoso. Algunas normas serían:

- La comunicación es muy importante, así que si alguna vez crees que un niño está siendo víctima de ciberacoso, habla con él en privado y pregúntale al respecto. También puedes hablar con los padres al respecto. Los profesores pueden ser un mediador entre el niño, los padres y la escuela.
- Promover un entorno de clase seguro. Ayudar a los niños a desarrollar la inteligencia emocional para que puedan aprender habilidades de autoconciencia y autorregulación y aprender a tener empatía con los demás.

- Anima a los alumnos a prestar atención a las señales que pueden ayudarles a identificar cuando ocurre algo en los medios digitales que les hace sentirse incómodos, preocupados, tristes o ansiosos.
- Enséñales a pensar antes de publicar.
- Explica a los alumnos las tres formas en las que pueden y deben responder si son testigos del ciberacoso: si apoyas a la víctima del acoso, eres un aliado, si intentas detener el ciberacoso eres un defensor y si eres víctima del ciberacoso tienes que denunciarlo a un adulto.

Como padre:

Es muy probable que los niños no reconozcan que están siendo ciberacosados porque pueden sentirse avergonzados. Es muy común que los jóvenes sufran en silencio. Pueden tener miedo de que los padres reaccionen restringiendo su acceso a Internet, pueden sentirse avergonzados por no poder ocuparse ellos mismos del acoso.

Por estas razones, si los padres ven algún signo en sus hijos, deben actuar inmediatamente. En primer lugar, intenten hablar con su hijo y escucharlo.

Entabla una conversación con ellos sobre lo que está ocurriendo de forma calmada. Tómate tu tiempo para entender exactamente lo que ha ocurrido y el contexto en el que se ha producido.

Una vez que lo sepa, ofrézcale consuelo y apoyo incondicional, ya que las víctimas de ciberacoso suelen experimentar sentimientos de aislamiento. Muéstrele a su hijo que esta situación puede ser tratada de una manera que no implique represalias en línea. Hacer que su hijo se sienta seguro, debe ser la prioridad principal, así como hacerle saber que no es su culpa.

A continuación, intente reunir todas las pruebas posibles. Imprime o haz capturas de pantalla o grabaciones de conversaciones, mensajes, fotos, vídeos y otros elementos que puedan servir como prueba clara de que tu hijo está siendo víctima de ciberacoso.

El siguiente paso es ponerse en contacto con el proveedor de contenidos, ya que el ciberacoso siempre viola las condiciones de servicio de todos los proveedores de servicios legítimos. Deberían tomar medidas al respecto para que tu hijo no vuelva a sufrirlo.

Si el ciberacosador es un compañero de clase o va al mismo colegio que tu hijo, debes notificarlo al centro educativo lo antes posible, ya que puede tener normas para responder al ciberacoso.

Los padres también pueden ponerse en contacto con la policía en caso de que los pasos anteriores mencionados no ayuden a mejorar la situación.

Si es necesario, intente buscar asesoramiento para su hijo. Los niños pueden beneficiarse de hablar con un profesional de la salud mental. Es posible que prefieran dialogar con un tercero que se perciba como más objetivo.

1.4 Medidas de prevención

No hay una manera infalible de evitar que un niño sea objeto de ciberacoso. Sin embargo, hay diferentes maneras de reducir la probabilidad de que sean el objetivo.

En primer lugar, es importante utilizar contraseñas en todo y no compartirlas con nadie.

Los niños tienen que saber que es importante mantener la privacidad de las cosas personales. Nunca deben compartir su dirección, número de teléfono móvil o dirección de correo electrónico en Internet. Deben tener cuidado con compartir demasiada información sobre el lugar al que van a la escuela, especialmente si tienen amigos o seguidores en línea que no conocen muy bien.

También deben saber que tienen que cerrar la sesión cuando utilicen dispositivos públicos, como ordenadores públicos o portátiles en la escuela o la biblioteca. Esto incluye cerrar la sesión del correo electrónico, las cuentas de las redes sociales, su cuenta escolar o cualquier otra cuenta que puedan abrir.

Por último, pero quizás lo más importante, los niños deben ser conscientes de que si alguna vez son víctimas de ciberacoso, deben denunciarlo a sus padres o profesores.

1.5 Cómo denunciar el ciberacoso
(Marco legal, instituciones, ONGs, etc.)

Uno de los aspectos más significativos de la denuncia del ciberacoso es que la mayoría de los países europeos no tienen una legislación específica sobre el ciberacoso.

A pesar de la importancia, el gran número de casos y la preocupación entre los jóvenes, la legislación no ha avanzado todavía en este ámbito. Esto ha hecho que la labor de las instituciones y organizaciones sea esencial para ayudar a identificar los casos, denunciarlos y dar apoyo a las víctimas.

2. Discurso de odio

2.1 ¿Qué es el discurso del odio?

No existe una definición universalmente aceptada de la incitación al odio. En esta sección, esbozaremos un par de definiciones que se recogen tanto en la legislación de la UE como en las principales organizaciones que luchan contra la incitación al odio.

- (Ilegal) La legislación de la UE define la incitación al odio como "*la incitación pública a la violencia o al odio basada en determinadas características, como la raza, el color, la religión, la ascendencia y el origen nacional o étnico*". Aunque la Decisión Marco se refiere al racismo y la xenofobia, la mayoría de los Estados miembros han ampliado su legislación nacional para incluir otros motivos como la orientación sexual, la identidad de género y la discapacidad. (5).

2.2 ¿Cómo prevenir el discurso de odio?

Una forma de combatir la incitación al odio es bloquear y denunciar las cuentas de incitación al odio que encuentres en la red (véase la siguiente sección sobre consejos para denunciar la incitación al odio).

Las Naciones Unidas recomiendan comprometerse con las siguientes prácticas para prevenir la incitación al odio (6):

((5) Code of Conduct- Illegal Online Hate Speech Questions and Answers, (European Commission 2016) https://ec.europa.eu/info/sites/default/files/code_of_conduct_hate_speech_en.pdf
(6) United Nations- how to deal with hate speech? https://www.un.org/en/hate-speech/take-action/engage

- **Haz una pausa** - evita hacer comentarios de odio y/o compartir ese tipo de contenido.
- **Comprueba los datos** - asegúrate de que detectas la información falsa y tendenciosa antes de difundirla.
- **Desafío** - difunde tu propio discurso de oposición y desafía el discurso de odio siempre que sea posible.
- **Apoyo** - adopte una postura pública y extienda su solidaridad a las víctimas de la incitación al odio.
- **Denuncia** - consulta las directrices comunitarias de las plataformas de medios sociales que utilizas y denuncia los casos de incitación al odio que infrinjan estas directrices. En los casos más graves, puedes presentar una denuncia ante la policía (por ejemplo, cuando hay incitación a la violencia).
- **Educa** - comparte recursos educativos y campañas públicas o inicia conversaciones con tus amigos y familiares.
- **Comprométete** - considera la posibilidad de unirte a una ONG o a una iniciativa que trabaje para hacer frente a la incitación al odio en tu comunidad.

www.un.org/en/hate-speech/take-action/engage

2.3 ¿Cómo denunciar los discursos de odio?

Los usuarios pueden denunciar directamente cualquier incidente de incitación al odio a través del canal de medios sociales en el que lo encuentren. El sitio web del Consejo de Europa ofrece información sobre cómo denunciar en los canales de las redes sociales. En algunos casos no es necesario tener una cuenta para denunciar. Por ejemplo, en Facebook puedes rellenar este formulario online sin tener o estar conectado a una cuenta de Facebook.

Algunos países europeos han introducido procedimientos y mecanismos nacionales de denuncia de la incitación al odio, los delitos de odio y el ciberacoso en el marco de la "Campaña Juvenil No Hate Speech" de los Consejos Europeos.

Otras sugerencias para denunciar la incitación al odio son:

- Denuncia el discurso de odio a la policía.
- Informa a un organismo autorizado, por ejemplo, un tribunal civil o administrativo.
- Denuncia a una ONG, por ejemplo, MiND es el centro nacional de denuncia de discursos de odio y contenidos discriminatorios en los Países Bajos.
- Habla con alguien de confianza, por ejemplo, un padre, un amigo, un profesor.

3. Ciberseguridad y privacidad

3.1. ¿Por qué es importante la protección de los datos personales?

El término protección de datos personales se define en el Art. 4 (1) del Reglamento General de Protección de Datos: los datos personales son cualquier información relacionada con una persona física identificada o identificable. Los nombres y las direcciones de correo electrónico son obviamente datos personales. La información sobre la ubicación, el origen étnico, el género, los datos biométricos, las creencias religiosas, las cookies de la web y las opiniones políticas también pueden ser datos personales. En los próximos párrafos exploraremos más a fondo los tipos de datos que requieren protección.

La protección de datos es importante, ya que evita el uso indebido de la información de un individuo o una organización, tiene como objetivo prevenir diferentes riesgos para la privacidad y la seguridad, como las actividades fraudulentas, la piratería informática, el phishing y el robo de identidad.

3.2. Tipos de datos personales y amenazas y delitos contra la privacidad

1 **Robo de identidad**

El robo de identidad es el delito que consiste en obtener la información personal o financiera de otra persona para utilizar su identidad para cometer un fraude, como realizar transacciones o compras no autorizadas. El robo de identidad se comete de muchas maneras diferentes y sus víctimas suelen quedar perjudicadas en su crédito, sus finanzas y su reputación. El ladrón de identidad puede utilizar su información para solicitar un crédito, declarar impuestos u obtener servicios médicos.

2 **Acoso sexual online**

El acoso sexual online se define como una conducta sexual no deseada en cualquier plataforma digital y se reconoce como una forma de violencia sexual. El acoso sexual en línea abarca una amplia gama de comportamientos que utilizan contenidos digitales (imágenes, vídeos, mensajes, páginas) en una variedad de plataformas diferentes (privadas o públicas).

3 Phishing

Los ataques de phishing son la práctica de enviar comunicaciones fraudulentas que parecen proceder de una fuente de confianza. Suele realizarse a través del correo electrónico. El objetivo es robar datos confidenciales, como la información de las tarjetas de crédito y los datos de acceso, o instalar un malware en la máquina de la víctima. El phishing es un tipo común de ciberataque que todo el mundo debería conocer para protegerse.

4 Fraudes y estafas en Internet

El fraude por internet implica el uso de servicios y programas informáticos con acceso a internet para estafar o aprovecharse de las víctimas. El término "fraude por internet" abarca generalmente la actividad cibercriminal que tiene lugar en internet o en el correo electrónico, incluyendo delitos como el robo de identidad, el phishing y otras actividades de piratería informática diseñadas para estafar a la gente.

5 Estafas de tarjetas de felicitación

Muchos ataques de fraude por Internet se centran en acontecimientos populares para estafar a las personas que los celebran. Esto incluye los cumpleaños, la Navidad y la Pascua, que suelen celebrarse compartiendo tarjetas de felicitación con amigos y familiares por correo electrónico. Los hackers suelen aprovecharse de ello instalando software malicioso dentro de una tarjeta de felicitación por correo electrónico, que se descarga e instala en el dispositivo del destinatario cuando éste abre la tarjeta de felicitación.

6 Estafas con tarjetas de crédito

El fraude con tarjetas de crédito suele producirse cuando los piratas informáticos adquieren de forma fraudulenta los datos de las tarjetas de crédito o débito de las personas en un intento de robar dinero o realizar compras. Para obtener estos datos, los estafadores de Internet suelen utilizar ofertas de tarjetas de crédito o préstamos bancarios demasiado buenas para ser verdad para atraer a las víctimas. Por ejemplo, una víctima puede recibir un mensaje de su banco diciéndole que puede optar a una oferta de préstamo especial, o que se ha puesto a su disposición una gran cantidad de dinero en forma de préstamo.

7 Estafas en las citas online

Otro ejemplo típico de fraude en Internet es el exceso de aplicaciones y sitios web de citas en línea. Los hackers se centran en estas aplicaciones para atraer a las víctimas a fin de que envíen dinero y compartan datos personales con nuevos intereses amorosos. Los estafadores suelen crear perfiles falsos para interactuar con los usuarios, entablar una relación, ganarse poco a poco su confianza, crear una historia falsa y pedir al usuario ayuda financiera.

8 Fraude en la cuota de la lotería

Otra forma común de fraude en Internet son las estafas por correo electrónico que dicen a las víctimas que han ganado la lotería. Estas estafas informan a los destinatarios de que solo pueden reclamar su premio después de haber pagado una pequeña cuota.

9 El Príncipe de Nigeria

La estafa utiliza la premisa de una familia o individuo nigeriano rico que quiere compartir su riqueza a cambio de ayuda para acceder a su herencia. Utiliza tácticas de phishing para enviar mensajes de correo electrónico que describen una historia emocional, y luego atrae a las víctimas con la promesa de una importante recompensa económica. La estafa suele comenzar pidiendo una pequeña cantidad para ayudar con los procesos legales y el papeleo con la promesa de una gran suma de dinero más adelante.

10 Spam

El spam es cualquier tipo de comunicación digital no deseada y no solicitada que se envía en masa. A menudo el spam se envía por correo electrónico, pero también puede distribuirse a través de mensajes de texto, llamadas telefónicas o redes sociales.

3.3. Cómo denunciar las amenazas a la ciberseguridad en las redes sociales/instituciones

Todas las redes sociales han establecido mecanismos para denunciar diferentes tipos de amenazas a la ciberseguridad, como la incitación al odio en línea, el robo de identidad, el acoso sexual, el ciberacoso, etc.

A continuación puedes encontrar información sobre algunas de las redes sociales más populares:

Facebook

- Los problemas de seguridad en Facebook tienen múltiples categorías. Puede haber un contenido abusivo o una página de odio que quieras denunciar, o tal vez alguien esté suplantando tu identidad en Facebook, etc. La mejor manera de denunciar un contenido abusivo o spam en Facebook es utilizando el enlace Denunciar que está cerca del propio contenido.

https://www.facebook.com/help

Twitter

- En el Centro de Ayuda de Twitter puedes encontrar información y apoyo en caso de cuentas comprometidas y hackeadas, sobre privacidad, spam y cuentas falsas, contenido sensible y ofensivo, comportamiento abusivo y su denuncia.

https://help.twitter.com/en

Instagram

- Denunciar los posts:

Si ves una publicación, un mensaje o una cuenta que crees que va en contra de las Normas de la Comunidad de Instagram, puedes denunciarlo. Puedes denunciar contenidos individuales tocando los tres puntos que aparecen sobre una publicación, manteniendo pulsado un mensaje o visitando una cuenta y denunciando directamente desde el perfil. Para más información, visita el Centro de Ayuda de Instagram.

- Denunciar las cuentas:

Las cuentas que infrinjan las Directrices de la Comunidad de Instagram pueden denunciarse en la aplicación o a través de un formulario web. Para más información, puedes consultar el Centro de ayuda.

https://help.instagram.com/

TikTok

- Si tienes preguntas, dudas o problemas con tu perfil, puedes encontrar información y ayuda escaneando el código que aparece a continuación. En la sección Seguridad puedes ir a Reportar un problema y reportar un video en vivo, un comentario en vivo, un video, un comentario, un mensaje directo, un sonido, un hashtag, y también puedes reportar a alguien. Los pasos son muy fáciles de seguir, sólo tienes que buscar la opción Denunciar y seguir las instrucciones.

https://support.tiktok.com/en/

3.3. Cómo evitar los riesgos de seguridad de los datos

Una de las cosas más importantes para mantener nuestros datos protegidos es tener una contraseña fuerte. Será muy útil ya que hoy en día los ciberdelincuentes siguen pensando en nuevas e innovadoras formas de hackear las cuentas y hacerse con los datos personales.

Además, para mantener su información protegida se recomienda utilizar sólo sitios web de confianza. Muchas personas no saben cómo comprobar si un sitio web es seguro o no, por lo que se darán algunos consejos.

1. En primer lugar, compruebe si la URL tiene la ortografía correcta, está asegurada con "https" y tiene algún tipo de indicador de que está verificada, como un signo de candado.

2. En segundo lugar, los sitios web que parecen inseguros suelen serlo. Si el propietario del sitio web no invierte en la apariencia y la experiencia del usuario, probablemente no esté invirtiendo en la seguridad del sitio.

3 En tercer lugar, debe poder comprobar que hay información de contacto disponible, así como una política de privacidad accesible. Éstas suelen encontrarse en la parte inferior de la página de inicio. Otro consejo útil es leer algunos testimonios y reseñas del sitio por parte de otras personas para que pueda conocer las experiencias que otras personas tuvieron al utilizar estos sitios web.

También hay otras prácticas que pueden poner en riesgo la seguridad digital como el uso de WIFI público. Es cierto que este servicio que ofrecen algunos hoteles y aeropuertos es gratuito, pero tiene un precio.

Estos puntos de acceso WIFI gratuitos permiten a los hackers situarse entre la persona que lo utiliza y el punto de conexión, por lo que, en lugar de hablar directamente con el punto de acceso, la gente envía su información al hacker, que luego la utiliza.

¿Cómo pueden los particulares proteger sus datos personales?

1 Proteja sus cuentas

2 Proteja su navegación por Internet

3 Utilice un software antivirus en su ordenador

4 Actualiza tus programas y dispositivos

5 No instales programas que no conozcas y en los que no confíes plenamente

6 Desactive el Bluetooth cuando no lo utilice

7 Sé demasiado cuidadoso a la hora de compartir información personal

8 Ten cuidado con los suplantadores de identidad

9 No compartas demasiada información en las plataformas de redes sociales

10 Personaliza la configuración de privacidad de tus redes sociales

11 No olvides cerrar la sesión

12 No abras correos electrónicos de personas que no conoces

13 No guardes las contraseñas en tu navegador

14 No utilices las credenciales de las redes sociales para registrarte o iniciar sesión en sitios de terceros

15 Elige un proveedor de correo electrónico seguro y de confianza

4. Conclusiones

A lo largo de este manual se han explicado y contextualizado el ciberacoso y el discurso de odio. Sus definiciones pueden variar a lo largo de los diferentes países, sin embargo ambos se consideran como una agresión a otras personas. En el caso del Ciberacoso normalmente hay tres actores (el autor, la víctima y los espectadores), en el caso del Discurso de Odio, es más difícil establecer un escenario común, pero igualmente implica a una persona que discrimina y al receptor que es discriminado.

Este manual incluye diferentes formas de identificar, tratar y denunciar el ciberacoso y la incitación al odio, por supuesto, dependerá de quién sea la víctima (tú mismo, un colega, tus hijos, etc.) pero también del marco legal del país.

Por ejemplo, en España se puede denunciar a la policía, mientras que en los Países Bajos existe una línea de ayuda nacional contra la discriminación. Además, se muestra por qué son importantes conceptos como la protección de datos o la tríada CIAD, así como los tipos de amenazas a la privacidad, como el robo de identidad, el acoso sexual en línea, el phishing o los fraudes.

En conclusión, este documento no sólo ofrece definiciones o conceptos clave sobre el ciberacoso y la incitación al odio, sino que también sirve de guía para prevenir, reaccionar y denunciar este tipo de abusos.

#DigitSafe
Boosting digital safe spaces and resilience

Co-funded by the
Erasmus+ Programme
of the European Union

Preguntas & informaciones:

info@digit-safe.com

www.digit-safe.com