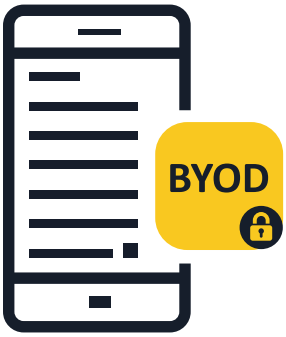
EUROPOL EC3 European Cybercrime Centre

SOFTWARE MALICIOSO EN DISPOSITIVOS MÓVILES

PAUTAS Y CONSEJOS PARA EMPRESAS

1 Informa a tu personal sobre los riesgos de los dispositivos móviles

- Trabajar desde un dispositivo móvil difumina la línea entre el uso empresarial y el personal. Las empresas pueden verse gravemente afectadas por ataques inicialmente dirigidos al dispositivo móvil de un empleado. Un dispositivo móvil es un ordenador y debe protegerse como tal.



2 Implanta una política de uso de dispositivos personales (BYOD) en la empresa

- Los empleados que utilicen sus propios dispositivos móviles para acceder a los datos y sistemas corporativos (aunque solo sea al correo electrónico, el calendario o la base de datos de contactos) deben seguir las políticas de la empresa. Elige con cuidado la tecnología que se utilizará para gestionar y proteger los dispositivos móviles y anima a tu personal a ser precavido.

3 Incluye políticas de seguridad en dispositivos móviles como parte de tu marco general de seguridad

- Si un dispositivo no cumple estas políticas, no debería poder conectarse a la red corporativa ni acceder a datos de la empresa. Las empresas deben implantar sus propias soluciones de gestión de dispositivos móviles (MDM) o gestión de la movilidad en la empresa (EMM).
- Para complementarlas, es básico instalar una solución de defensa contra amenazas móviles. Esto mejorará la visibilidad y la conciencia del contexto de las amenazas a apps, redes y sistemas operativos.

4 Sé precavido a la hora de utilizar redes wifi públicas para acceder a datos corporativos

- En general, las redes wifi públicas no son seguras. Si un empleado accede a datos de la empresa utilizando una conexión wifi abierta de un aeropuerto o una cafetería, la información podrá ser expuesta a usuarios maliciosos. Es aconsejable que las empresas desarrollen políticas a este respecto.

5 Mantén actualizados sistemas operativos y apps

- Diles a tus empleados que se descarguen las actualizaciones de software del sistema operativo de sus dispositivos móviles en cuanto se publiquen. Sobre todo en Android, consulta la política de actualizaciones de los proveedores y fabricantes de dispositivos móviles. Las últimas actualizaciones no solo harán que los dispositivos sean más seguros, también que funcionen mejor.

6 Instala aplicaciones solo de fuentes fiables

- Las empresas solo deben autorizar la instalación de aplicaciones procedentes de fuentes oficiales en aquellos dispositivos que se conecten a la red corporativa. No dejes de pensar en la posibilidad de abrir una tienda de apps corporativa a través de la cual los usuarios finales puedan acceder a apps aprobadas por la empresa, descargarlas e instalarlas. Habla con tu proveedor de seguridad para pedirle asesoramiento o créala con tus propios recursos.

7 Evita el jailbreaking

- Hacer jailbreak consiste en eliminar las limitaciones de seguridad impuestas por el proveedor del sistema operativo, accediendo así a todas las características y funciones del sistema operativo. Hacer jailbreak en tu dispositivo puede provocar que sea mucho más inseguro y crear fallos de seguridad que en un principio no estaban patentes. Los dispositivos rooteados no deben permitirse en un entorno corporativo.

8 Piensa en alternativas de almacenamiento en la nube

- Normalmente, los usuarios de dispositivos móviles quieren acceder a documentos importantes tanto a través de los ordenadores del trabajo, como desde sus teléfonos o tablets personales fuera de la oficina. Las empresas deben evaluar la creación de un servicio de almacenamiento y sincronización de activos en la nube para satisfacer esta necesidad de forma segura.

9 Anima a tu personal a instalar una app de seguridad móvil

- Todos los sistemas operativos corren el riesgo de ser infectados. Si dispones de ella, asegúrate de que utilizan una solución de seguridad móvil que detecte y evite malware, spyware y apps maliciosas, además de ofrecer otras funciones para proteger la privacidad y antirrobo.

GUARDIA CIVIL
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
OSI Oficina de Seguridad del Internauta
Norton by Symantec
TREND MICRO
KASPERSKY lab

#MobileMalware