GUÍA DE SEGURIDAD EN EL USO DE ACTIVOS INFORMÁTICOS

1. ¿Qué es Spam?

"El spam (en inglés, correo basura) son los mensajes no solicitados, principalmente de tipo publicitario, y enviados de forma masiva. La forma de envío más utilizada es el correo electrónico, puede presentarse por programas de mensajería instantánea (mensajes de texto, whatsapp, etc) o redes sociales."

También pueden ser correos o mensajes maliciosos o fraudulentos. El objetivo principal de estos es conseguir información sensible del destinatario, como datos de acceso de cuenta de correo para propagar más spam, datos de una cuenta bancaria o de una tarjeta. En otros casos se trata, directamente, de estafas o timos por vía digital.

2. *¿Cómo detectarlo?*

Los correos spam pueden llegar de una cuenta con dominio desconocido o parecer que proceden del mismo dominio siempre con la finalidad de robo de información, las características principales:

Contienen palabras como “Urgente”, “Da clic en el siguiente enlace/liga/link”, “para recuperar cuenta/contraseña/espacio en buzón”, “Para recuperar su cuenta deposite XXXX”, “Descargue el siguiente archivo/Factura/guia de envío”, etc., Tal cual se muestra en los siguientes ejemplos:

GUÍA DE SEGURIDAD EN EL USO DE ACTIVOS INFORMÁTICOS

Subject: Cómo estás tú y tu familia

Saludos de la señora Clara Belizaire

Mi nombre es la Sra. Clara Belizaire, nacida el 15 de julio de 1965, originaria de Francia, me diagnosticaron cáncer de esófago. Se ha contaminado toda forma de tratamiento médico, y en este momento solo tengo unos pocos meses de vida, según expertos médicos

En particular, no he vivido mi vida tan bien, ya que realmente nunca me importó nadie (ni siquiera yo) sino las compañías de mi difunto esposo. Aunque yo y mi difunto esposo (Jean-Pierre Belizaire) somos muy ricos, nunca fui generoso, siempre fui hostil con las personas y solo me enfoqué en nuestras compañías, ya que eso era lo único que me importaba. Pero ahora me arrepiento de todo esto porque sé que hay más en la vida que solo querer tener o ganar todo el dinero del mundo.

Estuvimos casados durante 18 años con una hija (IRENE) que luego murió en un accidente automovilístico. Antes de la prematura muerte de mi esposo, ambos somos buenos cristianos. Y desde después de su muerte, había decidido no volver a casarme o tener un hijo fuera de mi casa matrimonial. Le escribo para informarle de mi intención de usar mi dinero (US $ 800,000.00 dólares estadounidenses) para obras de caridad en su país.

No quiero que el banco / gobierno corrupto tenga mi dinero si no hago que la operación tenga éxito, mi salud está en Dios.
Si pudieras ayudarme fielmente y usar mi dinero para cuidar a los pobres y menos privilegios, contéstame pronto para obtener más detalles sobre mi intención.

Sra. Clara Belizaire

Santander

Estimado (a) Cliente ,

Su tarjeta ha sido bloqeuada !

Fecha : 15/06/2020

Motivo : Actividades inusuales.

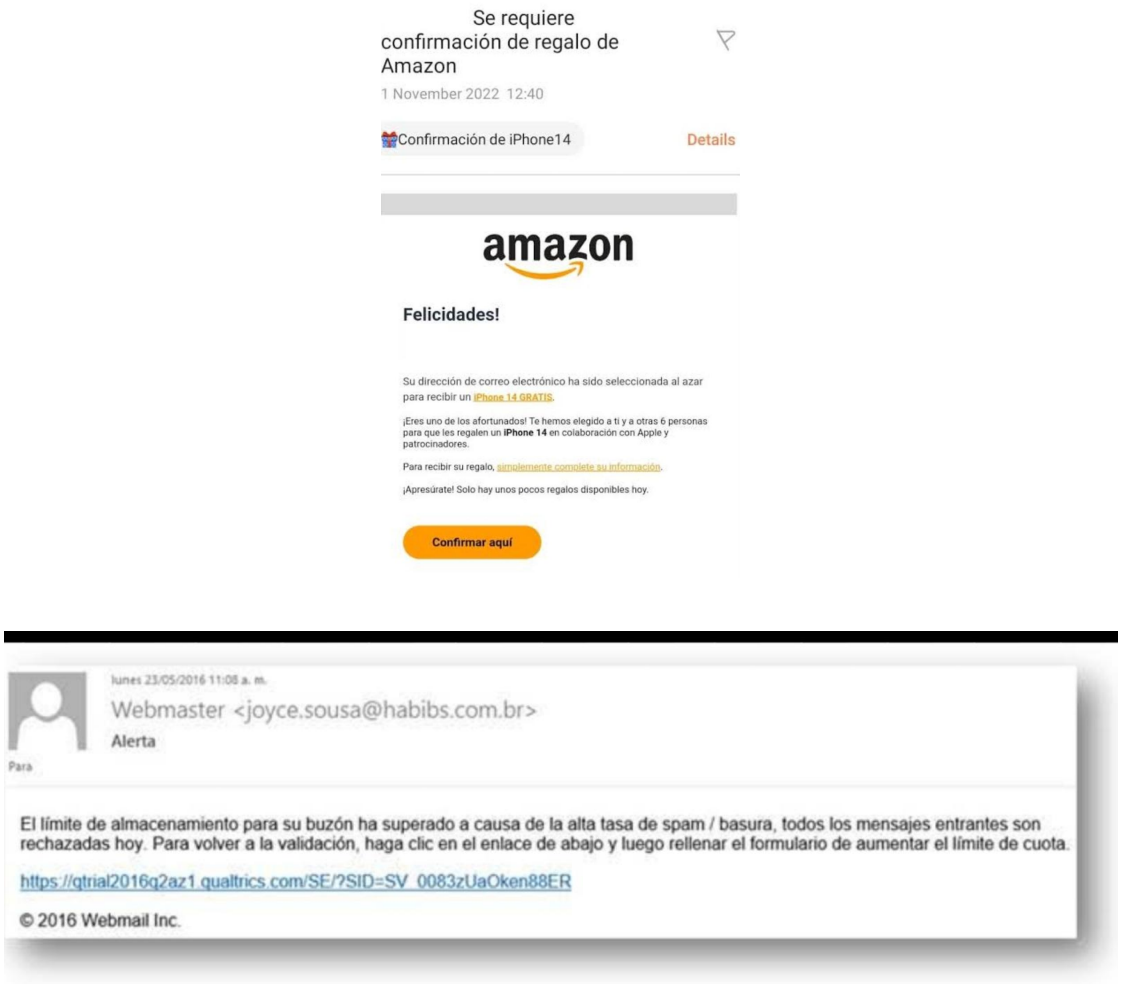
Puede desbloquear su tarjeta haciendo clic en el

siguiente enlace y siguiendo todos los pasos de verificacion.

Verificar y activar mi tarjeta

Gracias.

Grupo Santander 2020.



Pueden contener archivos encriptados en .zip, .rar, o .exe (son los más peligrosos), documentos disfrazados de word o excel que terminan siendo ejecutables los cuales al abrirlos tienen scripts para robar información.

NOTA: Al dar clic o descargar un archivo de dudosa procedencia, los delincuentes cibernéticos pueden obtener contraseñas y control total de la cuenta y en su caso hasta del equipo de cómputo completo, y comienzan a enviar y distribuir spam desde una cuenta legal robando información de más cuentas.

3. Consecuencias de enviar spam

GUÍA DE SEGURIDAD EN EL USO DE ACTIVOS INFORMÁTICOS

1.- Todo el dominio o subdominios se ven comprometidos por lo que las empresas o dependencias nos colocan con mala reputación y genera desconfianza.

2.- Se empieza a colocar el dominio en listas negras evitando la correcta recepción de correos fidedignos.

3.- No solo una dependencia se ve afectada, si no que todas las dependencias dependientes, en este caso, el dominio completo CDMX se ve afectado, dañando la reputación de diversas cuentas de servidores públicos.

4. *¿Cómo evitar que mi cuenta se vea comprometida?*

1.- Utiliza contraseñas seguras para todas las cuentas (con una extensión de al menos 12 caracteres),que no incluya palabras del diccionario, pero sí caracteres especiales (“@”, “.”,”#”, "$","% ","& ", etc.), mayúsculas, minúsculas y números. Los atacantes podrían forzar con facilidad las contraseñas simples, puede utilizar un gestor de contraseñas para crear contraseñas únicas y garantizar la privacidad de la identidad digital.

2.- Generar una contraseña única para cada cuenta. Si se reutilizan las contraseñas, la filtración en un servicio podría acabar por comprometer al resto.

3.- Mantener las contraseñas en secreto, sin excepción. No escribirlas, guardarlas en un archivo ni compartirlas con compañeros. Cualquier visitante o ex empleado resentido podría utilizar la contraseña para perjudicar a la dependencia, por mencionar lo más obvio, pero las posibilidades son prácticamente ilimitadas.

4.- Revisar minuciosamente los enlaces en correos electrónicos antes de acceder a ellos, un nombre de remitente convincente no garantiza su autenticidad. Uno de los muchos trucos que los ciberdelincuentes utilizan para que los usuarios hagan clic en sus enlaces de phishing es que personalizan los mensajes de acuerdo con la dependencia o incluso utilizan la cuenta comprometida de algún compañero.

5.- Nunca transfiera dinero a cuentas desconocidas basándose exclusivamente en un correo electrónico o mensaje directo. En su lugar, póngase en contacto con la persona que supuestamente ha autorizado la transferencia para confirmar la petición.

6.- No conectar medios de almacenamiento desconocidos al equipo de computo. Los ataques mediante unidades de memoria USB infectadas no solo aparecen en la ciencia ficción, los ciberdelincuentes ya han utilizado esta técnica con dispositivos maliciosos en lugares públicos y oficinas.

7.- Antes de abrir un archivo, compruebe que no sea ejecutable (con frecuencia los atacantes disfrazan los archivos maliciosos como documentos de oficina). No abra o ejecute archivos ejecutables de fuentes en las que no confíe, piense dos veces antes de dar clic en cualquier lugar debe ser consciente de dónde hace clic, especialmente en los enlaces o archivos adjuntos de los mensajes sms o emails. También revise que las

páginas que consulta tengan un certificado de seguridad válido para asegurarse de que la información que recibe de internet es segura.

8.- Borre las cookies de los principales navegadores web. Las cookies pueden representar un riesgo para la privacidad debido a la cantidad de información que pueden contener, como identificación personal para ayudar a completar formularios automáticamente en los navegadores. Si prefiere proteger su privacidad cuando se trata de cookies, es posible que desee eliminarlas.

9.- Ejecutar análisis completos de antivirus periódicamente.

10.- Mantener su equipo de cómputo y dispositivos móviles con las últimas actualizaciones del sistema, así como activar el antivirus y firewall en todos sus dispositivos y los cercanos.

5. *Responsabilidades del usuario en el uso del correo electrónico institucional*

1.- El correcto uso de la cuenta de correo la cual debe tener fines únicamente laborales e institucionales.

2.- Reportar cualquier anomalía o correo sospechoso (correos basura o spam),o aquellos que considere dañinos o sospechosos a su enlace para que a su vez sea canalizado a la mesa de servicios o directamente a la cuenta: mesadeservicio@cdmx.gob.mx.

3.-Evitar la descarga y ejecución de archivos adjuntos, responder correos de dudosa procedencia o dar clic en ligas/enlaces de origen desconocido o dudoso en los mensajes de correo electrónico.

4.- Evitar difundir contraseñas o compartir su cuenta con diferentes personas.

5.-Escanear todos los archivos adjuntos en los mensajes de correo electrónico que envíe o reciba utilizando el correo institucional.
6.-Realizar respaldos periódicos de la información contenida en su cuenta.

7.-Acceder al servicio de correo electrónico de forma constante no excediendo los 80 días hábiles.

8.-Cambiar su contraseña de forma periódica asignando una contraseña segura con un mínimo de 12 dígitos que incluya Mayúsculas, minúsculas, números y carácteres especiales, si le es posible active la autenticación multifactor (MFA), para que sea obligatorio identificarse a través de varios pasos de verificación y credenciales para poder acceder a datos..

9.- Minimizar la información personal y laboral que expone en sus redes sociales;

GUÍA DE SEGURIDAD EN EL USO DE ACTIVOS INFORMÁTICOS