LA SEGURIDAD EN LAS REDES SOCIALES

ORGANIZACIÓN JUVENIL ESPAÑOLA

David Sánchez-Porro Carmona

0. INTRODUCCIÓN:

¡Buenos días a todos!

Hoy nos encontramos aquí para hablar sobre un tema que nos afecta a todos en nuestra vida digital: la seguridad en las redes sociales.

Todos somos usuarios de las redes sociales y es importante ser consciente de los peligros de un mal uso de estas redes tanto en el ámbito profesional, personal o como miembros de una asociación juvenil como la OJE.

En la era de la conectividad y la comunicación "online", las redes sociales se han convertido en una parte esencial de nuestras vidas. Sin embargo, también han traído consigo riesgos en cuanto a nuestra privacidad y seguridad en internet.

En esta mesa de debate, exploraremos los riesgos asociados al uso de las redes sociales y proporcionaremos algunas pautas para mantenernos seguros mientras navegamos en este mundo de conectividad.

DAVID.

1. PRINCIPALES REDES SOCIALES

Esta es la lista de las 10 Redes Sociales con más usuarios a comienzos de 2023:

- **Facebook**: Es la red social más grandes y populares del mundo con casi 3.000M de usuarios. Permite a los usuarios compartir publicaciones, fotos, videos y conectarse con amigos y familiares.
- **YouTube**: Es la plataforma líder para compartir videos con 2.500M de usuarios. Los usuarios pueden subir, ver y compartir videos en una amplia variedad de temas.
- **WhatsApp** (2.000M): Una aplicación de mensajería instantánea que permite a los usuarios enviar mensajes de texto, voz, imágenes y videos, así como realizar llamadas de voz y video.
- **Instagram**: 2.000M. Una plataforma centrada en el contenido visual, donde los usuarios pueden compartir fotos y videos, así como interactuar con otras cuentas a través de “likes” (me gusta) y comentarios.
- **WeChat**: Con casi 1.400M de usuarios. Aplicación de mensajería instantánea, que permite a los usuarios conectarse entre sí, encontrar información y enviar mensajes (de las más usadas en China (Welxin)
- **Tiktok**: 1.000M. Una plataforma de redes sociales centrada en videos cortos y creativos, donde los usuarios pueden mostrar sus talentos y habilidades (con Douyin 715M de usuarios más).
- **LinkedIn**: 750M usuarios. Es una red social orientada al ámbito profesional. Los usuarios pueden establecer conexiones con colegas, buscar empleo, publicar currículos y participar en grupos de discusión relacionados con su industria.
- **Telegram**: 700M. Aplicación social de mensajería para compartir mensajes de texto, audio-llamadas, video-llamadas, archivos, “stickers”, ubicación,…
- **Snapchat**: 600M. Una red social basada en el intercambio de fotos y videos que desaparecen después de ser vistos por el destinatario.
- **Twitter**: 370M. Una red social de “microblogging” que permite a los usuarios compartir mensajes cortos, llamados "tweets", con sus seguidores. Es conocida por la rápida difusión de información y noticias.

2. RIESGOS DE LAS REDES SOCIALES

2.1 Pérdida de la privacidad:

Uno de los mayores riesgos que enfrentamos en las redes sociales es la exposición de nuestra información personal. A menudo, compartimos detalles sobre nuestras vidas, nuestras familias o nuestras actividades sin considerar las consecuencias que esto puede tener. Los datos personales pueden ser utilizados por personas malintencionadas para cometer robo de identidad, estafas o acosar a los usuarios.

Compartir información personal “online” puede tener consecuencias negativas si no se protege adecuadamente. La privacidad en las redes sociales es fundamental para evitar el robo de identidad, el acoso cibernético y otras formas de delitos “online”.

Riesgos asociados con la falta de privacidad: Cuando no se protege la privacidad en las redes sociales, los ciberdelincuentes pueden recopilar información personal como nombres, direcciones, números de teléfono, e incluso detalles sobre la ubicación y las actividades diarias. Esta información puede ser utilizada para cometer fraudes, enviar “spam”, acosar o difamar a los usuarios.

Conclusión: La privacidad en las redes sociales es un aspecto esencial de nuestra seguridad “online”. Es importante ser consciente de los riesgos asociados con la falta de privacidad y tomar medidas para proteger nuestra información personal en plataformas digitales. Al ajustar la configuración de privacidad, compartir información con responsabilidad y ser cauteloso con las solicitudes de amistad y etiquetado, podemos disfrutar de una experiencia más segura y protegida en las redes sociales. ¡Recuerda, tu privacidad es tu responsabilidad!

2.2 Ciberacoso:

Las redes sociales pueden ser un espacio propicio para el acoso “online”. La facilidad de comunicación puede dar lugar a la difamación, el odio y el acoso cibernético, afectando negativamente la vida de las personas.

El ciberacoso usa tecnologías digitales, como redes sociales, mensajes de texto, correos electrónicos y otras plataformas “online”, para acosar, intimidar, hostigar o molestar a otra persona. Esta forma de acoso puede tener efectos graves en la víctima y puede ocurrir en cualquier contexto, ya sea en la escuela, en el trabajo o en la vida personal o social.

Algunas formas comunes de ciberacoso incluyen:

a) “**Ciberbullying”:** El acoso “online” entre niños y adolescentes, que puede incluir el envío de mensajes amenazantes o insultantes, la difusión de

rumores malintencionados o la publicación de contenido humillante o vergonzoso.

b) “**Grooming online”:** Cuando un adulto se hace pasar por un niño o adolescente para ganar la confianza de un menor con el fin de explotarlos sexualmente o emocionalmente.

c) **Difamación “online”:** La publicación de información falsa o difamatoria sobre alguien “online” con la intención de dañar su reputación.

d) “**Sextorsión”:** Cuando un acosador amenaza con difundir imágenes o videos íntimos de la víctima a menos que cumpla con sus demandas.

e) **“Trolling”:** Comportamiento provocativo y hostil “online” con el propósito de generar respuestas emocionales y conflictos.

El ciberacoso puede tener graves consecuencias para las víctimas, que pueden experimentar ansiedad, depresión, aislamiento social y problemas académicos o laborales. En algunos casos extremos, el ciberacoso ha llevado al suicidio de la víctima.

Conclusión: Es importante tomar medidas para prevenir y abordar el ciberacoso. Esto incluye educar a las personas sobre el uso responsable y respetuoso de la tecnología, fomentar una cultura de apoyo y empatía “online”, y denunciar cualquier caso de acoso a las autoridades o plataformas “online” correspondientes.

Además, es esencial brindar apoyo y ayuda a las víctimas para que se sientan seguras y protegidas. La prevención y la concienciación sobre el ciberacoso son fundamentales para garantizar un entorno “online” seguro y respetuoso para todos.

2.3 “Phishing”:

El término ""“phishing”" proviene de la combinación de las palabras inglés "password" (contraseña) y "fishing" (pescar), haciendo alusión al acto de pescar información confidencial.

El “phishing” (o estafa de suplantación de identidad) es una técnica de ciberdelincuencia en la que los estafadores intentan engañar a las personas para que revelen información confidencial, como contraseñas, información bancaria o datos personales, haciéndose pasar por una entidad o persona de confianza.

Las redes sociales son un caldo de cultivo para los ciberdelincuentes que intentan engañarnos para que revelemos información confidencial o hagamos clic en enlaces maliciosos. Las estafas de “phishing” pueden llevar a la instalación de software malicioso en nuestros dispositivos o la pérdida de acceso a nuestras cuentas. Pueden enviar mensajes engañosos que parecen legítimos, pero en realidad buscan obtener información confidencial, como contraseñas o datos bancarios.

Esta estafa generalmente se lleva a cabo a través de correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web falsos que imitan a empresas, instituciones o individuos legítimos. Los mensajes o sitios web falsos suelen tener una apariencia muy similar a la de las entidades que están suplantando, lo que puede hacer que los destinatarios caigan en la trampa.

Los estafadores pueden utilizar tácticas emocionales o de urgencia para incitar a las personas a actuar rápidamente y proporcionar su información. Algunos ejemplos comunes de “phishing” incluyen:

a) Correos electrónicos que afirman ser de un banco o entidad financiera solicitando información de cuenta o contraseñas.

b) Mensajes que indican que el destinatario ha ganado un premio o está siendo seleccionado para una oferta especial, pero debe proporcionar información personal para reclamarlo.

c) Sitios web falsos que imitan el diseño y la apariencia de plataformas populares, como redes sociales o tiendas “online”, para robar las credenciales de inicio de sesión de los usuarios.

Es importante ser consciente de las tácticas de “phishing” y estar atento a las señales de advertencia, como errores gramaticales o de ortografía en los mensajes, direcciones de correo electrónico o sitios web sospechosos, y solicitudes inusuales o inesperadas de información personal.

Conclusión: La concienciación y la precaución son fundamentales para evitar caer en una estafa de “phishing” y proteger nuestra información personal y financiera de posibles fraudes.

2.4 Suplantación de identidad:

En las redes sociales, es fácil hacerse pasar por otra persona o crear perfiles falsos. La suplantación de identidad puede llevar a la difamación, el acoso y otras formas de manipulación.

Para llevar a cabo la suplantación de identidad en redes sociales, los impostores pueden utilizar fotos e información personal de otras personas, utilizar nombres similares a personas conocidas o empresas, o incluso crear cuentas que parezcan ser de entidades legítimas.

Algunas razones comunes por las que alguien podría suplantar la identidad en redes sociales incluyen:

a) Estafas y fraudes: Los impostores pueden crear perfiles falsos para obtener información confidencial, como contraseñas, datos bancarios o información personal, con el fin de cometer estafas financieras o robo de identidad.

b) Ciberacoso: Algunas personas pueden crear perfiles falsos para acosar, amenazar o difamar a otros sin ser identificados.

c) Manipulación o engaño: Los impostores pueden crear identidades falsas para manipular emocionalmente a otros usuarios o para difundir información falsa o desinformación.

d) Falsificación de reputación: En algunos casos, las empresas o individuos pueden crear perfiles falsos para mejorar su reputación o para dañar la reputación de otros.

Conclusión: La prevención y la educación sobre la suplantación de identidad son fundamentales para proteger la seguridad y la privacidad en redes sociales y evitar ser víctima de engaños o fraudes “online”.

Es importante que los usuarios estén alerta y tomen precauciones para evitar caer en trampas asociadas a la suplantación de identidad en redes sociales.

3. ROL DE LOS PADRES/EDUCADORES EN LA PROTECCIÓN DE LA SEGURIDAD EN RRSS DE LOS MENORES

Los padres/educadores desempeñan un papel fundamental en la seguridad de las redes sociales, especialmente en los entornos donde los jóvenes están expuestos a estas plataformas y deben promover un uso seguro, ético y responsable de las RRSS potenciando:

a) **Concienciación y educación:** Se debe informar a los jóvenes sobre los riesgos asociados con el uso de las redes sociales, como el ciberacoso, el robo de identidad y la difusión de información falsa. Fomentar charlas de concienciación y seguridad "online" puede ayudar a que los jóvenes comprendan los peligros y aprendan a protegerse.

b) **Uso ético y responsable:** Enseñando a los jóvenes a utilizar las redes sociales de manera segura, responsable y ética. Esto incluye enfatizar la importancia de no compartir información personal sensible, respetar la privacidad de los demás y evitar el comportamiento dañino u ofensivo.

c) **Promover la privacidad:** Instruyendo a los jóvenes sobre cómo ajustar la configuración de privacidad en sus cuentas de redes sociales para controlar quién puede ver su contenido y cómo pueden proteger su información personal.

d) **Identificar señales de advertencia:** Debiendo estar atentos a posibles señales de que un joven está siendo acosado o afectado negativamente por el uso de redes sociales. Saber cómo identificar y abordar situaciones de ciberacoso es crucial para proteger a los jóvenes.

e) **Fomentar el respeto y la empatía "online":** Promoviendo un ambiente de respeto y empatía "online", alentando a los jóvenes a ser amables con los demás y a no participar en la difusión de rumores o información falsa.

f) **Modelar un comportamiento adecuado:** Sirviendo de ejemplo de uso responsable de las redes sociales. Al mantener una presencia "online" profesional y ética, pueden inspirar a los jóvenes a seguir su ejemplo.

g) **Fomentar la comunicación abierta:** Alentando a los jóvenes a hablar sobre sus experiencias "online" y a buscar ayuda si se sienten inseguros o incómodos en alguna situación en las redes sociales.

En definitiva, los padres y educadores tienen la responsabilidad de guiar a los jóvenes en el uso seguro y responsable de las redes sociales. Al proporcionar información, educación y apoyo, pueden ayudar a los jóvenes a navegar "online" de manera más segura y positiva.

La seguridad en las redes sociales debe ser un tema prioritario en la educación digital, ya que puede tener un impacto significativo en la vida de los chicos.

4. ¿QUÉ RESPONSABILIDAD TIENEN LAS EMPRESAS U ORGANIZACIONES (COMO LA OJE) EN LA PROTECCIÓN DE LA INFORMACIÓN DE SUS EMPLEADOS/ASOCIADOS EN LAS REDES SOCIALES?

Las asociaciones juveniles (y las empresas) tienen una gran responsabilidad en el uso de las redes sociales, ya que estas plataformas pueden ser una herramienta poderosa para la comunicación, la promoción de causas y la movilización de jóvenes en torno a temas de interés.

A continuación, se describen algunas de las responsabilidades clave de las asociaciones juveniles en las redes sociales:

a) **Fomentar un ambiente seguro y respetuoso**: Deben promover un ambiente "online" seguro y respetuoso para sus miembros y seguidores. Esto incluye establecer pautas de comportamiento adecuado en redes sociales y responder de manera proactiva a cualquier forma de acoso, discriminación o comportamiento inapropiado.

b) **Proteger la privacidad de los miembros**: Deben ser cautelosas con la información personal que comparten en las redes sociales, tanto de sus miembros como de otras personas. Es importante proteger la privacidad y la confidencialidad de los datos de los miembros y evitar compartir información que pueda poner en riesgo su seguridad.

c) **Transmitir información veraz y confiable:** Se debe ser cuidadosas al compartir información en las redes sociales y asegurarse de que sea precisa y verificada. Es importante evitar la propagación de noticias falsas o desinformación que pueda causar confusión o daño a la comunidad.

d) **Promover el respeto a los derechos de autor y propiedad intelectual:** Asegurándose de que el contenido que comparten en las redes sociales respeta los derechos de autor y la propiedad intelectual de terceros. No se deben utilizar imágenes, textos o cualquier otro material protegido por derechos de autor sin el permiso correspondiente.

e) **Impulsar la participación activa y la interacción de sus miembros** en las redes sociales y alentar la interacción y el diálogo constructivo. Esto puede incluir la realización de encuestas, debates y actividades "online" que involucren a la comunidad.

f) **Utilizar las redes sociales para promocionar sus objetivos y causas**: Las asociaciones juveniles pueden aprovechar las redes sociales para difundir información sobre sus actividades, eventos y proyectos, así como para sensibilizar sobre temas relevantes para los jóvenes. Esto puede ayudar a aumentar la visibilidad y el impacto de la asociación en la sociedad.

g) **Ser transparentes y responsables** con respecto a su identidad, objetivos y actividades en las redes sociales. También deben ser responsables de sus acciones y de la forma en que gestionan las interacciones "online".

Es importante también asegurar que las asociaciones juveniles vigilen posibles perfiles vinculados a ellas pero que no cumplan con algunos de los criterios u objetivos descritos anteriormente

Conclusión: Las asociaciones juveniles, y en particular me gustaría personalizar en la OJE, tienen la responsabilidad de utilizar las redes sociales de manera ética, segura y efectiva para promover sus objetivos y causas, proteger la privacidad y la seguridad de sus miembros y seguidores, y fomentar un ambiente de respeto y diálogo “online”.

Al hacerlo, pueden maximizar el potencial de las redes sociales como herramienta para la participación y el cambio positivo en la sociedad.

5. SEGURIDAD EN REDES SOCIALES. RESPONSABILIDADES DE LA PLATAFORMA

La seguridad en las redes sociales es una responsabilidad compartida entre los usuarios y las plataformas. Ambos tienen roles importantes que desempeñar para garantizar un entorno “online” seguro y protegido.

Responsabilidad de la Plataforma:

La disposición de plataforma Web o Redes Sociales obligan a cualquier organización (ya sea empresarial o asociación juvenil) al aseguramiento de unas pautas que promuevan un uso seguro del entorno, entre otras podemos destacar:

a) **Protección de datos del usuario:** Las plataformas deben tomar medidas para proteger los datos personales de los usuarios y garantizar que no sean compartidos o utilizados de manera indebida, cumpliendo la Ley de Protección de Datos de usuarios vigente en cada país.

b) **Políticas de seguridad y privacidad claras:** Las plataformas deben tener políticas de seguridad y privacidad claras y accesibles para los usuarios, para que estos estén informados sobre cómo se utilizarán sus datos y qué medidas de seguridad se implementan.

c) **Detección y eliminación de contenido dañino:** Es responsabilidad de la plataforma detectar y eliminar contenido dañino, como discurso de odio, acoso, noticias falsas y otros contenidos inapropiados, para mantener un ambiente seguro para los usuarios.

d) **Verificación de cuentas y perfiles:** Las plataformas deben implementar mecanismos de verificación de cuentas y perfiles, especialmente para figuras públicas o cuentas de alto impacto, para evitar la suplantación de identidad y proporcionar mayor confianza a los usuarios.

e) **Actualizaciones de seguridad:** Las plataformas deben mantener sus sistemas actualizados y protegidos contra vulnerabilidades de seguridad conocidas.

En conclusión, la seguridad en las redes sociales es una responsabilidad compartida entre los usuarios y las plataformas.

Las plataformas deben implementar políticas y medidas de seguridad efectivas para proteger la privacidad y seguridad de sus usuarios y crear un ambiente “online” seguro y protegido para todos.

6. TRUCOS PARA UNA “NAVEGACIÓN” SEGURA (USUARIO)

Para asegurar una navegación segura por las redes sociales evitando los riesgos expuestos anteriormente, debemos tomar ciertas medidas de seguridad que eviten nuestra exposición excesiva a la red, las más destacables serían:

1. **Actualizar contraseñas:** Cambiar regularmente las contraseñas y no usar la misma para todas las aplicaciones Las contraseñas deben contener letras, números y caracteres especiales. Evitar el uso de información personal es algo obvio.
2. **Autenticación de dos factores (2FA):** Activa la autenticación de dos factores siempre que sea posible. Esto añade una capa adicional de seguridad y requiere un código único enviado a tu dispositivo para iniciar sesión.
3. **Cerrar las sesiones activas en dispositivos que no sean de confianza** ayuda a prevenir el acceso no autorizado a nuestras cuentas de redes sociales.
4. **Ajustar la configuración de privacidad:** Es esencial revisar y ajustar cuidadosamente la configuración de privacidad en nuestras cuentas de redes sociales. Cada plataforma ofrece opciones para controlar quién puede ver nuestras publicaciones, quién puede enviarnos solicitudes de amistad y qué información personal está disponible públicamente. Limitar quién puede ver nuestra información personal y nuestras publicaciones es fundamental para proteger nuestra privacidad.
5. **Ser selectivos con las solicitudes de amistad:** No aceptar solicitudes de amistad de personas desconocidas o sospechosas. Es importante conocer a las personas con las que nos conectamos “online”. Es posible que los delincuentes cibernéticos intenten conectarse con nosotros para obtener acceso a nuestra información personal y…
6. **Evitar proporcionar información personal o confidencial a través de enlaces a sitios web o correos electrónicos no verificados** que solicitan información personal o financiera de manera inusual, revisando cuidadosamente la información y detalles de la cuenta para detectar señales de advertencia de posibles cuentas falsas o contactando directamente a la entidad o persona que supuestamente los envió.
7. **Cuidado con los enlaces y adjuntos:** No acceder a enlaces sospechosos o descargar archivos adjuntos de remitentes desconocidos. Estos pueden contener malware, virus que pueden dañar nuestros dispositivos y robar nuestra información o dirigirnos a sitios web maliciosos.
8. **Compartir información con responsabilidad**: Antes de publicar cualquier contenido en las redes sociales, es importante preguntarnos si realmente es necesario compartir esa información y las posibles consecuencias. Se debe tener especial cuidado con la información compartida en grupos o foros públicos, ya que puede ser accesible para una amplia audiencia y…
9. Ser consciente de los **riesgos del etiquetado y geolocalización**: Etiquetar a personas en publicaciones y usar la función de geolocalización puede

comprometer la privacidad. Es importante ser consciente de quiénes pueden ver las publicaciones en las que estamos etiquetados y desactivar la geolocalización si no es necesaria.

10. **Mantener el software y las aplicaciones actualizadas** para protegerse contra vulnerabilidades de seguridad conocidas.
11. **Reportar perfiles falsos o sospechosos (o comportamientos inapropiados)** a la plataforma de redes sociales para que sean investigados y eliminados.

En resumen, los usuarios deben tomar precauciones para proteger su información personal y mantenerse informados sobre las amenazas “online”.

7. CONCLUSIÓN:

Las redes sociales son una herramienta poderosa para conectarnos y comunicarnos, pero también pueden exponernos a riesgos significativos en términos de seguridad y privacidad.

Es fundamental que todos tomemos medidas para protegernos a nosotros mismos y a nuestros datos mientras navegamos "online".

Proteger nuestra privacidad y mantenernos alerta en internet nos ayudará a hacer un uso más positivo y beneficioso de las redes sociales.

Al ser conscientes de los riesgos y seguir las pautas de seguridad, podemos disfrutar de una experiencia más segura y positiva en las redes sociales.

La seguridad en las redes sociales es una responsabilidad que todos debemos asumir.

Recordad, la seguridad "online" es un trabajo en equipo, ¡así que compartan estos consejos con amigos y familiares!

¡Gracias por su atención!

REFERENCIAS:

- National Cybersecurity Alliance: http://staysafeonline.org
- Federal Trade Commision: http://onguardonline.gov
- Centro de Internet Segura (Internet Matters): https://www.internetmatters.org/
- INformation Commissioner's Office (ICO): https://ico.org.uk/
- National Cybersecurity Center (NCSC): https://www.ncsc.gov.uk/
- Nationl Institute of Standards and Technology (NIST) US.: https://www.nist.gov/cybersecurity-framework
- https://es.statista.com
- Información obtenida a través de comunicación personal con chatbot de IA, julio-agosto 2023
- Páginas de ayuda y soporte de las redes sociales: Facebook, Instagram,…