INSTITUTO ELECTORAL
DEL ESTADO DE GUANAJUATO

CONSIDERACIONES DE SEGURIDAD PARA EL "BUEN FIN - 2024"

Al ser el "Buen Fin" uno de los eventos con mayor flujo de capital durante esta temporada, se incrementan los intentos de ataque a organizaciones y sus clientes, con la intención de obtener beneficios principalmente económicos.

Por lo anterior, es importante considerar los tipos de ataques y recomendaciones que se describen a continuación para prevenir ser una víctima en esta temporada.

CIBERATAQUES MÁS COMUNES DURANTE EL "BUEN FIN"

Ataques de suplantación de identidad (phishing) y de malware de tipo troyanos bancarios

- Mensajes de correo electrónico y SMS falsos
- Phishing en redes sociales
- Malware de tipo troyanos bancarios

Recomendaciones para usuarios

- No abrir correos electrónicos o mensajes SMS de remitentes sospechosos, ni abrir los enlaces que se compartan sin validar que los perfiles en redes sociales sean los oficiales. En caso de recibir algún mensaje de un perfil que no sea el oficial, eliminarlo.
- No utilizar cuentas de correo institucionales para registrarse en servicios de terceros.
- No descargar archivos o software de fuentes no confiables o de enlaces compartidos a través de medios electrónicos de remitentes desconocidos.
- Establecer el MFA como método complementario de autenticación.



Ingeniería social y estafas bancarias

- Estafas en marketplaces o sitios web de compraventa entre usuarios.

- El uso de la IA (Inteligencia Artificial) como vector de ataque(crean imágenes, audios y videos pidiendo realizar acciones con urgencia).

Recomendaciones para usuarios

- En caso de recibir supuestas llamadas de bancos o comercios por supuestas "compras no autorizadas", mantener la calma, no dar datos personales o privados, colgar y llamar a la institución para reportar esta situación al número de teléfono que viene al reverso de la tarjeta.
- Evitar hacer negocios con personas que sean supuestos colaboradores autorizados de alguna institución bancaria o comercio si no se tiene certeza de su origen.
- Asegurar de interactuar solo con chatbots oficiales del sitio web consultado.
- Desconfía de videos o llamadas que pidan datos sensibles, y verificar siempre directamente con la tienda a través de sus canales oficiales.
- Considera utilizar bloqueadores de anuncios y herramientas de privacidad que limiten el seguimiento excesivo por parte de los sitios web visitados.



Fuente:Scitum, S.A. de C.V, 2024.

Ataques de web skimming, métodos de pasarelas de pago y puntos de venta (POS):

- Magecart y scripts maliciosos: los actores de amenaza inyectan scripts maliciosos en sitios web legítimos de e-commerce para capturar datos de tarjetas de crédito y otra información sensible cuando los usuarios realizan transacciones como compras en línea.

Recomendaciones para usuarios

- Evitar almacenar credenciales de acceso y datos de tarjetas bancarias en los navegadores web.
- No introducir datos de tarjetas de crédito en caso de identificar patrones como errores ortográficos, logotipos desactualizados, que no correspondan a los sitios web que utiliza habitualmente.
- Utilizar los medios de pago con tarjetas virtuales (Ej. PayPal o tarjetas que brinden protección contra fraude).
- Evita transferencias bancarias directas.

Ataques de tipo ransomware

Los actores de amenaza buscan vulnerar los servidores de tiendas en línea y otras infraestructuras esenciales, para afectar a la organización en días críticos e incitar a hacer el pago del rescate.

Recomendaciones para usuarios

- No descargar archivos o aplicaciones de fuentes no confiables o de enlaces compartidos a través de medios electrónicos de remitentes desconocidos.
- Mantener actualizado su sistema operativo o móvil con los últimos parches del fabricante.
- No descargar archivos o aplicaciones de fuentes no confiables o de enlaces compartidos a través de medios electrónicos de remitentes desconocidos.



Aplicaciones móviles maliciosas y Falsificación de sitios web (Typosquatting y Domain Spoofing)

- Apps falsas de compras o descuentos (de pago o tiendas populares en sistemas operativos basados en Android)
- Los actores de amenaza crean sitios web que imitan los de tiendas populares o la posición de manera no orgánica en los resultados de los buscadores web.

Estas podrían infectar dispositivos y robar información personal o financiera.

Recomendaciones para usuarios

- Descargar aplicaciones de las tiendas oficiales de acuerdo con su sistema operativo (App Store para iOS y Google Play Store para Android).
- No abrir enlaces de supuestos anuncios de problemas en el dispositivo, ya que estos redirigen o realizan la descarga de aplicaciones que pueden ser maliciosas.
- Antes de comprar en una tienda en línea desconocida, busca reseñas de otros usuarios para verificar la autenticidad del comercio. Sitios fraudulentos suelen tener pocas reseñas o experiencias negativas.
- Revisar tus transacciones durante y después del "Buen Fin". Si se detecta alguna transacción sospechosa, repórtala de inmediato a la institución bancaria o comercial.