JUAN LUIS PÉREZ RÁNDEZ

CONSEJOS DE SEGURIDAD PARA UTILIZAR EN REDES SOCIALES

19 ABRIL 2018

ÍNDICE

ÍNDICE

¿QUÉ ES SEGURIDAD EN INTERNET?

La seguridad en internet son todas aquellas precauciones que se toman para proteger todos los elementos que hacen parte de la red como infraestructura e información, la más afectada por delincuentes cibernéticos.

Principales riesgos en internet:

Robo de información

Daño de información

Ataques a sistemas o equipos

Suplantación de identidad

Venta de datos personales

Robo de dinero

Ciberacoso

CIBERACOSO

Los ciberacosadores espían a los amigos, compañeros o familiares de la víctima para conseguir información de ella.

El acosador manipula a otras personas con falsa información en la red para afectar a una persona.

El acosador monitorea las actividades de la víctima en redes sociales y busca sacar información.

Estas actitudes se dan de forma repetitiva y dejan de ser un caso aislado de burla o chisme.

El acosador se burla frecuentemente de la víctima haciendo quedar mal a esta en internet, usando las redes sociales o los famosos memes, que son aquellas imágenes que buscan ser graciosas, pero que pueden generar muchos problemas.

Stalking

STALKING

Evita dar tu información personal, como correos electrónicos o números de teléfono, a desconocidos

No aceptes personas extrañas en tus redes sociales.

Configura la privacidad de tus redes sociales, según los intereses que consideres necesarios. Mira cómo hacerlo en Twitter y Facebook.

Reporta los correos sospechosos

Sé precavido con las cosas que publicas en internet.

Ante una situación sospechosa de alguien que te contactó por internet, acércate donde las autoridades pertinentes y cuéntales tu caso.

Sexting

SEXTING

Evita al máximo enviar contenido tuyo íntimo por medio de internet.

Cuando envíes material privado a otra persona, asegúrate que esta sea de plena confianza.

Si envías fotos o videos, ten certeza que el material sea borrado tanto del dispositivo de envío como en el de llegada.

Mantén actualizado tus equipos con antivirus para evitar que sean hackeados.

Ten contraseñas seguras en tus aparatos electrónicos para que en caso de pérdida o robo otras personas no puedan acceder a este material.

PISHING

PISHING

Mantenga buenos hábitos y no responda a enlaces en correos electrónicos no solicitados o en Facebook.

No abra adjuntos de correos electrónicos no solicitados.

Proteja sus contraseñas y no las revele a nadie.

No proporcione información confidencial a nadie por teléfono, en persona o a través del correo electrónico.

Compruebe la URL del sitio (dirección web). En muchos casos de phishing, la dirección web puede parecer legítima, pero la URL puede estar mal escrita o el dominio puede ser diferente (.com cuando debería ser .gov).

Mantenga actualizado su navegador y aplique los parches de seguridad.

CONSEJOS SEGURIDAD EN INTERNET

Configura la protección WPA2 en tu router

Tener buenas contraseñas en tus cuentas de usuario

Activar la verificación en dos pasos siempre que se pueda

Entender qué webs son seguras y cuáles no

Educar a los más jóvenes (y mayores) en seguridad

IMPORTANCIA CONTRASEÑAS

CONTRASEÑAS

Elige contraseñas fuertes o robustas de al menos 8 caracteres y compuesta por:

- mayúsculas (A, B, C…)
- minúsculas (a, b, c…)
- números (1, 2, 3…)
- y caracteres especiales ($, &, #...)

CONTRASEÑAS

NO utilices contraseñas fáciles de adivinar como:
“12345678”, “qwerty”, ”aaaaa”,
nombres de familiares,
matrículas de vehículos, etc.

CONTRASEÑAS

NO compartas tus contraseñas.
Si lo haces, dejará de ser secreta y estarás dando acceso a otras personas a tu privacidad.

CONTRASEÑAS

NO uses la misma contraseña en varios servicios.

CONTRASEÑAS

Elige un símbolo especial: “&”.
Piensa una frase que no se te olvide nunca y quédate
con sus iniciales: “En un lugar de la Mancha” -> “EuldlM”.
A continuación, selecciona un número: “2”

CONTRASEÑAS

Cuando manejas muchas contraseñas y no eres capaz de recordarlas todas, utiliza un gestor de contraseñas. Es un programa que te permite almacenar de forma segura tus claves de acceso a los diferentes servicios.
Solo necesitas recordar la clave de acceso al gestor de contraseñas, conocida como clave maestra, para consultar el resto de tus contraseñas.
Eso sí, si la olvidas no podrás consultar el resto, por tanto, memorízala bien en tu cabeza.

A PARTIR DE UNA FRASE

COMBINA DOS PALABRAS

COMBINA DOS PALABRAS

UNA PALABRA Y UN NÚMERO MEZCLADOS (PERO NO AGITADOS

Cambia tus contraseñas regularmente

Utiliza autenticación de dos factores

REDES SOCIALES

Utiliza contraseñas seguras

REDES SOCIALES

No aceptes solicitudes de amistad de desconocidos

REDES SOCIALES

Utiliza https:// y no http://

REDES SOCIALES

Se precavido cuando utilices un ordenador compartido

REDES SOCIALES

Usa herramientas para
administrar la seguridad

REDES SOCIALES

Utiliza antivirus actualizados

REDES SOCIALES

Cuidado con las estafas

REDES SOCIALES

Cuidado con el contenido de lo que publicas

REDES SOCIALES

Configura correctamente tu privacidad

REDES SOCIALES

REDES SOCIALES

Si el contenido es privado, párate y piensa si compartirlo

REDES SOCIALES

Cuidado con los contactos con los que compartes contenidos

REDES SOCIALES

Atento al dispositivo que utilices
(LOCALIZACIÓN)

REDES SOCIALES

Atento al dispositivo que utilices
(LOCALIZACIÓN)

REDES SOCIALES

No publicar nunca información privada

REDES SOCIALES

Al registrarnos en una red social, usar nuestra dirección de correo personal (no el correo de la empresa)

REDES SOCIALES

Tener cuidado con lo que publicamos sobre otras personas

REDES SOCIALES

Tenga cuidado al instalar apps extras

REDES SOCIALES

Leer con atención y de principio a fin la política de privacidad y las condiciones y términos de uso de la red social que escojamos

REDES SOCIALES

Usar opciones orientadas a la privacidad (comprobar quién puede ver nuestras fotos, quién puede ponerse en contacto con nosotros y quién puede añadir comentarios)

REDES SOCIALES

Usar opciones orientadas a la privacidad (comprobar quién puede ver nuestras fotos, quién puede ponerse en contacto con nosotros y quién puede añadir comentarios)

REDES SOCIALES

Hay cierto tipo de información que no deberías publicar en tus perfiles para que no comprometa tu privacidad ni sea utilizada en tu contra acarreándote problemas o conflictos personales o laborales:

- Datos personales
- Contraseñas
- Datos bancarios
- Teléfono móvil
- Planes para las vacaciones
- Comportamientos inapropiados
- Insultos, palabras malsonantes
- Ideologías
- Datos médicos o relativos a tu salud

REDES SOCIALES

Conocer quién tiene acceso a tus publicaciones

Saber quién te puede etiquetar

Si tu perfil está visible a los buscadores de Internet

Conocer la geolocalización de las publicaciones, etc.

REDES SOCIALES Y NIÑOS

Es necesario que los padres aprendan a utilizar el ordenador.

REDES SOCIALES Y NIÑOS

Fomentar el diálogo sobre hábitos de navegación y sus riesgos

REDES SOCIALES Y NIÑOS

Acordar unas normas de uso claras

REDES SOCIALES Y NIÑOS

Es una buena ayuda utilizar filtros de control de acceso a la red.

REDES SOCIALES Y NIÑOS

Es necesario colocar el ordenador en una zona de uso común.

REDES SOCIALES Y NIÑOS

Enseñarles en qué consiste la privacidad.

REDES SOCIALES Y NIÑOS

Explicarles que en la red también hay que respetar a los demás.

REDES SOCIALES Y ADOLESCENTES

Sexting: publicación de fotografías con fines “sexuales” o de "coqueteo" publicadas por los menores.

Grooming: acciones emprendidas por un adulto para ganarse la confianza de un menor y tratar de conseguir una cita para abusar sexualmente de él, extorsionarlo o incitar al sexting, entre otras acciones.

REDES SOCIALES Y ADOLESCENTES

Ciberbullying: ciberacoso psicológico entre los menores usando los canales sociales y de mensajería.

Hacking: suplantación de la identidad al acceder a las cuentas o perfiles de los menores.

REDES SOCIALES Y ADOLESCENTES

Phishing: obtención de datos personales a través de web ficticias con el fin de realizar hacking sobre alguna persona.

REDES SOCIALES Y ADOLESCENTES

Ser discreto: no dar datos personales.

No creerse todo lo que se lee.

Pensar dos veces antes de escribir.

Hacer un uso responsable y/o “profesional”.

Estar siempre alerta ante posibles comportamientos extraños.

REDES SOCIALES PRÁCTICO

PRIVACIDAD

REDES SOCIALES PRÁCTICO

PRIVACIDAD

REDES SOCIALES PRÁCTICO

PRIVACIDAD

REDES SOCIALES PRÁCTICO

PRIVACIDAD

REDES SOCIALES PRÁCTICO

REDES SOCIALES PRÁCTICO

PÁGINAS DE CONTROL PARENTAL GRATUITO

REDES SOCIALES PRÁCTICO

PRiVACiDAD Y SEGURiDAD EN iNTERNET

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta