

sedian

Seguridad Digital
de Andalucía



Ficha técnica

Dispositivos móviles: un nuevo vector de ataque

Acción formativa en modalidad Charla Virtual.
27 de enero de 2023.



Junta de Andalucía

Índice

1 DATOS BÁSICOS DE LA ACCIÓN FORMATIVA.....	3
2 DESCRIPCIÓN.....	3
3 OBJETIVOS.....	4
4 CONTENIDOS.....	4
5 TEMPORALIZACIÓN.....	5
6 METODOLOGÍA.....	6
7 DOCENTE.....	7
8 EVALUACIÓN.....	7

1 DATOS BÁSICOS DE LA ACCIÓN FORMATIVA

Nombre de la acción formativa: Dispositivos móviles: un nuevo vector de ataque

Modalidad: Charla Virtual.

Fecha de celebración: 27 de enero de 2023.

Horario: 09:00 a 10:30 A.M.

Dirigido a: Profesionales TIC de la Junta de Andalucía y entidades vinculadas.

Número máximo de personas participantes: 100.

2 DESCRIPCIÓN

En esta charla analizaremos e identificaremos los diferentes elementos que deberemos tener en cuenta como posibles vectores de ataque a nuestros dispositivos inteligentes.

El uso de estos dispositivos, como los Smarthome, Asistentes virtuales, SmartCity, Smartphone, etc. se ha generalizado en los últimos años y en la mayoría de las ocasiones sus sistemas de defensa ante ataques externos son muy deficientes.

Para poder tener un conocimiento de las amenazas a las que podemos enfrentarnos, estudiaremos los diferentes ataques a los que podemos estar expuestos y definiremos las medidas de prevención y respuesta ante un posible incidente.

3 OBJETIVOS

Generales

- Examinar las vulnerabilidades y amenazas más frecuentes para los dispositivos móviles.

Específicos

- Analizar los diferentes vectores de ataque para evitar convertirnos en un blanco fácil.
- Determinar los tipos de malware a los que se nos exponemos los usuarios de dispositivos móviles.
- Establecer buenas prácticas de uso orientadas a dispositivos móviles.
- Conocer los diferentes ataques de ingeniería social actuales, como phishing o smishing.
- Entender los peligros de conectarnos a redes desconocidas o públicas
- Aprender como localizar un dispositivo perdido o robado.

4 CONTENIDOS

- Presentación.
- Malware.
- Ingeniería social.
- OWASP Móvil.
- Fuga de datos.
- Permisos.

- Robo de información.
- Redes Wifi.
- Software desactualizado.
- Configuración débil o inexistente de seguridad (Contraseñas)
- Acceso físico.
- Pérdida o robo del dispositivo.
- Conclusiones.
- Ruegos y Preguntas.

5 TEMPORALIZACIÓN

Fecha: 27/01/2023. **Horario:** 09:00 a 10:30 (90 minutos).

Modalidad: Charla Virtual.

PLANIFICACIÓN HORARIA

1 MINUTO.	Presentación.
10 MINUTOS.	Malware.
10 MINUTOS.	Ingeniería social.
5 MINUTOS.	OWASP Móvil.
5 MINUTOS.	Fuga de datos.

10 MINUTOS.	Permisos.
7 MINUTOS.	Robo de información.
10 MINUTOS.	Redes Wifi.
5 MINUTOS.	Software desactualizado.
7 MINUTOS.	Configuración débil o inexistente de seguridad (Contraseñas)
5 MINUTOS.	Acceso físico.
5 MINUTOS.	Pérdida o robo del dispositivo.
10 MINUTOS.	Ruegos y Preguntas.

6 METODOLOGÍA

La sesión formativa se desarrollará en **modalidad Charla Virtual**, es decir, un seminario impartido en línea donde la interactividad con el alumno es en tiempo real de forma virtualizada con herramientas informáticas diseñadas para tal fin. La herramienta usada para esta sesión se denomina **GoToWebinar**.

7 DOCENTE

IMPARTIDO POR: David Sánchez Jiménez.

CSE de Elevenpatchs, CEO de Sputnik Ciberseguridad, pentester y auditor.

Apasionado de la ciberseguridad volcado en la formación de los nuevos talentos para las nuevas tecnologías.

Actualmente, profesor de ciberseguridad en Mastermind. Ha participado como director académico y docente del programa nacional de ciberseguridad "Actualízate", y además ha sido profesor y director de desarrollo profesional del Máster oficial en Dirección de Ciberseguridad, Hacking Ético y Seguridad Ofensiva en la Escuela Internacional de Posgrados.

Acceso a su [perfil LinkedIn](#)

8 EVALUACIÓN

Para la evaluación de la Charla Virtual se tendrán en cuenta las siguientes variables: la asistencia y el tiempo de conexión a la Charla Virtual, que deberá ser igual o superior al 50%.

- ✓ Asistencia a la jornada con un tiempo de conexión superior al 50%.
- ✓ Superar el cuestionario de conocimientos con un porcentaje de acierto del 60% o superior (en un plazo de 72 horas tras el evento).

Los valores de estas variables serán extraídos de diferentes informes generados por la herramienta **GoToWebinar** usada para celebrar la sesión.

Criterios de evaluación

Evidencias para la evaluación	Peso
Asistencia	50%
Evaluación de Conocimientos	50%

Sistema de evaluación.

Valoración de Asistencia.

Cálculo realizado a partir de los informes extraídos de la plataforma **GoToWebinar** denominados:

- ✓ Informe de Rendimiento.
- ✓ Informe de Asistentes.

Valoración de Conocimientos.

Indicador obtenido a partir de un cuestionario de 10 ítems sobre aspectos tratados durante la sesión.