Aprende a Identificar un Correo Fraudulento o Phishing

A medida que los usuarios toman más precauciones sobre los fraudes en la Internet, los cibercriminales se vuelven más astutos y creativos para atraer nuevas víctimas. Un buen ejemplo de esto son los llamados correos fraudulentos o «Phishing» (tambien llamados: «carding» o «spoofing»). Los cibercriminales ya no solo recurren a enviarte correos donde te notifican que eres el feliz ganador de un jugoso premio de la lotería de Lituania ni que alguien de la realeza Africana necesita de tu ayuda.

Ahora estos correos son más elaborados y en muchos casos imitan de manera casi exacta los enviados por las entidades o personas reales. A continuación listare una serie de características que ayudarán a identificar correos fraudulentos:

Te solicitan información personal

Este el el principal objetivo de un correo electrónico de phishing. En la actualidad ninguna empresa seria te solicitará que le envíes información personal o sensible por correo electrónico (a no ser que tu hayas iniciado algún proceso que requiera confirmar algún dato).

En este tipo de correos se te ofrecerá un enlace para que ingreses desde ahí la información personal que te solicitan, una práctica sana y recomendable es abrir una nueva ventana del navegador e ingresar a la página del solicitante y verifiques ahí si realmente se requiere realizar la acción que se te solicita.

Enlaces

Los enlaces son presentados de tal forma que parecen muy auténticos. Estos enmascaran, detrás de un texto conocido y relacionado con el remitente, enlaces hacia la página del cibercriminal donde te pueden infectar con algún virus para hacerse de tu información o te presentan una pagina casi idéntica a la del remitente solicitandote ingresar ciertos datos para continuar.

El texto del enlace te mostrará un nombre amigable para no levantar sospechas, pero no garantiza que te llevara a donde el texto te indica. Verifica siempre hacia donde dirige el enlace antes de hacer clic sobre el, posiciona el puntero del mouse sobre el enlace y mira en la parte inferior del navegador, ahí se debe mostrar el enlace completo hacia donde te redirigira.

Contenido

Están redactados pensando en crear un sentido de urgencia a hacer clic en los enlaces que contiene. Te animan a hacerlo incluyendo frases como: se detectó actividad sospechosa en tu cuenta, tu cuenta está a punto de ser eliminada, tu cuenta debe ser actualizada, acciones que saben pueden ser enviados por los servicios que están suplantando y requieren tu verificación, entre otros similares.

El destinatario del correo no es acorde con la dirección de origen

Averiguar de quién procede realmente el correo, la forma más sencilla de averiguarlo es verificar el dominio desde donde viene dirigido el correo. Por lo general son enviados

desde servicios de correo gratuitos como Hotmail, Gmail, Outlook, etc.

Los más profesionales pueden tener un dominio personalizado (de pago) pero con un nombre muy similar al del servicio que quieren suplantar, un ejemplo puede ser un correo enviado supuestamente por Deezer sería mail@dezer.com, que aunque se ve muy legítimo de Deezer no lo es Nota que en el anterior ejemplo suprimieron una letra “e” en el nombre del dominio para que fuera diferente al original pero se sigue viendo muy parecido.

Remitido a muchos pero dirigido a una sola persona

Si te das cuenta en los campos Para, CC o CCO del mensaje va dirigido a muchas personas, por lo general cuentas que ni conoces, pero en el cuerpo del mensaje habla en singular: Querido Amigo, Estimado Cliente, Señor Usuario, entre otras más.

En ocasiones puede haber sido enviado solo a ti pero notaras que no se dirigen por tu nombre, el que pudiste haber usado para registrarte, sino que usan el nombre de tu cuenta, por ejemplo: Estimado carlos.andres.123.

Suelen también enviarlos a cuentas de correos similares utilizando posibles variaciones de tu nombre y apellido, que para Carlos Ardila pudieran ser: carlos.ardila, cardila, carlosardila, etc y entre todas ellas una coincide con tu dirección de correo electrónico.

Gramatica y Ortografia

Las empresas se cuidan mucho al redactar su comunicados tratando de cometer cero errores gramaticales y ortográficos, por lo que una señal de que un correo puede

tratarse de una suplantación es encontrar errores de estos

Uso de mayúsculas y signos de exclamación suelen ser comunes en este tipo de mensajes, expresando emoción desbordante para atraer tu atención.

También suelen cometer errores ortográficos para ocultar palabras que los filtros antispam pudieran detectar. Por ejemplo Vi@gra.

La regla general es no enviar nunca información personal, siempre desconfiar un poco, ser precavido. Recordar que, como se dice por acá en Colombia, “De eso tan bueno no dan tanto”.

Ver también:¿Ya eres un ninja en Gmail ?; ¿Qué hace tan popular a gmail? Usar password Sniffer para capturar datos de email, inicios de sesión FTP y web