TIC para el desarrollo

Seguridad en internet

Introducción

Intentar comunicar un secreto en voz alta en un entorno con mil testigos potenciales como Internet es difícil, y la probabilidad de que alguien escuche una conversación entre dos interlocutores se incrementa conforme lo hace la distancia que las separa. Dado que Internet es verdaderamente global, ningún secreto de valor debería ser comunicado a través de ella sin tener en cuenta aspectos de seguridad.

En el mundo de los negocios, información como números de tarjetas de crédito, autentificaciones de clientes, correos electrónicos e incluso llamadas telefónicas acaba siendo enrutada a través de Internet. Ya que gran parte de esta información corporativa no debe ser escuchada por terceras personas, la necesidad de seguridad es obvia.

Sin embargo, la Seguridad en Internet no es sólo una preocupación empresarial. Toda persona tiene derecho a la privacidad y cuando ésta accede a Internet su necesidad de privacidad no desaparece. La privacidad no es sólo confidencialidad, sino que también incluye el anonimato. Lo que leemos, las páginas que visitamos, las cosas que compramos y la gente a la que hablamos representan información que a la mayoría de las personas no les gusta dar a conocer.

Si las personas se ven obligadas a exponer información que normalmente desean ocultar por el hecho de conectarse a Internet, probablemente rechazarán todas las actividades relacionadas con la red. Por ello es fundamental tomar conciencia de los riesgos que implica la navegación en internet y el uso de aplicaciones electrónicas que ya son de uso cotidiano para nosotros, pero que encierran un riesgo potencial y no tomamos en cuenta medidas básicas de seguridad. El siguiente gráfico muestra algunos de los riesgos más comunes a los que estamos expuestos en internet.

Spam

El spam o correo basura son aquellos correos electrónicos que recibes de **personas que no conoces**. Normalmente buscan venderte algún producto, un servicio o promocionar un lugar por internet. Son muy incómodos porque llenan la capacidad de tu cuenta de correo con e-mails que no te interesan, impidiendo que te lleguen aquellos que sí quieres leer, y quitándole mucho de su valioso tiempo en identificarlos y borrarlos.

El spam es el instrumento preferido por los criminarles de internet para enviarte virus, gusanos y cualquier otro tipo de archivo que dañará tu computador. También es utilizado para engañarte, robar tu información personal e incluso también tu dinero.

Phising

Otra amenaza es el llamado *"phishing"*, palabra que hace alusión a "pescar" en inglés. Eso es lo que quieren precisamente estos criminales: te envían un e-mail como carnada tratando de engañarte para que entregues **información personal sensible** como tu nombre, documento de identificación, claves de banco, claves de e-mail o de cualquier otra cuenta que tengas por internet. Quieren pescar su información.

Estos correos parecen venir de una compañía confiable y se ven exactamente igual a como se ve la página de esa compañía. Incluyen un enlace al que le dicen debes entrar para actualizar datos o cambiar tus claves; y te asustan diciendo que perderás tu cuenta si no lo haces. Una vez ingresas y escribes tus datos, los criminales adquieren toda tu información y tratarán de utilizarla para robar tu dinero.

Debes ser cuidadoso y nunca acceder a tus cuentas desde los enlaces que le llegan por correo, sino que se debe teclear el nombre de la página que siempres has utilizado desde el navegador. Cuando recibas este tipo de e-mails consulta directamente con tu banco o la compañía de donde te piden datos para verificar y denunciar en caso de ser necesario.

Robo de identidad

Los criminales de internet a menudo intentan robar la identidad de las personas para hacerse pasar por ellos y robar su dinero.

Cómo lo hacen? Consiguen tu información personal y acceden a tus cuentas bancarias o a tus tarjetas de crédito para hacer compras no autorizadas y robarte.

Para evitarlo es importante **NUNCA entregar su número de tarjeta de crédito** en un lugar Esta y otras fichas están disponibles en formato digital **en www.imaginar.org**de internet que no conoces o en el cual no confías. Compra siempre en lugares bien conocidos. Tampoco entregues información sensible por

Fraude electrónico

Uno de los mecanismos que los criminales en línea usan para cometer fraudes electrónicos es enviándote e-mails que tratan de engañarte para que les dinero voluntariamente.

Algunos de los ejemplos más comunes son: Te envían un e-mail diciendo que ganó la lotería y le piden comprar un boleto por internet para que pueda reclamar el premio. **Pueden robarte el dinero o robar tus claves al hacerlo.**

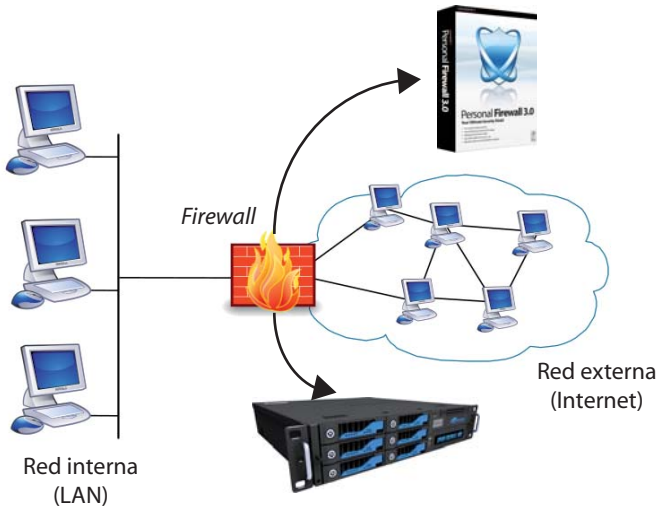
Te envían un e-mail pidiéndote una donación de dinero para una persona enferma de cáncer y te envían una foto de esa persona que te impresiones. Te piden hacer una transferencia de dinero para ayudar cuando en realidad te robarán el dinero.

10 Consejos de seguridad

1. Instala en tu computador un software antivirus. Paga una licencia y suscríbete a las actualizaciones. NO Piratees un software antivirus.
2. Complementa tu antivirus con protección anti-spyware para mantener la confidencialidad de la información de tu computador.
3. Una contraseña segura debe ser lo más larga posible y tener una mezcla de letras mayúsculas, minúsculas, número y símbolos.
4. No utilices las mismas claves que utilizas en chats o juegos, en otros lugares que requieren mayor seguridad como banca en línea o compras por internet.
5. Cambia las claves de seguridad de manera periódica.
6. Evita publicar tus cuentas de correo electrónico en páginas web de dudosa reputación.
7. No envíes datos confidenciales por correo electrónico.
8. No ejecutes archivos adjuntos que no hayas solicitado, cualquiera que sea la fuente y el medio de los que provengan.
9. Ten cuidado con noticias impactantes o curiosas, pues muchos piratas informáticos se aprovechan de este tipo de mensajes.
10. No compartas información demasiado personal o confidencial en redes sociales y recuerda que no todos son lo que dicen ser en internet.

Utilice un firewall

Un *firewall* o un cortafuegos es una parte de un sistema o una red que está diseñada para **bloquear el acceso no autorizado,** permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.



Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets.

Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar al cortafuegos a una tercera red, llamada Zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior. Un cortafuegos correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

Términos

LAN: de las siglas en inglés *Local Area Network,* es decir Red de Área Local. Se refiere a la red de computadoras y equipamiento privado de una organización.

Virus: Un virus informático es un programa que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.

Encriptacion: en el ámbito informático es el programa o dispositivo que altera las representaciones de un mensaje para transmitirlo con seguridad.

Cookie: literalmente galleta, es un fragmento de información que se almacena en el disco duro del visitante de una página web a través de su navegador.