Los 25 errores más comunes en seguridad de correo electrónico

Artículo original en inglés: http://www.itsecurity.com/features/25-common-email-security-mistakes-022807/

Traducción: Angel Gottfriedt (F{-NixARg)

Adaptación y publicación: Lic. Cristian Borghello Director de www.segu-info.com.ar

Todavía recuerdo recibir mi primer correo electrónico de phishing en mi cuenta de AOL. Yo había ganado la lotería de AOL! Sonaba tan bien que fui escéptico en el mejor de los casos. Así sin pensarlo demasiado, abrí el correo electrónico e hice clic en el enlace para verificar si yo verdaderamente era un millonario después de todo. Casi instantáneamente, mi computadora se colgó, y con cada subsiguiente inicio se colgaba de nuevo.

Innumerables cuelgues y miles de correos electrónicos no deseados, más tarde, aprendí la lección de que sólo abriendo correos electrónicos no deseados puedo dañar mi computadora. Desafortunadamente existen trampas y errores que atraen a nuevos usuarios de correo electrónico.

En este artículo nos enfocamos en los 25 errores más comunes y fáciles de solucionar, que las personas cometen cuando se trata de seguridad de e-mail. Diseñamos este artículo con el nuevo usuario de Internet en mente, así que si Ud. es un experto de correo electrónico, puede pasar esto a todos sus amigos novatos.

Manejar correctamente sus cuentas de correo electrónico

1. Usar solamente una cuenta de correo electrónico

Los individuos nuevos de correo electrónico a menudo consideran su cuenta de correo electrónico como consideran su dirección domestica, solo tiene una dirección domestica, así que deben tener sólo un correo electrónico. En vez de eso, Ud. debe considerar su dirección de correo electrónico como considera sus llaves, mientras que puede estar bien usar la misma llave para su puerta de frente y posterior, tener una sola llave para las dos puertas es impractico e inseguro.

Un buen método práctico para el usuario de correo electrónico medio es mantener un mínimo de tres cuentas de correo electrónico. Su cuenta de trabajo debe ser usada exclusivamente para conversaciones relacionadas al trabajo. Su segunda cuenta de correo electrónico debe ser usada para conversaciones y contactos personales, y su tercera cuenta de correo electrónico deba ser usada como una captura general para cualquier comportamiento "peligroso". Esto significa que Ud. debe siempre suscribirse a boletines de noticias y concursos sólo con su tercera cuenta de correo electrónico. Similarmente, si Ud. tiene que informar su cuenta de correo electrónico en línea (mostrarla al público), tal como para su blog personal, Ud. debe usar sólo su tercer cuenta de correo electrónico.

Mientras que sus primera y segunda cuentas de correo electrónico pueden ser pagas o gratuitas, su tercera (captura-todo) cuenta siempre debe ser una cuenta gratuita tal como esas ofrecidas por Gmail o Yahoo!. Ud. debe planear vaciarla y/o cambiarla cada seis meses, ya que la "captura-todo" se convertirá en victima (y será spammeada)

cuando un dueño de boletín de noticias decida vender su nombre o un spammer robe esta dirección de un sitio Web público.

2. La posesión de cuentas con demasiado spam

Es simplemente una verdad de la vida que las cuentas de correo acumularán correos no deseados (de ahora en adelante "Spam") con el transcurso del tiempo. Esto es especialmente cierto cuando la cuenta que usa para suscribirse a boletines de noticias y que informa en línea es su cuenta principal (que como se manifestó anteriormente no se debe utilizar esta cuenta para estos fines). Cuando esto sucede, es mejor vaciar simplemente la cuenta de correo electrónico y empezar de nuevo. Desafortunadamente, sin embargo, muchos nuevos usuarios de correo electrónico se apegan mucho a sus cuentas de correo electrónico y en vez de comenzar de nuevo prefieren acumular docenas de Spam todos los días. Para evitar el problema, prepárese mentalmente para la idea que tendrá que vaciar/eliminar su cuenta "captura todo" cada seis meses.

3. No cerrar el Navegador después de desloguearse

Cuando está verificando su correo electrónico en una biblioteca o cybercafé, Ud. no solo necesita desloguearse de su correo electrónico cuando termine, también necesita asegurarse de cerrar la ventana del navegador completamente. Ciertos servicios de correo electrónico muestran su usuario (pero no su contraseña) aún después del deslogueo del sistema. Si bien el servicio hace esto para su conveniencia, también compromete la seguridad de su correo electrónico.

4. Olvidar borrar la cache del navegador, su historial y las contraseñas

Después de usar una terminal pública, es importante que recuerde borrar la cache del navegador, el historial de navegación y las contraseñas almacenadas. La mayor parte de los navegadores "recuerdan" de forma automática todas las páginas web que Ud. ha visitado (historial), y algunos "recuerdan" cualquier contraseña e información personal que Ud. haya ingresado a fin de ayudarle a completar formularios similares en el futuro.

Si esta información cae en malas manos, puede llevar a hurto de identidad, robo bancario y robo de información desde su cuenta correo electrónico. Ya que las amenazas son tan considerables, es importante que los nuevos usuarios de Internet tengan conciencia de cómo limpiar las caches de los navegadores de computadoras públicas, de modo que puedan borrar su información privada antes de que intrusos al acecho puedan conseguirla.

Para aquellos de Ud.es que usan Mozilla Firefox, simplemente pueden apretar CTRL+Shift+Del.

En Opera necesitan ir a herramientas >> borra datos privados.

Los usuarios de Microsoft Internet Explorer necesitan ir a herramientas >> Opciones de Internet y hacer click sobre "Eliminar Historial", "Eliminar Cookies" y luego "Borrar archivos Temporales".

5. Usar cuentas de correo electrónico no seguras para enviar y recibir información corporativa sensible

Las corporaciones grandes invierten cantidades enormes de dinero para asegurar que sus redes informáticas y correo electrónico permanezcan seguras. A pesar de sus esfuerzos, los empleados descuidados, que usan cuentas de correo personales para

conducir el negocio de la compañía y pasarse de uno a otro datos sensibles, pueden socavar las medidas de seguridad. Así que asegúrese de no arriesgar la seguridad de su compañía, y de su trabajo, por transmitir datos sensibles de la compañía vía su propia computadora personal o dirección de correo electrónico.

6. Olvidar la opción de Teléfono

Una de las lecciones más importantes sobre la seguridad de correo electrónico es que no importa cuantos pasos siga para asegurar su correo electrónico, el mismo nunca será completamente seguro de ataques. Esto nunca es más cierto que cuando usa una computadora pública. Así que a menos que necesite un registro escrito de algo o se esté comunicando a través del globo, considere que una llamada de teléfono puede ser una mejor opción que el correo. Mientras que una conversación de teléfono puede requerir unos cuantos minutos extras, cuando se compara con acceder al correo a través de una computadora pública, una llamada de teléfono es una opción mucho más segura y no deja un rastro de papel.

Enviar correo electrónico a la gente adecuada

7. No usar la opción copia de carbón oculta (BCC)

Cuando pone las direcciones de correo electrónico de una persona en el "BCC" ninguno de los receptores pueden ver las direcciones de los otros receptores de correo electrónico, mientras que si utiliza "CC", si se verán los destinatarios.

Nuevos usuarios de correo electrónico a menudo dependen demasiado del "TO" porque es la vía implícita de enviar correos electrónicos. Esto es correcto cuando Ud. está escribiendo para sólo una persona o unos cuantos miembros familiares. Pero si Ud. está enviando correo a un grupo diverso de personas, confundiendo "BCC" y "CC" aumenta seriamente aspectos de la privacidad y la seguridad. Solo hace falta un spammer para conseguir todos los correos electrónicos e inmediatamente todos en su lista serán spameados.

Aún si la honradez del grupo no esta en cuestión, muchos programas de correo electrónico son estructurados/programados para agregar de forma automática las direcciones de correo electrónico entrantes. Esto significa que ciertas personas en el grupo habrán añadido inadvertidamente la lista entera a su libreta de direcciones, y como consecuencia, si una de sus computadoras esta infectada con malware que silenciosamente envía spam, Ud. habrá sido la causa de que la lista entera sea spammeada.

8. Ser un clickeador contento del botón "contestar todo" o "Reply All"

A veces la equivocación no es al decidir entre CC: y BCC: sino entre clickear conteste todo en lugar de Contestar. Cuando clickea Contestar todo, su mensaje de correo electrónico es enviado para todos, incluyendo a todos los que estaban en el correo electrónico original, y si Ud. no pensaba incluirles, la información puede ser desastrosa desde la perspectiva de seguridad y de humillación personal:

Ejemplo 1 (Inglés): "un vendedor muy exitoso de nuestra compañía tuvo una gran libreta de direcciones llena de sus mejores clientes, incluyendo cierto gobierno muy importante y conservador. Con un sencillo clic, él, accidentalmente envió un archivo completo de sus caricaturas pornográficas favoritas y bromas a todos en su lista de clientes especiales. Sobra decir, está cerrando tratos para otra compañía estos días."

Ejemplo 2 (Inglés): "una mujer estaba atormentada por un romance roto. Ella escribió un mensaje largo y detallado a una novia, añadiendo que su ex novio prefería hombres a mujeres. Pero en lugar de contestar a un mensaje previo de su novia, ella clickeo contestar a todos. Su secreto se envió a docenas de personas que ella no conocía (incluyéndome), más el susodicho ex y su nuevo novio. Como si esto no fuera suficiente, hizo esto dos veces más.

9. El Spam a causa de reenviar correo electrónico

El reenviar correos puede ser una excelente vía para atraer a alguien rápidamente, sin tener que escribir algo muy extenso, pero si Ud. no es lo suficientemente cuidadoso, reenviando los correos electrónicos, puede crear una significativa amenaza a la seguridad para Ud. y los receptores del correo. Cuando un correo electrónico se reenvía, los receptores del correo (hasta ese punto) son de forma automática agregados al listado en el cuerpo del correo electrónico. Como la cadena permanece continuamente en movimiento, más y más receptores son agregados a la lista.

Desafortunadamente, si un spammer (o alguien que sólo esté mirando como hacer dinero rápido) puede hacerse con una gran cantidad de direcciones, puede vender la lista entera y todos empezarán a ser spameados. Sólo toma unos cuantos segundos borrar todos las direcciones de mail recibidas antes de reenviar una parte o su totalidad del correo, y ello puede evitar la situación terrible de que Ud. sea la causa de que todos sus amigos o compañeros de trabajo sean victimas del Spam.

Hacer los Backups y mantener una custodia.

10. Fracasar para hacer Backups de los correos electrónicos

Los correos electrónicos no son solo para conversaciones personales, también pueden ser para contactos legales, de contratos, decisiones financieras importantes y manejar juntas y reuniones profesionales. Tal como Ud. mantendría una copia de otros archivos empresariales y personales de mayor importancia, es importante que regularmente haga un backup de su correo electrónico para preservar un registro y no perder los sus datos (tal como le sucedió al mismo Gmail en diciembre de 2006).

Por suerte la mayoría de los proveedores de correo electrónico hacen esto simple, permitiéndole exportar correos electrónicos a una carpeta particular y luego puede crear una copia de la carpeta y almacenarla en un CD, DVD, disco desmontable, o cualquier otro tipo de medio. Si ese proceso exportador simple suena demasiado complicado, puede comprar un software de Backup automatizado que cuidará de todo esto por Ud.

Ya sea que Ud. compre el software o decida hacer un Backup manualmente, es importante que haga y siga un horario de soporte regular. Este es el tipo de cosa que los nuevos usuarios de correo electrónico tienden a dejar de lado. La frecuencia de los Backups necesaria dependerá por supuesto del uso de su correo electrónico, pero bajo ninguna circunstancia debe ser hecha menos frecuentemente que cada 3 meses.

11. Acceso móvil: Presumir la existencia de un Backup

El acceso móvil al correo electrónico, tal como Blackberry, ha revolucionado la vía que consideramos normal en el correo electrónico; y este ya no esta atado a una PC y puede verificarse de camino a cualquier parte. La mayor parte de los nuevos usuarios móviles simplemente asumen que una copia de los correos electrónicos que ellos verifican y borran de la Blackberry estará disponible en la computadora de su casa u

oficina.

Es importante tener presente, sin embargo, que algunos servidores de correo electrónico, descargan los correos electrónicos al dispositivo móvil y después los borran del servidor. Así, para ciertos dispositivos de acceso a correo electrónico móvil, si Ud. borra el mail del dispositivo, lo está borrando de su casilla.

Sólo tenga conciencia de las configuraciones estándares de su cliente de correo electrónico y asegúrese de que si Ud. quiere una copia del correo electrónico retenido, debe ajustar las configuraciones del cliente para hacer que ello suceda. Y preferiblemente asegúrese de esto antes que decida borrar un correo electrónico importante.

12. El pensamiento que un correo electrónico borrado ha dejado de existir para siempre

Todos hemos enviado un correo electrónico desconcertante o desafortunado y suspirado de alivio cuando se borraba finalmente, pensando que el episodio entero ha quedado detrás de nosotros. Vuelva a pensar. Sólo porque borra un mensaje de correo electrónico de su casilla y el remitente lo borro de su "casilla de mensajes enviados", no quiere decir que el correo electrónico se ha perdido para siempre. En realidad, los mensajes que son borrados a menudo todavía existen en carpetas suplementarias en servidores remotos durante años, y puede ser recuperado por hábiles profesionales.

Así que empiece a considerar lo que inserta en un correo electrónico como un documento permanente. Tenga cuidado acerca de lo que escribe, porque puede regresar para atormentarle muchos años después de que Ud. asumió que ha dejado de existir para siempre.

Evitar correo electrónico fraudulento

13. Creer que a ganado la lotería… y otros títulos

Los correos electrónicos no deseados usan una gran variedad de títulos inteligentes para conseguir que Ud. los abra. Nuevos usuarios de correo electrónico a menudo cometen el error de abrir estos correos electrónicos. Así en un esfuerzo para atraerlo, déjeme decir rápidamente:

- Ud. no a ganado la lotería irlandesa, la lotería de Yahoo, o ningún otro premio en efectivo grande.
- No existe ningún rey de Nigeria o príncipe tratando de enviarle $10 millones.
- Sus detalles de cuenta bancaria no necesitan ser reconfirmados inmediatamente.
- No tiene una herencia sin reclamar.
- Ud. nunca envió en realidad ese "correo retornado".
- Los correos electrónicos con los Titulares de Noticias no es alguien informándole sobre las noticias diarias.
- Ud. no a ganado un IPOD Nano.

14. No reconocer los ataques de phishing en el contenido del correo electrónico

Aún el más experimentado usuario de correo electrónico ocasionalmente abrirá accidentalmente un correo electrónico de phishing. En este punto, la clave para limitar el daño está en reconocer el correo electrónico de phishing por lo que es.

Phishing es un tipo de fraude en línea donde el remitente del correo electrónico prueba engañarlo y le solicita contraseñas personales o información de bancos. El remitente puede típicamente robar el logo de un banco muy conocido o PayPal (Inglés) y trata de diseñar el correo electrónico para parecerse al que vendría del banco. Normalmente el correo electrónico de phishing le invita a hacer click en un enlace a fin de confirmar su información de banco o contraseña, pero también puede invitarlo a contestar al correo electrónico con su información personal.

De cualquiera forma el intento de phishing, tiene como objetivo engañarle para ingresar su información en algo que parezca estar a salvo y seguro, pero en realidad es sólo un engaño que coloca el scammer. Si proporciona al phisher información personal, él usará la información para tratar de robar su identidad y su dinero.

Los signos del phishing incluyen:

- Un logo que parece distorsionado u estirado.
- Correo electrónico que se refiera a Ud. como "cliente estimado" o "usuario estimado" en lugar de incluir su nombre real.
- El correo electrónico que le advierte que una cuenta suya se cerrará a menos que reconfirme su información de facturación inmediatamente.
- Un acto procesal del correo electrónico amenazante.
- Correo electrónico que venga de una cuenta similar, pero diferente de una que la compañía real normalmente usa.
- Un correo electrónico que reclama "compromisos de seguridad" o "amenazas a la seguridad" y requiera efecto inmediato.

Si sospecha que un correo electrónico es un intento de phishing, la mejor defensa es nunca abrir el correo electrónico en primer lugar. Pero asumiendo que Ud. lo ha abierto ya, no conteste o no haga clic en el enlace en el correo electrónico. Si Ud. quiere verificar el mensaje, teclee manualmente en el URL de la compañía en su Navegador en lugar de hacer clic en el enlace insertado.

15. Transmisión de información financiera o personal a través del correo electrónico

Bancos y tiendas en línea proporcionan, casi sin excepción, una sección asegurada en su sitio Web donde puede entrar su información personal y financiera. Ellos hacen esto precisamente porque el correo electrónico, por muy bien que protegido que sea, es violado más fácilmente que los sitios bien asegurados. Por lo tanto, Ud. debe evitar escribir a su banco por la vía de correo electrónico y considere cualquiera tienda en línea que le envié la información privada por correo electrónico como sospechosa.

Esta misma regla de evitar poner información financiera en correos electrónicos a negocios en línea sirve también para correos electrónicos personales. Si, por ejemplo, necesita dar su información sobre la tarjeta de crédito a su hijo estudiante en la universidad, es mucho más seguro hacerlo por el teléfono que por la vía de correo electrónico.

16. Eliminarme de la suscripción a boletines de noticias que nunca pedí

Una técnica común usada por correos electrónicos no deseados es enviar miles de boletines de noticias falsos de organizaciones con un vínculo "Remover del Boletín" o "Unsubscribe" en la parte inferior del boletín de noticias. Los usuarios de Mail que

ingresan su correo electrónico en ese link de la supuesta lista serán víctimas de un montón de Spam. Así si Ud. no recuerda específicamente haberse subscrito al boletín de noticias, es mejor poner en lista negra la dirección de correo electrónico, antes que ir detrás el enlace y posiblemente recogiendo un Troyano o, sin saberlo, anotarse para recibir más Spam.

Evitar el malware

17. Confiar en sus amigos el correo electrónico

La mayor parte de los nuevos usuarios de Internet son muy cuidadosos cuando se trata de correos electrónicos de remitentes que no reconocen. Pero cuando un amigo envía un correo electrónico, toda la cautela se va por la ventana y asumen que están a salvo porque saben que el remitente no desea ni piensa causarles daños. La verdad es que es tan o más probable que un correo electrónico de un amigo contenga un virus o malware como uno de un extraño. La razón es que la mayor parte del malware es circulado por las personas que no tienen ninguna idea de que están enviándolo, porque los intrusos usan su computadora como un zombi.

Es importante mantener actualizado el software antivirus y el scanner de mail, y usarlo para que escanee todos los correos electrónicos entrantes.

18. Borrar correos electrónicos no deseados en lugar de ponerlos en lista negra

Una lista negra de correo electrónico es la lista de las cuentas de correo electrónico que son rotuladas como los correos electrónicos no deseados. Cuando agrega un remitente a la "lista negra", Ud. está diciendo a su cliente de correo electrónico que desconfía de este remitente particular y que empiece a asumir que son correos electrónicos no deseados (spam).

Desafortunadamente, nuevos usuarios de Internet son a menudo tímidos para usar la lista negra en su cliente de correo electrónico, y en vez de eso sólo borran los correos electrónicos no deseados. Mientras que cada correo electrónico no deseado no es del mismo remitente, una cantidad sorprendente de ellos sí lo es. Así ingresando esos remitentes en la lista negra en lugar de borrarlos, Ud. puede, en el transcurso de unos cuantos meses, limitar drásticamente la cantidad de correos electrónicos no deseados que llega a su casilla.

19. Inhabilitar los filtros de correo electrónico de deseado

Nuevos usuarios de correo electrónico típicamente no reciben una gran cantidad de correos electrónicos no deseados en su cuenta de correo y así no valoran la ayuda que un filtro de correos electrónicos no deseados puede proporcionar al comienzo de su uso. Ningún filtro de correos electrónicos no deseados es perfecto e, inicialmente, tener que identificar el spam del correo real buscando correos electrónicos mal bloqueados lleva a muchos nuevos usuarios a inhabilitar sus filtros de spam.

Sin embargo, cuando una cuenta de correo electrónico se va haciendo "vieja" tiende a recibir más spam y, sin los filtros, puede volverse rápidamente difícil de manejar. Así en lugar de inhabilitar su filtro, los nuevos usuarios de Internet deben tomarse el tiempo de agregar los mails de amigos que consiguen atrapar en el filtro de correos electrónicos no deseados a la whitelist (lista blanca). Entonces, cuando los niveles de mails no deseados empiece a aumentar, la cuenta de correo permanecerá útil y menos correo deseado será atrapado en el filtro.

20. Suspender el escaneo de archivos adjuntos

Nueve de cada diez virus que infectan una computadora llegan a través de un adjunto en algún mail. Sin embargo a pesar de esta relación, mucha gente todavía no escanea toda la entrada de adjuntos. Cuando vemos un correo electrónico con adjunto de alguien que nosotros conocemos, asumimos que el correo y su adjunto están a salvo. Por supuesto esa suposición no tiene razón, ya que la mayoría de los virus por correo electrónico son enviados por "zombis" que han infectado una computadora causando el envió del virus sin que el dueño (su amigo) lo sepa.

Lo que hace este descuido aún más escandaloso es el hecho que varios clientes de correo electrónico libres proporcionan un scanner de adjuntos de correo electrónico incorporado. Por ejemplo, si usa Gmail o Yahoo! para su correo electrónico, cada mail y adjunto que Ud. envía o reciba son escaneados de forma automática.

Si Ud. no quiere hacer una inversión en un scanner de terceras partes y su proveedor de correo electrónico no proporciona el escaneo de adjuntos incorporado, Ud. puede acceder a sus adjuntos por un proveedor de correo electrónico que ofrece examinadores de virus gratuito primero remitiendo archivos a esa cuenta antes de abrirlos.

Mantener los intrusos a raya

21. Compartir su información de cuenta con otros

Todos lo hemos hecho: necesitamos una comprobación de mail urgente, llamamos a nuestro cónyuge o amigo y le pedimos verificar nuestro correo electrónico. Por supuesto, confiamos en estas personas, pero una vez la contraseña es conocida por alguien aparte de Ud., su cuenta no es tan segura como solía serlo.

El problema real es que quizás su amigo no use las mismas medidas de seguridad que Ud. Él podría estar accediendo a su correo electrónico por una cuenta inalámbrica sin garantía, quizás no mantenga su antivirus actualizado, o podría infectarse con un keylogger que roba de forma automática su contraseña una vez que la ingresa.

Así, asegúrese que Ud. es la única persona que sabe su información de acceso personal, y si Ud. la escribe en algún lado, asegúrese de hacerlo de tal manera que los extraños no sean capaces de comprender fácilmente lo que están mirando, si sucede que encuentran sus notas.

22. Usando las contraseñas simples y fáciles de suponer

Los intrusos usan software que buscan nombres comunes para armar posibles nombres de usuario y cuentas validas de correo electrónico. Cuando Ud. abre un spam, un trozo de código en el mail envía un mensaje de vuelta al intruso dejándole saber que la cuenta es válida, y entonces ahora tratarán de suponer su contraseña.

Los intrusos a menudo también crean programas que pasan por un ciclo de palabras comunes y combinaciones de números a fin de tratar de adivinar una contraseña. En consecuencia, las contraseñas que consisten de una palabra sencilla, un nombre, o una fecha son frecuentemente "adivinadas" por los intrusos. Así al crear una contraseña use números poco comunes y combinaciones de letras que no forman una palabra que se puedan encontrar en un diccionario. Una contraseña segura (Inglés) debe tener un mínimo de ocho caracteres, tan sin sentido como sea posible, así como usar letras en mayúsculas y en minúsculas. Crear una contraseña segura significa que el programa de computadora del intruso tendrá que desplazarse por millones de ellas antes de

adivinar la contraseña, y en ese caso la mayor parte de los intrusos simplemente se darán por vencidos.

También puede ver como crear contraseñas en este artículo.

23. No cifrar sus correos electrónicos importantes

No importa cuantos recaudos tome para minimizar las chances de que su correo este controlado por intrusos, siempre debe asumir que alguna otra persona está mirando cualquier cosa que entre y salga de su computadora. Dado esta suposición, es importante cifrar sus correos para asegurarse de que si alguien está controlando su cuenta, al menos no pueden comprender lo que está hablando.

Existen algunos servicios de encriptación que están a la vanguardia del mercado para aquellos que cuentan con un gran presupuesto, pero si Ud. es nuevo en el uso de correo y sólo quiere una solución simple, barata y utilizable, puede seguir estas instrucciones de 20 minutos paso por paso (Inglés) para instalar PGP o GPG (libre y gratuito), la forma más común de cifrado para email.

Cifrar todo su correo electrónico puede ser poco práctico, pero ciertos correos son demasiado sensitivos ser enviados libremente, y para esos correos electrónicos, PGP o GPG es un paso importante para su de seguridad.

Puede leer estos artículos en castellano para cifrar sus correos:

http://www.segu-info.com.ar/articulos/articulo9.htm

http://www.segu-info.com.ar/articulos/articulo11.htm

http://www.segu-info.com.ar/articulos/articulo13.htm

http://www.segu-info.com.ar/articulos/articulo50.htm

http://www.segu-info.com.ar/articulos/articulo53.htm

http://www.segu-info.com.ar/articulos/articulo56.htm

24. No cifrar su conexión inalámbrica

Al cifrar sus correos electrónicos importantes hace las cosas difíciles a los intrusos que tienen acceso a su correo electrónico para comprender lo que dice, pero uno de los puntos más vulnerables en el viaje de los mails es el punto entre su ordenador portátil y el Router inalámbrico que usa para conectarse a Internet.

Por lo tanto, es importante que cifre su red de Wi-Fi con la norma de codificación WPA2 si es posible (o bien con WEP o WPA). El proceso es relativamente simple y directo, aún para un usuario novato de Internet, y los quince minutos que toma son de gran valor para la seguridad de su correo electrónico.

25. La falta de uso firmas digitales

La ley ahora reconoce correo electrónico como una forma importante de comunicación para emprenden grandes negocios como el firmado de un contrato o un acuerdo financiero. Mientras que la habilidad para mantener estos contratos en línea ha hecho nuestra vida más fácil, ello ha creado también la necesidad de alguien para acceder a sus correos electrónicos para conocer sus acuerdos y utilizarlo en su beneficio.

Una vía para combatir la falsificación de correo electrónico es usar una firma digital

siempre que firma un correo electrónico importante. Una firma digital ayudará a probar que y de cual computadora/usuario procede un correo electrónico, y que el correo electrónico no se ha alterado en el camino.

Al establecer el hábito de usar una firma de correo electrónico siempre que firma mails importantes, Ud. no solo hará más difícil a la otra parte modificar sus correos, sino que también le dará la credibilidad extra cuando alguien trate de reclamar algo por Ud.

Para una impresión rápida en firmas digitales, puede leer YoudZone (Ingles) y los artículos de Wikipedia (Inglés) del asunto.

También puede leer en castellano los artículos mencionados en el punto 23 para aprender a firmar sus correos.

Conclusión

Este artículo ha sido desarrollado para proporcionarle la información básica que Ud. necesita para evitar muchos de los errores comunes de seguridad en el correo electrónico que cometen los usuarios nuevos.

Ningún artículo sencillo puede cubrir aún las bases de la seguridad en el correo pero, evitando los 25 errores comunes listados en este artículo, hará una gran diferencia mejorando la seguridad de su computadora, su información personal, y sus correos electrónicos.