COLEGIO DE ODONTÓLOGOS Y ESTOMATÓLOGOS A CORUÑA

Informe ICOEC

La redes sociales y la comunicación con los pacientes

Un cambio de paradigma

Con la llegada de Internet el modelo de comunicación tradicional ha sufrido un cambio sin precedentes en la sociedad. La comunicación unidireccional ha perdido su monopolio con una fuerte competencia en cuanto a las posibilidades de informarse y comunicarse. Entramos en la era de la comunicación bidireccional, donde el emisor se vuelve receptor y el receptor emisor de la información. Las fuentes de información se democratizan y el acceso a las bases de datos es ya universal. El acceso a la información por parte del paciente es cada vez más fácil y cambia el modelo de relación Odontólogo- paciente, ya que éste cada vez está más informado, conoce mejor su patología y posibilidades de tratamiento y tiene acceso a las mismas fuentes de información que el propio profesional de la Odontología.

El papel clave de las Redes Sociales

Cuando parecía que los modelos de comunicación interactivos habían alcanzado su máximo nivel con la llegada de Internet, aparecen en escena las Redes Sociales que han transformado nuevamente los modelos de comunicación. La eclosión de las Redes Sociales ha traído consigo el desarrollo de la expresión más pura de la comunicación interactiva, englobando en ello la comunicación personalizada. Un fenómeno social que está cambiando la forma de relacionarnos y comunicarnos entre nosotros. Los datos hablan por si solos. En poco menos de una década, más de veinticinco millones de españoles utilizamos las Redes Sociales en sus diferentes facetas, y este fenómeno social también está influyendo de una forma determinante en la comunicación entre los pacientes y en el modelo de relación Odontólogo- paciente.

Hoy día ya pocos dudan de la labor que las Redes Sociales ejercen sobre los pacientes, facilitando la búsqueda de información sobre síntomas o enfermedades, interactuando con asociaciones y grupos de apoyo que padecen la misma enfermedad, interactuando con los profesionales sanitarios o intercambiando informaciones y experiencias con personas que están en su misma situación.

Pero este modelo de comunicación no sólo ha traído ventajas al paciente, sino que el profesional de la Odontología también se beneficia de ello, facilitando su actualización contínua, y al tiempo consiguen que la relación entre profesionales sea más fácil y fluida, posibilitando la interactuación con los pacientes o facilitando la transmisión de información fiable y de calidad a la población sobre prevención de patologías y control de enfermedades.

COLEGIO DE ODONTÓLOGOS Y ESTOMATÓLOGOS A CORUÑA

Informe ICOEC

No existe sin embargo ningún tipo de reglamentación ni normas que adecuen la utilización de las redes sociales a nuestros códigos éticos y deontológicos, y por ello hemos querido en este breve informe, reflejar la opinión que este Colegio profesional – ICOEC – tiene acerca de la adecuada utilización de las redes sociales en nuestra relación con nuestros pacientes.

Decálogo ICOEC sobre redes sociales

Consideraciones preliminares

- Las redes sociales suponen un beneficio real en la comunicación con nuestros pacientes pero en modo alguno pueden sustituir a la relación interpersonal, que es el elemento clave en la relación Odontólogo – Paciente.
- La utilización de las redes sociales debe estar en todo momento controlada por el profesional de la Odontología, quién a su vez se hace responsable de los contenidos científicos y técnicos que en su web y en sus redes sociales se utilicen y propaguen.
- En las comunicaciones se debe respetar la privacidad del paciente, no lesionar su derecho al honor y evitar la difusión de imágenes y vídeos que no supongan un beneficio real para el tratamiento del paciente.
- Creemos que es necesario distinguir entre difusión de la ciencia y exhibición pública de un profesional, acción que por desgracia es cada vez más habitual en nuestra profesión, y cuyo objetivo tiene un claro y exclusivo interés comercial.
- Cuando nos comuniquemos con otros profesionales sobre nuestros pacientes con los cuales intercambiamos información, debemos de respetar el secreto profesional y no comprometer la identidad del paciente
- Los datos sensibles o confidenciales que compartamos con otros profesionales deben evitar redes no seguras como Dropbox o wifis gratuítas. Te aconsejamos consultar el documento que adjuntamos sobre seguridad en redes sociales.
- No debemos de contribuir al desprestigio de otros profesionales mediante nuestra participación activa en redes sociales. Recordemos que nuestras opiniones siempre hablan por boca de un profesional de la Odontología.

COLEGIO DE ODONTÓLOGOS Y ESTOMATÓLOGOS A CORUÑA

Decálogo básico del Odontólogo en Redes Sociales

- La comunicación profesional entre el Odontólogo y el paciente mediante SMS, correo electrónico, WhatsApp ..etc, debe sustentarse y contar con el consentimiento expreso y por escrito del paciente.
- Nuestros comentarios en redes sociales pueden ser considerados legalmente como parte de nuestra actividad profesional
- Nunca debemos compartir en redes sociales datos o imágenes que puedan desvelar la identidad del paciente
- No debemos asociar los videos de nuestras intervenciones clínicas o quirúrgicas con la inserción de publicidad explícita o subliminal
- Siempre debemos de tener en cuenta la magnificación de las redes sociales y su implicación jurídica
- Ante una crisis de reputación profesional en internet, nunca debemos de actuar de manera irracional o impulsiva, sino siguiendo criterios profesionales, ya que nuestra probabilidad de una nueva equivocación es muy elevada.
- No debemos generar comentarios favorables en internet que no sean ciertos, ni tampoco borrar continuamente mediante procedimientos informáticos, los comentarios que consideramos desfavorables.
- Es necesario monitorizar de vez cuando las redes sociales para conocer nuestro estatus profesional y así poder diseñar una estrategia adecuada, proporcional y coherente con nuestra actividad profesional.
- La difusión explícita de imágenes o videos con procedimientos quirúrgicos o invasivos, suelen generar entre la población, el efecto contrario del que a veces queremos alcanzar
- Las Redes Sociales no deben ser la disculpa para que modifiquemos los criterios éticos y deontológicos que deben seguir guiando nuestra actividad profesional.

Colegio de Odontólogos y Estomatólogos de A Coruña

ICOEC 2017

Guía de Seguridad en Redes Sociales

INTRODUCCIÓN

Las redes sociales son parte de los hábitos cotidianos de navegación de gran cantidad de personas. Cualquier usuario de Internet hace uso de al menos una red social y muchos de ellos participan activamente en varias de ellas. Para muchos usuarios (especialmente los más jóvenes), **las redes sociales son el principal motivo para conectarse a Internet.**

Sin embargo, a partir de su uso, los usuarios se ven expuestos a un conjunto de amenazas informáticas, que pueden atentar contra su información, su dinero o incluso su propia integridad.

Ante la creciente tendencia de los ataques informáticos a utilizar las redes sociales como medio para su desarrollo, se vuelve de vital importancia para el usuario, estar protegido y contar con un entorno seguro al momento de utilizarlas.

¿Cuáles son los principales ataques? ¿Cuáles son las principales medidas de seguridad? Esta guía responderá estas dos preguntas y mostrará al usuario las mejores prácticas para alcanzar una mayor protección mientras utiliza redes sociales.

REDES SOCIALES

Facebook

- Es la red social más popular del mundo.
- Durante el 2011 ha superado los 600 millones de usuarios en todo el planeta.
- Es la predilecta entre los más jóvenes; utilizada para armar redes de contactos entre amigos, entre otros usos.
- También es utilizada por empresas y organizaciones para comunicarse con el público.

MySpace

- Otra plataforma basada en las relaciones sociales, permite compartir perfiles de usuarios, amigos, fotos, música, etc.
- Facebook le ha quitado usuarios, aunque mantiene su importancia, por ejemplo, para la difusión de bandas musicales.
- A marzo del 2011, posee 34 millones de usuarios.

Twitter

- Red social de microblogging.
- Los usuarios comparten contenidos en un máximo de 140 caracteres.
- Ha sido una de las redes sociales de mayor crecimiento durante 2010.
- Posee más de 200 millones de usuarios.

Linkedin

- Red social para profesionales. Es la más utilizada en el ámbito corporativo.
- Permite a las personas tejer redes de contactos laborales, cargar sus curriculum vitae en la web, y disponer de ellos en formato público.
- A marzo del 2011, cuenta con 100 millones de usuarios registrados.

¿Cuáles son los riesgos en las redes sociales?

La información y el dinero de los usuarios son el objetivo de los atacantes, por lo que a mayor cantidad de usuarios, más atrayente se vuelve un sitio web para el atacante. Por lo tanto, más allá de todas sus ventajas, la navegación por los sitios web de redes sociales, implica exponerse a una serie de amenazas informáticas.

Malware

Imagen 1 – Sitio web de propagación de Boonana

- Acrónimo en inglés de las palabras malicious y software, es decir, código malicioso.
- Son archivos con fines dañinos que, al infectar una computadora, realizan diversas acciones, como el robo de información, el control del sistema o la captura de contraseñas.
- Virus, gusanos y troyanos; son las variantes más conocidas en este campo.

A partir de estrategias de Ingeniería Social, los desarrolladores de malware suelen utilizar las redes sociales para propagar los códigos maliciosos.

El troyano Koobface es el más conocido de este tipo. Con nombre de acrónimo de la red social más popular (Facebook), este troyano se caracterizó en sus primeras campañas de propagación, por utilizar mensajes atractivos en redes sociales. Esta amenaza conforma una botnet, una red de equipos zombis que pueden ser controlados remotamente por el atacante.

En octubre del 2010 (a casi dos años de su aparición) surgió una nueva variante de Koobface (identificada como Boonana: Java/Boonana.A o Win32/Boonana.A) que tiene la particularidad de propagarse a través de Java, una tecnología multi-plataforma y que podía llevar a cabo una infección tanto en sistemas Windows, Linux y Mac OS. Al momento que la víctima visita la página maliciosa, la misma identifica qué sistema operativo está ejecutando el usuario, y descarga el archivo correspondiente a esa plataforma.

Phishing

- Consiste en el robo de información personal y/o financiera del usuario, a través de la falsificación de un ente de confianza.
- Es frecuentemente realizado a través del correo electrónico y sitios web duplicados, aunque puede realizarse por otros medios.

¿Cómo identificar un sitio de phishing?

No siempre es sencillo identificar un sitio web duplicado, aunque por lo general para llegar allí, el usuario ya debe haber sido víctima de alguna técnica de Ingeniería Social o de una infección de malware que lo enlazó al sitio malicioso.

Para el primer caso, es recomendable evitar hacer clic en enlaces sospechosos y en caso que alguna entidad solicite información sensible, acceder manualmente al sitio web esto es, sin utilizar ningún tipo de enlace, para verificar si en el mismo existe dicha solicitud.

Además, es recomendable verificar tanto el dominio en el sitio web, como que se utilice cifrado para transmitir los datos (protocolo HTTPS). Esto último, aunque no es garantía de la legitimidad de un sitio, sí es requisito indispensable y por lo general, los sitios de phishing no lo poseen.

Phishing

Ejemplo II: phishing a través de correo electrónico

Asunto: Facebook Password Reset Confirmation. Customer Support.
Fecha: Tue, 8 Dec 2009 10:13:58 +0800
De: Facebook Service <customer@facebook.com>
A: [redacted] com

Hey [redacted] ,

Because of the measures taken to provide safety to our clients, your password has been changed.
You can find your new password in attached document.

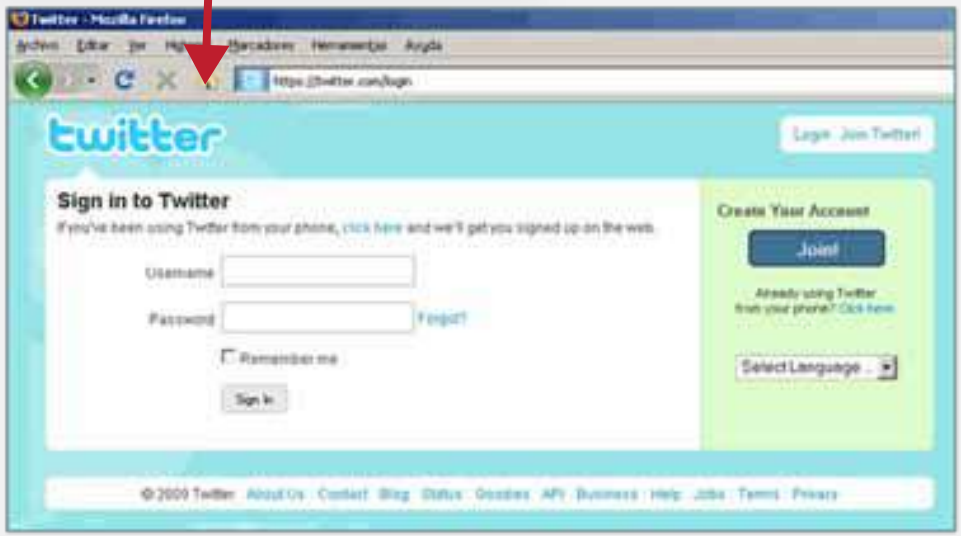
Thanks,
Your Facebook.

- - - -

Facebook_Password_833fd.zip
22 K Descargar

Ejemplo I: phishing a Twitter

El sitio original utiliza el protocolo seguro HTTPS:



El sitio original tiene el dominio correcto:

Robo de información

• En el uso diario de las redes sociales, los usuarios suben a la web diversos datos de índole personal que pueden ser de utilidad para los atacantes.

• El robo de información en redes sociales se relaciona directamente con el robo de identidad, uno de los delitos informáticos que más ha crecido en los últimos años.

• Los dos vectores de ataque más importantes para el robo de información son:

- **Ingeniería Social:** se busca el contacto directo con el usuario víctima, extrayendo información a través de la comunicación, la "amistad" o cualquier comunicación que permita la red social.
- **Información pública:** una mala configuración de las redes sociales puede permitir que información de índole personal esté accesible más allá de lo que el usuario desearía o le sería conveniente para su seguridad, por lo que personas malintencionadas podrían acceder a dicha información.

A Acoso y menores de edad

• Los niños utilizan las redes sociales desde muy temprana edad, incluso más allá de lo que las propias redes sociales indican como conveniente (Facebook, por ejemplo, fue concebida para mayores de 18 años).

• Existen una serie de amenazas que están enfocadas específicamente en los jóvenes que utilizan estos servicios: acoso (cyberbulling), grooming, sexting; son algunos de los riesgos a los que se ven expuestos al navegar por redes sociales.

• El rol de los adultos es fundamental para la protección de los niños: éstos no deberían utilizar las redes sociales sin contar con el apoyo, el diálogo y la educación de sus padres o cualquier otro adulto de referencia, incluso los propios maestros.

Formas de protección

Ante este escenario de amenazas, el uso de redes sociales puede parecer peligroso. No obstante, si se siguen los consejos brindados a continuación, es posible utilizarlas y contar con niveles de protección adecuados para un uso correcto y seguro de las redes sociales.

Se destacan como principales medidas: utilizar tecnologías de seguridad, configurar correctamente los usuarios en las redes sociales y utilizar el protocolo HTTPS para la navegación. No obstante, la constante educación del usuario y el uso cuidadoso al momento de la navegación, siempre permitirán minimizar de forma importante los riesgos a los que se ve expuesto.

UTILIZAR TECNOLOGÍAS DE SEGURIDAD

Siendo los códigos maliciosos la amenaza masiva más importante, la utilización de un software antivirus con capacidades proactivas de detección y con una base de firmas actualizadas, es un componente fundamental para prevenir el malware que se propaga por redes sociales.

Las herramientas de antispam y firewall también permiten optimizar la seguridad del sistema ante estos riesgos.

También es fundamental no utilizar un usuario administrador al momento de navegar por estas redes y contar con perfiles en las computadoras para cada usuario que las utilice. Esta es una forma de minimizar el impacto en caso que ocurra un incidente.

Finalmente, para controlar el uso por parte de los menores de edad, existen herramientas de control parental que permiten bloquear sitios web indeseados, así como también restringir el horario o cantidad de horas en que el niño utiliza las redes sociales.

CONFIGURAR LA PRIVACIDAD EN LAS REDES SOCIALES

Por defecto, no siempre las configuraciones en las redes sociales son las más óptimas para la seguridad del usuario. Por lo tanto, es recomendable dedicar un tiempo prudencial al momento de crear el usuario, además de revisar cuáles son las posibles fugas de información ante una mala configuración del sistema.

Configuraciones de privacidad en Facebook

• Evitar que ninguna configuración de perfil esté disponible de forma pública, sin limitaciones. Preferentemente, mostrar la información sólo a los amigos y, de ser posible, solo a un grupo de estos en caso de contar con un número elevado.

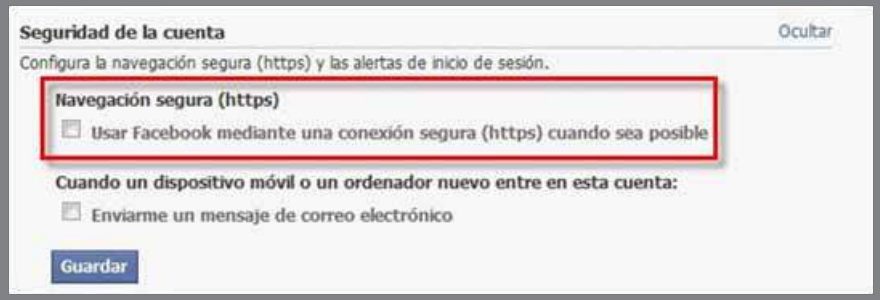
• Limitar el público que observa las fotos donde el usuario fue etiquetado, especialmente si se trata de un niño.

• Evitar que las aplicaciones puedan acceder a información personal, o publicar en el muro.

Más información: http://blog.eset.com/2011/05/25/facebook-privacy

En Facebook

Elegir la opción "Configuración de cuenta" en el menú "Cuenta" de la esquina superior derecha. Luego, dirigirse hacia la pestaña de "Seguridad de la cuenta" y se encontrará la posibilidad de optar por la navegación segura:



En Twitter

Ir a la configuración de la cuenta y marcar la casilla "usar siempre HTTPS", como se indica en la siguiente imagen:

CÓMO CONFIGURAR HTTPS EN FACEBOOK Y TWITTER

Configurar la navegación por el protocolo HTTPS, permite que todos los ataques relacionados a la interceptación de información que viaja en texto claro (legíble) a través de redes de computadoras, sean controlados. Con el protocolo HTTPS, todos los datos – no solo el usuario y la contraseña – viajarán cifrados y serán ilegibles para cualquier atacante en la red.

Es recomendable aplicar estas configuraciones especialmente útiles cuando el usuario se conecta a las redes sociales desde redes inalámbricas públicas.

GUÍA PARA EVITAR ENLACES MALICIOSOS EN TWITTER

- Solo hacer clic en aquellos enlaces publicados por contactos conocidos. Más allá que esto no es una garantía de seguridad, es una recomendación que vinculada con las siguientes, adquiere un peso considerable.
- Evitar seguir contactos desconocidos para disminuir la posibilidad de recepción de mensajes maliciosos.
- Si se sospecha de la legitimidad de un mensaje, es recomendable buscar partes del mismo o incluso el link dentro del buscador de Twitter y observar tanto su repetición como las opiniones de la comunidad quienes, al descubrir uno de estos engaños, no tardan en exponerlo dentro del mismo medio.
- Instalar un plugin para el navegador que resuelva las direcciones URL cortas y permita ver las originales sin la necesidad de hacerles clic en ellas, como es LongURL Mobile Expander.

DECÁLOGO DE SEGURIDAD EN EL CIBER ESPACIO

1. Evitar los enlaces sospechosos
2. No acceder a sitios web de dudosa reputación
3. Actualizar el sistema operativo y aplicaciones
4. Descargar aplicaciones desde sitios web oficiales
5. Utilizar tecnologías de seguridad
6. Evitar el ingreso de información personal en formularios dudosos
7. Tener precaución con los resultados arrojados por buscadores web
8. Aceptar sólo contactos conocidos
9. Evitar la ejecución de archivos sospechosos
10. Utilizar contraseñas fuertes

CONCLUSIÓN

Sin lugar a dudas las redes sociales son un valioso recurso para los internautas. No obstante, como se desarrolló en la presente guía, existen una serie de amenazas a las cuales se puede exponer el usuario durante el uso de las mismas. Por este motivo es recomendable no subestimar a los delincuentes informáticos y para ello, se debe hacer un buen uso de herramientas tecnológicas, tener configuraciones correctas, además de una conducta adecuada durante la navegación.

De esta forma, **será posible utilizar las redes sociales de forma segura.**