

sedian

Seguridad Digital
de Andalucía



Propuesta

Charla de sensibilización:

Cómo acceder y comprar por internet sin
poner en riesgo tus datos.

Contraseñas, control parental y
transacciones en la red.

Fecha documento: 23/11/2021



Junta de Andalucía

Consejería de Economía, Conocimiento,
Empresas y Universidad

ÍNDICE

1. Estructura de la sesión	2
2. Propuesta de contenido	3
3. Información sobre el Ponente	10

1. Estructura de la sesión

- **Destinatarios:** Ciudadanía en general con **bajos conocimientos en tecnología.**
- **Temática:** Concienciación en el uso de gestores de contraseñas y dar a conocer consejos sobre cómo proteger tus dispositivos móviles en caso de pérdida, robo o extravío, además de implementar el control parental de dichos dispositivos.

Aprender a realizar compras seguras en internet, desde cualquier dispositivo y descubrir las grandes amenazas que tenemos cuando compramos por internet.

- **Duración:** 1 hora y 15 minutos + 15 minutos preguntas
- **Fecha:** viernes día **3 de diciembre,**
- **Canales de visualización del evento:** GotoWebinar
- **Software empleado:** GotoWebinar
- **Nº de usuarios concurrentes estimados:** 100 usuarios aprox.

2. Propuesta de contenido

Para la realización de esta charla de sensibilización utilizaremos la herramienta de seminarios web GotoWebinar.

Será necesario crear un evento desde la cuenta de Avante y difundir el formulario de inscripción.

Hemos desarrollado una propuesta de contenido ajustada a las necesidades planteadas. Esto es, un público objetivo con capacidades digitales básicas y con escasa conciencia sobre seguridad digital, en particular en la gestión de contraseñas.

Proponemos dos temáticas, una relacionada con las contraseñas y otro con el control parental.

1. Si tu contraseña falla, ¿sabes cómo actuar?

La seguridad informática es fundamental en el ámbito personal y familiar. A medida que pasamos más tiempo en línea, a menudo creamos y compartimos más datos personales. Si estos datos caen en las manos equivocadas, la información privada y financiera podría estar en riesgo. La protección de los datos confidenciales es fundamental, pero todo comienza con una contraseña.

- La importancia de una contraseña robusta, la puerta de entrada a cualquier servicio internet
- El peligro de una clave única para muchos servicios...
- ¿Por qué cambiar periódicamente tus contraseñas puede en realidad hacerte más vulnerable ante los hackers?

- Veamos algunas reglas útiles para crear contraseñas, pero no te olvides de llevar en el bolsillo un generador automático (IOS, Android y Web escritorio).
- Seamos creativos con las respuestas a las preguntas sobre la recuperación de su cuenta.
- Gestores de contraseñas para evitar memorizarlas (algunas herramientas específicas y navegadores web).
- Copia de seguridad de mis contraseñas y distribución automática entre mis dispositivos.
- OAuth: inicio de sesión único en varias plataformas.
- La biometría no es lo mismo que las contraseñas. ¿Son seguros los sistemas biométricos? Prolifera el uso como selfies para desbloquear un móvil o abrir una cuenta bancaria, pero ¿conocemos los riesgos, que puedo hacer?
- Como reforzar mi contraseña con sistemas de autenticación de doble factor (SMS, generadores de clave única, etc.)

2. ¿Cómo podemos proteger a nuestros hijos de las amenazas de Internet?

Un control parental es fundamental en la sociedad actual con todos los dispositivos que los menores tienen a su alcance. El hecho de que los menores obtengan dispositivos a una edad más temprana hace que este tipo de servicios sea fundamental en las familias.

Un control parental debe tener algunas características esenciales:

- Un control parental único para administrar diferentes dispositivos es vital para mantener una protección eficiente del dispositivo.
- Control web: la gestión de contenido web es la primera característica clave para los padres.
- Control de aplicaciones: evitar que los menores utilicen aplicaciones no adecuadas para ellos es otra característica clave.
- Límite de tiempo de aplicación: los padres necesitan limitar el tiempo que sus hijos pasan usando aplicaciones.
- Pausas: otra característica interesante es poder establecer pausas en períodos de tiempo específicos para que el dispositivo esté bloqueado y que no se puedan usar.
- Geolocalización: Una característica fundamental para los padres es la geolocalización, la utilizan para saber dónde están sus hijos en cualquier momento.
- Estadísticas y logs: los padres también necesitan saber qué sitios y apps ha usado su hijo y estadísticas para saber qué tiempo pasan sus hijos usando sus teléfonos inteligentes y cuánto tiempo dedican a ello.

3. Cómo realizar compras seguras por Internet

La preparación previa a la compra.

Es habitual que cuando vamos a realizar una compra online empecemos a plantearnos la seguridad durante el proceso, pero a veces es necesario preocuparnos antes de iniciarla. Un dispositivo seguro nos puede ayudar a prevenir problemas incluso antes de empezar.

Contenido:

- La seguridad del dispositivo
- Conexiones seguras
- Usando el móvil para comprar.

Buscando las mejores ofertas y las tiendas más seguras.

A veces descartamos una tienda de nuestra ciudad porque nos desagrada su escaparate, el trato de sus profesionales o bien porque los productos parecen de escasa calidad.

Al realizar compras online algunas de estas comprobaciones son más difíciles de realizar por eso tenemos que aprender a analizar ciertos detalles.

Contenido:

- Tipos de tienda online (de empresas, de terceros, segunda mano, ...)
- ¿Es una empresa fiable?
- Revisar las opiniones
- Avisos legales
- Sellos de confianza online

La gran estafa. ¿Cómo la reconocemos?

Todos estamos expuestos a posibles estafas en transacciones online. Algunas son más difíciles de detectar que otras. En este apartado veremos algunas pistas que nos ayudarán a detectar cuando quieren engañarnos.

Contenido:

- Correos y promociones sospechosas
- El regalo que no llega
- Introducción de datos peligrosos
- ¿Es esta página segura?
- La trampa de los precios bajos
- Publicidad engañosa.

- La trampa del tipo de pago inexistente

El momento clave: el pago.

Uno de los objetivos de las acciones fraudulentas es la obtención de nuestros datos bancarios y, por supuesto, de nuestro dinero.

El método de pago es una de las características que más define la seguridad de una transacción, por eso debemos conocer cuáles son estos métodos y qué ventajas y desventajas ofrecen a los consumidores.

Contenido:

- Tipos de forma de pago
- Peligros y Ventajas
- La política de devolución
- Spam ¿qué es y cómo evitarlo?

Aplicaciones. ¿Qué precauciones tenemos que tomar para utilizarlas?

El último punto nos lleva las aplicaciones, el corazón de nuestros dispositivos.

¿Las estamos usando correctamente?

Veremos todo lo necesario para reconocer cuales son las aplicaciones que debemos usar y cuales nos están usando a nosotros.

Contenido:

- Instalando desde la tienda oficial
- Actualizaciones ¡activando!
- Permisos de las aplicaciones
- Cuidado al hacer “clic”.

3. Información sobre el Ponente

Nuestro formador David Rodríguez, será el ponente de esta sesión, ya que reúne todas las características necesarias para llegar hasta el público objetivo: nivel de comunicación, capacidad para conectar rápido con el auditorio, conocedor de las tecnologías de la información desde 2005. Gran bagaje con alumnos con bajo nivel tecnológico, experto en herramientas de productividad personal y experiencia sensibilizando en seguridad TI a usuario no tecnólogos.

Perfil de LinkedIn: <https://www.linkedin.com/in/davidrodriguezporras/>