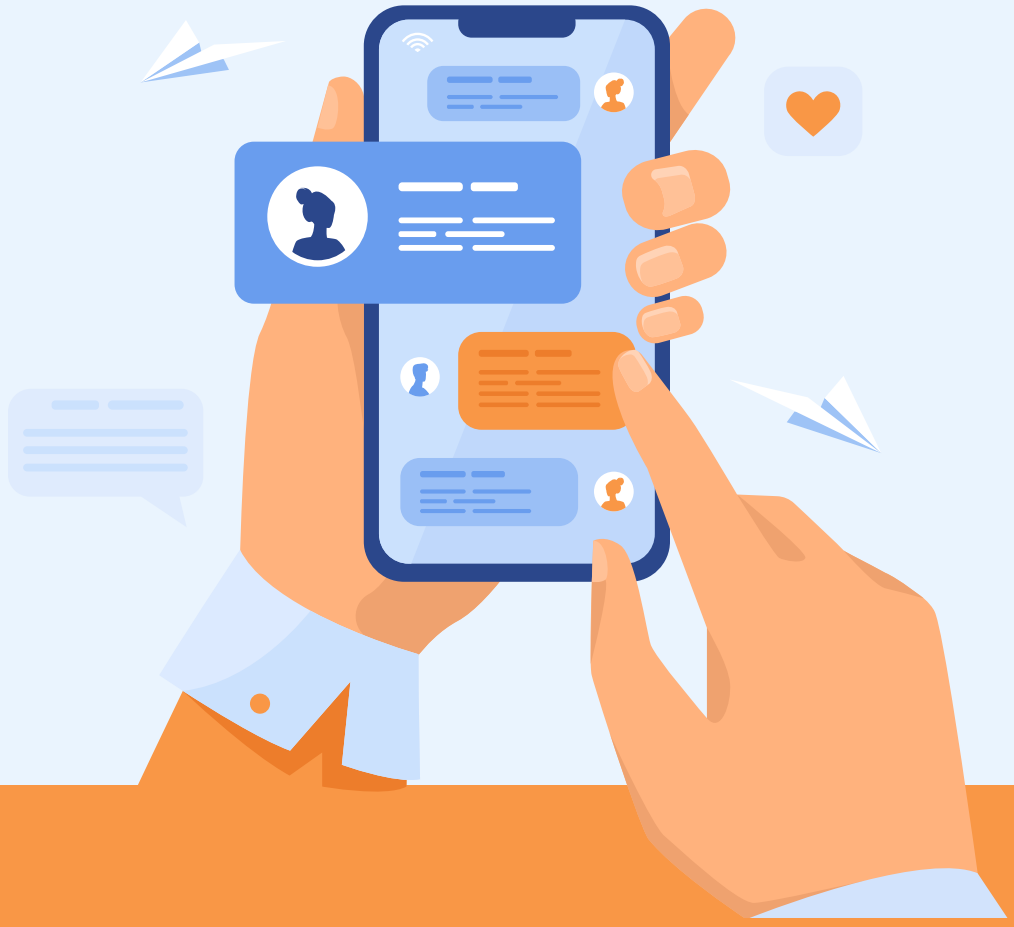
PLUS TI

WHITE PAPER

Cómo proteger al cliente de los riesgos de sus dispositivos



Contraseñas comunes en 2018-2020

123456	123456789	picture1	password	12345678
111111	123123	senha	qwerty	password1
qwerty123	123qwe	qwertuiop	admin	abc123

Fuente: CSO Online

Mucho se ha dicho de las debilidades que presentan las contraseñas como barrera de seguridad. Además de los ataques y otras condiciones y desafíos, el nivel de seguridad resulta relativamente bajo debido a:

1. Alto porcentaje de usuarios que no han cambiado nunca sus claves.
2. Alto porcentaje de usuarios que han utilizado las mismas claves por varios años.
3. Contraseñas de bajo nivel de complejidad.
4. Reutilizamiento de la misma contraseña en diferentes sitios o servicios.
5. Percepción de complejidad al manejar múltiples contraseñas únicas.

Los modelos de autenticación y autorización han evolucionado y fortalecido; han pasado de ser procesos simples de identificar y autenticar al usuario mediante la combinación de código de usuario y clave, a esquemas de autenticación fuerte multifactor (MFA). Estos esquemas han creado un modelo sobre la premisa de que un tercero no autorizado probablemente no será capaz de obtener todos los factores necesarios, y todos deberán ser comprometidos para obtener acceso.

De esta forma se combinan diferentes variables respecto a:

Este esquema de autenticación fuerte provee múltiples beneficios y seguridad más robusta: su distribución e implementación en dispositivos móviles es fácil; proporciona una capa adicional de defensa; reduce el riesgo de fraude en línea, phishing y otras técnicas; y permite el cumplimiento de normas y esquemas regulatorios.

Sin embargo, las amenazas al usuario son múltiples y entre estas destaca el phishing como la más común. Esta modalidad es exitosa debido a que utiliza técnicas de ingeniería social para la manipulación del usuario y su implementación es de costo relativamente bajo.

Formas de entrega de ataques de phishing:

Los ataques de phishing se esconden detrás de una fachada de legitimidad. Esto se evidencia en el reporte de 2020 de Sonic Wall respecto a Amenazas Cibernéticas, que identificó los archivos de PDF y Microsoft Office como los vehículos más comunes para entrega de archivos maliciosos debido a la confianza universal que reciben.

El reporte de transparencia de Google Safe Browsing muestra el pico más alto del año con 4.985.064 alertas generadas el 21 de marzo de 2021 respecto a sitios no seguros. Estas alertas son enviadas a los dueños de los sitios para su corrección, quienes muestran un tiempo de respuesta entre 12 y 90 días para arreglar sus sitios después de la notificación, según la misma fuente. Sin embargo, los sitios pueden volver a ser infectados si aún cuentan con vulnerabilidades.

Tiempo promedio que un adulto pasa en su teléfono al día

La cantidad de tiempo que interactúa la persona promedio con su teléfono móvil no ha pasado desapercibida para los cibercriminales, como tampoco lo ha sido la cantidad de información y la sensibilidad de esta que es almacenada en estos dispositivos. Por esta razón, lo que puede ser monetizado es la información y los ataques son sofisticados.

Existe gran cantidad de aplicaciones falsas que son distribuidas por medio de campañas de ingeniería social, técnicas de phishing o smishing, o tiendas no oficiales que permiten descargar aplicaciones pagadas de forma gratuita. Estas aplicaciones maliciosas pueden ser diseñadas para Android o iOS e imitar el aspecto y funcionalidad de aplicaciones legítimas para engañar a los usuarios desprevenidos.

Una vez instaladas, estas aplicaciones realizan acciones maliciosas como mostrar anuncios publicitarios, robar credenciales, interceptar datos y desviar mensajes SMS que contengan segundos factores de autenticación. Detectar estas aplicaciones falsas es un proceso complejo ya que se asemejan fuertemente a aquellas que buscan suplantar, y frecuentemente pasan un período de varios meses en tiendas de aplicaciones antes de ser removidas.

Categorías de aplicaciones maliciosas:

Backdoor	Fraude de facturación	Descargadores de aplicaciones
Botnet	Spyware comercial	Ransomware
Bot de anuncios	Contenido hostil	Troyanos

La complejidad de detección de aplicaciones falsas obliga a mantener una actitud vigilante, lo que contrasta con el diseño de la experiencia en los dispositivos móviles que se enfoca hacia la comodidad. Esto facilita que las aplicaciones falsas se propaguen con facilidad, y algunas recomendaciones comunes para que el usuario pueda evitarlas son:

1. Buscar errores en la ortografía o formato del título.
2. Revisar el ícono para asegurarse de que es correcto.
3. Verificar el desarrollador.
4. Revisar la cantidad de descargas, favoreciendo aquellas que han sido descargadas muchas veces.
5. Leer los comentarios y retroalimentación.
6. Estar atento a los permisos que se le otorgan.

Dentro de esta categoría de aplicaciones se encuentran los troyanos bancarios, programas que se ejecutan como una aplicación legítima en el sistema, pero realizan tareas maliciosas sin conocimiento del usuario. A diferencia de otros virus y gusanos, no se replican a sí mismos y son instalados por descargas automáticas de un archivo al entrar a un sitio web, tiendas falsas e incluso pueden ser descargados por otro malware.

La amenaza de los troyanos es su capacidad de mantenerse en segundo plano y a la espera de que el usuario acceda a su aplicación bancaria. Cuando esto sucede, el troyano sobrepone su propia interfaz a la del banco para robar las credenciales del usuario cuando son introducidas. Posteriormente intercepta los SMS entrantes al dispositivo para robar el segundo factor de autenticación.

Métodos de ataque de troyanos bancarios:

Intercepción de SMS en tiempo real para robo de segundo factor de autenticación.

Imita las aplicaciones móviles de los bancos para capturar credenciales.

Permiten al delincuente realizar transferencias bancarias por montos pequeños desde la cuenta del usuario a cuentas fraudulentas.

Los troyanos y sus formas de ataque evolucionan constantemente y obligan a evaluar diferentes criterios para generar una estrategia de prevención de fraude multicapa que abarque la prevención interna en el dispositivo móvil, múltiples factores de autenticación y análisis del riesgo transaccional.

Algunas recomendaciones para prevenir ataques por troyanos:

- Descargar aplicaciones desde tiendas oficiales.
- Utilizar buscadores seguros.
- Comprobar los permisos de cada aplicación.
- Nunca abrir un enlace que parezca provenir de su banco; ingrese de forma directa.
- Hacer copias de seguridad de sus archivos más importantes.
- Integrar una solución de seguridad dentro de la aplicación bancaria.
- Contar con mecanismos fuertes de autenticación en múltiples factores por diferentes canales.
- Actualizar constantemente las aplicaciones y sistema operativo del dispositivo.

PLUS TI

REFERENCIAS:

- Arzayus, A. (2021) “Más allá de las contraseñas”
- Curbow, A. (2020) “Prevent Banking Trojan Attacks on Your Organization”
- Fruhlinger, J., Martin, J. (2021) “The Password Hall of Shame (and 10 Tips for Better Password Security”
- Google (2021) “Google Transparency Report”
- Khan, S. (2021) “3 Tips to Prevent Mobile Banking Trojans”
- NordVPN (2021) “How to Spot a Fake App”
- SonicWall (2020) “2020 Cyber Threat Report”
- Surfshark (2021) “Fake Apps and How to Spot Them”
- Veliz, O. (2020) “Fake Apps y otras estafas en dispositivos móviles”
- Veliz, O. (2020) “Troyanos bancarios: la mayor amenaza cibernética móvil”
- Zalani, R. (2021) “Screen Time Statistics 2021: Your Smartphone is Hurting You”