Boletín Informativo

TIC SSM

N°2

Servicio de Salud Magallanes

Región de Magallanes

Ministerio de Salud

Tegnologías de la Información y Comunicación
Servicio de Salud Magallanes
Ministerio de Salud

Seguridad de la Información

Uso seguro del correo electrónico

Tegnologías de la Información y Comunicación
Servicio de Salud Magallanes
Ministerio de Salud

Servicio de Salud Magallanes
Región de Magallanes
Ministerio de Salud

En la actualidad, las amenazas más habituales asociadas al uso del correo electrónico son las siguientes:

•**SPAM:** Es un conjunto de mensajes publicitarios que son enviados de forma masiva a un número grande de usuarios al mismo tiempo, sin ser solicitados y que perjudican con el resto de mensajes recibidos.

•**Phishing:** Consiste en un método fraudulento de capturar información sensible, como nuestros números y claves de cuentas bancarias o de tarjetas de crédito. Se nos intenta engañar con mensajes que aparentan ser mensajes oficiales de entidades financieras o empresas de nuestra confianza.

•**Estafas de todo tipo:** Donde se nos intenta vender productos falsos o inexistentes, se nos solicita dinero aludiendo a buenas causas, ofertas de trabajo inexistentes, etc.

•**Correos con archivos adjuntos maliciosos:** Actualmente es una de los peligros más extendidos. Recibimos un mensaje de un remitente no necesariamente desconocido ya que puede estar falsificado con un archivo adjunto que nos invita a abrirlo. Dicho fichero contiene código malicioso que, si no disponemos de software antivirus o antimalware adecuado, infecta nuestro equipo, con consecuencias diversas. Muchos de estos ficheros infectados a menudo utilizan la libreta de direcciones de nuestro cliente de correo para renviarse a su vez a todos nuestros contactos.

•**Cadenas de mensajes falsos:** Generalmente se trata de mensajes variados acerca de hechos o falsas alarmas de cualquier tipo, en los que se nos pide que reenviemos y difundamos el mensaje entre nuestros conocidos. El problema de las cadenas de mensajes falsos es el volumen de correos electrónicos que crea de forma progresiva.

Un buen consejo práctico es mantener varias cuentas de correo electrónico para diferentes usos. Se recomienda usar dos o tres cuentas de correo diferentes: una para el trabajo, otra para uso personal y una tercera para suscripciones y recepción de información.

La cuenta o correo institucional debe ser usada exclusivamente para temas relacionados con el trabajo. La segunda cuenta de correo electrónico debe ser usada para conversaciones con nuestros contactos personales, y la tercera cuenta de correo electrónico deba ser usada para ser expuesta en Internet, usándola para suscripciones a boletines de noticias y demás fuentes de información, sin problema de que nos la puedan capturar.

Igualmente, si tenemos que proporcionar nuestra cuenta de correo electrónico en algún sitio de Internet, debemos usar esta tercera cuenta de correo electrónico. Probablemente, será en esta tercera cuenta donde recibiremos la mayor parte del SPAM o correo sospechoso, pero las demás las tendremos más protegidas.

Aprende a reconocer los fraudes por correo electrónico. Los correos electrónicos no deseados usan una gran variedad de títulos atractivos para conseguir que el destinatario los abra. Muchos usuarios a menudo cometen el error de abrir estos correos electrónicos, abrir o ejecutar un adjunto malicioso o hacer clic en un link incluido en el propio mensaje.

Ten especial cuidado en no abrirlos y elimine directamente aquellos correos en los que:

•Nos informen de que hemos ganado en cualquier tipo de lotería o sorteo o que vamos a recibir cualquier tipo de premio.

•Correos en los que nos informan de reyes o príncipes de Nigeria tratando de enviarnos una enorme cantidad de dinero.

•Los detalles de ninguna cuenta bancaria en ningún caso necesitan ser reconfirmados inmediatamente.

•Si nos informan de algún tipo de herencia sin reclamar.

•Si nos indican que hemos ganado cualquier tipo de dispositivo electrónico o nos informan de alguna oferta sospechosa.

•Cualquier otro tipo de correo que nos resulte altamente sospechoso y que provenga de remitentes que no conocemos.

Servicio de Salud Magallanes
Región de Magallanes
Ministerio de Salud

Otras consideraciones

Nunca abras ningún mensaje ni fichero adjunto de un remitente que desconozcas o que te resulte sospechoso.

Elimina directamente este tipo de mensajes. Una buena práctica si no estamos seguros es contactar con la persona que lo envía, para ver si realmente lo ha enviado. Si al abrir un mensaje automáticamente nos aparece alguna ventana o se nos redirige a una página web donde se nos pide que instalemos algo, cierra la ventana automáticamente y elimina el mensaje de correo electrónico.

No uses contraseñas simples y fáciles de adivinar. Los intrusos usan software que buscan nombres comunes para generar posibles nombres de usuario y cuentas validas de correo electrónico. Cuando abrimos un SPAM, en muchos casos se envía un mensaje de vuelta al intruso indicándole que la cuenta es válida, por lo que el siguiente paso es tratar de adivinar su contraseña.