10 consejos de seguridad para el uso del correo electrónico

El correo electrónico actualmente se ha constituido en uno de los medios de propagación e infección más utilizados. Personas mal intencionadas utilizan este medio de comunicación para reproducir todo tipo de **amenazas informáticas** que atentan contra la seguridad de los usuarios.

Mensajes en cadena (**Hoax**), correos electrónicos no deseados (**Spam**), estafas en línea por medio de **scam** o ataques de **phishing**, así como mecanismos de infección a través de **enlaces maliciosos** o por medio de **archivos adjuntos**, son solo algunos casos que demuestran la importancia de incorporar buenas prácticas de seguridad respecto al manejo del correo.

Consejos de seguridad orientados a aumentar los niveles de prevención y de esta manera mitigar el riesgo de sufrir un potencial ataque durante el uso del correo electrónico:

1. **No envíes correos en cadena**. Evita esta práctica ya que este tipo de mensajes generalmente suelen estar relacionados con algún tipo de engaño (**Hoax**). Ahora bien, si por algún motivo se desea reenviar el mensaje a muchos destinatarios, se recomienda entonces usar el campo **CCO** (**con copia oculta**) para insertar allí las direcciones. De esta manera las direcciones de correo de los usuarios de destino, no podrán ser visualizadas. Además, tomate un segundo para borrar aquellas direcciones del mensaje anterior que, por lo general, al momento de reenviar quedan consignadas en el cuerpo del mensaje.
2. **No publiques tu correo electrónico** en foros, sitios web, blog, redes sociales, conversaciones en línea y demás, ya que esto lo que hace es facilitarles las cosas a los *usuarios dedicados al envío de spam (spammers)* que podrán capturar tu cuenta e incluirla en su selecta lista para envió masivo de spam. Nunca publiques la cuenta de correo laboral.
3. **Utiliza cuentas de email alternativas** para los casos en los que se requiera tener que navegar o registrarse en sitios de dudosa procedencia o baja reputación. Esto con el fin de evitar la recepción de un mayor volumen de spam en la bandeja de entrada de nuestro email principal. También es recomendable usar cuentas de correos temporales y desechables, utilizando servicios como, por ejemplo: 10 Minute Mail, así es posible usar servicios en línea sin llenar nuestro buzón de correos no deseados. Siempre es bueno tener más de una cuenta de email, por lo menos 2 o 3 y cada una con un propósito específico, es decir, una para el trabajo, otra personal y alguna otra para uso público. Recuerda que la cuenta laboral es sólo para uso laboral.
4. **NO respondas a los correos tipo spam**, ya que, de hacerlo, le estará confirmando al spammer que su cuenta de correo se encuentra activa y en consecuencia seguirá recibiendo más mensajes de esta clase.
5. **Utilice contraseñas seguras para el acceso a su cuenta de correo** y configure su pregunta secreta de manera tal que sea difícil de adivinar. De esta forma evitamos el robo de nuestra cuenta.
6. **Elimine el historial de navegación, archivos temporales, cookies, datos en cache, etc.,** cuando termine una sesión de correo electrónico a la que haya accedido desde en una red pública. También en estos casos de uso de email en sitios públicos como por ejemplo un ciber-café o un hotel, resulta una buena práctica utilizar el modo de navegación anónima o privada, la cual es una funcionalidad disponible en muchos navegadores web en la actualidad.

10 consejos de seguridad para el uso del correo electrónico

7. **No descargue archivos adjuntos si no está seguro de su procedencia.** En caso de hacerlo, revíselo con su antivirus y así garantizar que no se traté de algún código dañino que pueda afectar su equipo. Además, verifique si estos archivos tienen doble extensión; si es así, sea precavido ya que probablemente se trate de un gusano o troyano, los cuales utilizan este modo de engaño para su propagación.
8. **Tenga presente que las empresas, no adjuntan archivos en sus actualizaciones de productos.** El envío de archivos con supuestas actualizaciones se constituye en un tipo de engaño muy común hoy día para propagar malware a través del email. Del mismo modo las organizaciones bancarias y financieras, nunca le solicitaran información personal por medio del correo. Si llega a recibir un mensaje de este tipo, tenga cuidado ya que puede ser víctima de un ataque de phishing que busque robarle sus datos. En estos casos denuncie el hecho en su entidad financiera de confianza.
9. **Como medida de seguridad, considere bloquear la visualización de imágenes en el cuerpo de los mensajes de sus correos**. Muchos servicios de webmail actualmente cuentan con esta funcionalidad. De esta manera es posible descargar o hacer visibles la imagen solo cuando estemos seguros de que el correo es de confianza. Muchos spammers en la actualidad, utilizan las imágenes para propagar sus anuncios publicitarios y evitar de esta manera los filtros antispam.
10. **Configure su cliente de correo electrónico con el filtro de correo no deseado**, personalizando las opciones para bloquear la recepción de estos correos.

Fuente: Hans Steffens en Consejos Seguridad Informática

En resumen:

1. No envíes correos en cadena y utiliza la opción de copia oculta (cco).
2. No publiques tu correo electrónico en foros, sitios web, blog, redes sociales, conversaciones en línea …
3. Utiliza cuentas de email alternativas para los casos en los que se requiera tener que navegar o registrarse en sitios de dudosa procedencia o baja reputación.
4. NO respondas a los correos tipo spam, ya que, de hacerlo, le estará confirmando al spammer que su cuenta de correo se encuentra activa
5. Utilice contraseñas seguras para el acceso a su cuenta de correo
6. Elimine el historial de navegación, archivos temporales, cookies, datos en cache, etc., cuando termine una sesión de correo electrónico a la que haya accedido desde en una red pública.
7. No descargue archivos adjuntos si no está seguro de su procedencia. En caso de hacerlo, revíselo con su antivirus
8. Tenga presente que las empresas, no adjuntan archivos en sus actualizaciones de productos. El envío de archivos con supuestas actualizaciones se constituye en un tipo de engaño muy común. Del mismo modo las organizaciones bancarias y financieras, nunca le solicitaran información personal por medio del correo.
9. Como medida de seguridad, considere bloquear la visualización de imágenes en el cuerpo de los mensajes de sus correos
10. Configure su cliente de correo electrónico con el filtro de correo no deseado