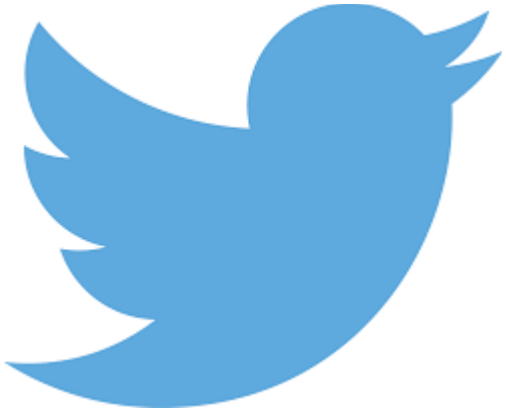
VenCERT

PREVENIMOS Y GESTIONAMOS
LOS INCIDENTES CIBERNÉTICOS

Recomendaciones de Seguridad Red Social Twitter



Av. Andrés Bello, Torre BFC, Piso 13, Sector Guaicaipuro, Caracas – Venezuela
Tlfs. +58 212 5785674 – Fax +58 212 5724932 . http://www.vencert.gob.ve

Medidas de seguridad para Twitter

Tras varios ataques a cuentas de reconocidas empresas, Twitter anunció nuevas medidas de seguridad. Cualquier usuario que tenga un email y número de teléfono verificado puede habilitar desde Configuración el inicio de sesión en dos pasos. De esta manera, cada vez que se ingrese a la red social se deberá cargar también un número de identificación de seis dígitos que será enviado por SMS.

Twitter nunca envía correos que pidan tu contraseña o que descargues archivos. Nunca debes escribir tu contraseña en una pantalla web que no sea de Twitter, o una aplicación en la que confíes. Siempre puedes asegurarte de que estás en Twitter fijándote en la dirección en la barra de URLs de tu navegador, para asegurarte de que el dominio es Twitter.com.

- **Recomendaciones generales para proteger Su cuenta**

1. Utilice una contraseña segura, la misma debe ser fuerte y única, Además de crear una cuenta de contraseña segura Twitter, también debe hacer lo mismo con su dirección de correo electrónico asociada con su cuenta de Twitter.
2. Utilice la verificación de inicio de sesión.
3. Tenga cuidado con los enlaces sospechosos, y siempre asegurarse de que está en Twitter.com antes de ingresar su información de acceso.ç
4. Nunca le dé su nombre de usuario y contraseña a terceros no confiables, especialmente aquellos que promete conseguirle seguidores o hacer dinero.
5. Asegúrese de que su ordenador y su sistema operativo está actualizado con los más recientes parches, actualizaciones y software anti-virus.
6. Estamos trabajando para mejorar nuestras respuestas a las amenazas a la seguridad, pero las cuentas de usuarios y computadoras a veces puede llegar a ser comprometida por phishing, hacks o virus. Si crees que tu cuenta ha sido comprometida, por favor visite nuestra página de ayuda para cuentas comprometidas para averiguar cómo solucionarlo rápidamente.

Que hacer:

1. No crear una contraseña de al menos 10 caracteres de longitud. Al crear la contraseña esta debe ser fuerte con al menos 10 caracteres y una combinación de letras, números y símbolos para tu cuenta de Twitter. Usa una contraseña única para cada uno de los sitios web que usas (email, banca electrónica etc). De esta forma si una cuenta es comprometida, las otras estarán seguras. Una cuenta de correo electrónico comprometida es la segunda forma más común en

la que un intruso puede ganar acceso a tu cuenta de Twitter.

2. No utilice una contraseña diferente para cada sitio web que visite.
3. Mantenga su contraseña en un lugar seguro. Considere el uso de software de gestión de contraseñas para almacenar toda su información de inicio de sesión de forma segura.

Qué no hacer:

1. No utilice información personal de su contraseña como números de teléfono, cumpleaños, etc.
2. No utilice palabras comunes del diccionario como "contraseña", "iloveyou", etc.
3. No utilice secuencias tales como "abcd1234", o secuencias de teclado como "QWERTY".
4. No vuelva a usar las contraseñas a través de sitios web. Su contraseña de la cuenta de Twitter debe ser único a Twitter.
5. Además, puede seleccionar "Requerir información personal para restablecer mi contraseña" en la configuración de seguridad y privacidad. Si marca esta casilla, se le pedirá que introduzca su dirección de correo electrónico o número de teléfono para restablecer su contraseña si alguna vez olvida.

- **Compromiso con tu cuenta Twitter**

1. Verificación Usar inicio de sesión
2. Verificación de inicio de sesión es una característica que le ayuda a mantener su cuenta más segura. En lugar de depender sólo de una contraseña, la verificación de inicio de sesión introduce una segunda comprobación para asegurarse de que usted y sólo usted puede acceder a su cuenta de Twitter. Sólo las personas que tienen acceso a la contraseña y el teléfono será capaz de acceder a su cuenta.
3. Asegúrese de que está en Twitter.com antes de iniciar sesión, Compruebe siempre que estás en twitter.com antes de iniciar, ya que puede ser victima de un phishing y el mismo obtendra su nombre de usuario y contraseña de Twitter o correo electrónico, por lo general, para que puedan enviar spam a todos sus seguidores de su cuenta. A menudo, los que van a tratar de engañarlo con un link que dirige a una página de acceso falsa Siempre que se le pedida que introduzca su contraseña de Twitter, sólo eche un vistazo rápido a la URL y asegúrese de que está realmente en Twitter.com.

4. Tenga cuidado con los enlaces extraños en DMs: Tenga cuidado al hacer clic en enlaces impares en MD. Incluso si el enlace de vino de un amigo, es posible que su cuenta se ha visto comprometida y la URL en realidad fue enviado por un spammer.
5. Las cuentas de usuarios pueden ser comprometidas si se ha facilitado el nombre de usuario y contraseña a un tercero, si la cuenta de Twitter es vulnerable por tener una contraseña débil, por virus y malware (que recolectan contraseñas) en tu computadora, teléfono celular , tablas o por utilizar una conexión en una red insegura como por ejemplo los llamados “Cyber”. De igual forma se puede dar el caso de que una aplicación de terceros (por ejemplo TweeDeck, Twitter de Android) tiene una falla de seguridad que causa un comportamiento inesperado.
6. Si una cuenta de Twitter ha sido comprometida o existen sospechas de posibles comportamientos dudosos en el uso de la misma, se deben seguir ciertas recomendaciones.

Las siguientes evidencias comunes que indican el uso no autorizado de las cuentas como los que se describen a continuación:

a) Tweets inesperados hechos desde tu cuenta.
b) Mensajes directos (MDs) inesperados, enviados desde su cuenta.
c) Otros comportamientos en la cuenta que se desconocen (como seguir, dejar de seguir o bloquear)
d) Notificaciones de parte de Twitter que indiquen algún cambio de dirección de correo electrónico o contraseña.

7. Si olvida su contraseña, puede restablecerla usted mismo, Si usted está recibiendo mensajes de correo electrónico de restablecimiento de contraseña que usted no haya solicitado, es posible que considere la verificación de un teléfono con su cuenta para evitar que otros usuarios por error a escribir su nombre de usuario en nuestro formulario de restablecimiento de contraseña. Siempre pedimos teléfono número de confirmación antes de enviar cualquier correo electrónico de restablecimiento de contraseña solicitadas por los usuarios.

Enlaces Evaluando en Twitter

1. Un montón de enlaces son compartidos en Twitter, y muchos se publican con acortadores de URL. Acortadores de URL, como bit.ly o TinyURL, crear vínculos únicos, más cortos que redirigen a su enlace más largo para que pueda ser más fácilmente compartida. Acortadores de URL también puede oscurecer el dominio final, por lo que es difícil saber dónde va el enlace.

2. Algunos navegadores tienen plug-ins gratuitos que le mostrará las URL

prolongados sin que tenga que hacer clic en ellos. Éstas son conexiones con plug-ins para Internet Explorer y Firefox (que es un navegador gratuito-para-descarga):

3. Expansores URL para Internet Explorer
4. Expansores URL para Firefox
5. En general, por favor tenga cuidado al hacer clic en enlaces. Si hace clic en un enlace y se encuentra inesperadamente en una página similar a la página de inicio de sesión de Twitter, no te rindas tu nombre de usuario y contraseña! Sólo tienes que escribir en Twitter.com en la barra del navegador y acceder directamente desde la página principal de Twitter.
6. Mantenga su computadora y navegador hasta al fecha y libre de virus
7. Mantenga su navegador y sistema operativo actualizado con las versiones y parches más actuales; parches a menudo son liberados para hacer frente a las amenazas de seguridad particulares. Asegúrese también de analizar el equipo con regularidad en busca de virus, spyware y adware.
8. Si estás utilizando un ordenador público, como en una biblioteca o en la escuela, asegúrese de que siempre la sesión en Twitter cuando haya terminado (hay un enlace "Salir" en la parte superior derecha de la página).