cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

USO SEGURO DE DISPOSITIVOS EN UN MUNDO DIGITAL INSEGURO

Documento para profesorado

da Vinci college

VARIA VANTAAN AMMATTIOPISTO

New College Lanarkshire

SRC Business Support & Innovation

BCS Koolitus

HETEL

Duración del reto

3-6 hours

Descripción del reto (enunciado para el alumnado)

Te han regalado un nuevo dispositivo digital (el profesor o profesora te dirá qué tipo, si un móvil, una Tablet… o si tu equipo puede escogerlo libremente). Como usuario/a responsable, quieres asegurarte de que el dispositivo y la información que introduzcas en él están lo más protegidos posible.

Tu intención es usar el dispositivo para uso general: e-mail, explorador web, redes sociales, banca on-line…

Tu reto es demostrar que eres consciente y entiendes los riesgos que presenta el uso de dispositivos digitales y que sabes cómo protegerte a nivel de usuario.

Resultados de aprendizaje

U1L01. El alumno/a es capaz de identificar riesgos físicos y virtuales asociados a la tecnología

U1L02. El alumno/a es capaz capaz de implementar las estrategias para prevenir riesgos y se auto actualiza en esta materia

U1L03. El alumno/a es capaz de instalar y actualizar software anti malware.

U1L04. El alumno/a es capaz de protegerse frente al fraude a través del uso de contraseñas seguras.

U1L05. El alumno/a es capaz de proteger distintos dispositivos vulnerables a distintas amenazas digitales (malware, phishing, etc.).

U1L06. El alumno/a es capaz de identificar información sensible/valiosa así como ataques a distintos tipos de datos

Requisitos mínimos para realizar el reto

Conocimiento previo	Equipamiento/software	Recursos
Haber usado un dispositivo conectado a internet, como un ordenador, una Tablet o Smartphone.	Un dispositivo conectado a Internet. Ordenador Portátil Smartphone Tablet	• https://en.wikipedia.org/wiki/Computer_security • https://en.wikipedia.org/wiki/Digital_security • https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more • https://passwordsgenerator.net • https://howsecureismypassword.net/ • https://www.roboform.com/how-secure-is-my-password • https://lastpass.com/howsecure.php *Hay una cantidad enorme de recursos disponibles, así que utiliza los que prefieras o sean más fácilmente accesibles. Estos recursos que aquí facilitamos también se proporcionan al alumnado en el enunciado del reto dirigido a este colectivo.*

Fases del reto

A continuación sugerimos la duración para cada fase de implantación del reto:

- 0,5 horas para identificar los parámetros del reto (posiblemente incluyendo la identificación quién realizará cada tarea)
- 1 hora para buscar información
- 0,2 horas para seleccionar información
- 0,2 horas para generar alternativas
- 0,3 horas para identificar propuestas y discutirlas en el equipo
- 0,2 horas para identificar cómo se pueden presentar los resultados (siguiendo las instrucciones que les proporciones)
- 0,3 horas para preparar la presentación de resultados (por ejemplo, elaborando un PowerPoint, una simulación...).
- 0,15 horas para que los grupos presenten sus conclusiones y debatirlas
- 0,15 horas para evaluar cómo se han resuelto los retos y qué mejoras se podrían proponer.

Presentación de resultados

Los resultados pueden presentarse en el formato que decida el grupo, incluyendo (pero no restrictivamente):

- Vídeo
- Presentación usando Software
- Oral \ verbal (esto debería de grabarse)
- Informe escrito
- Blog / vlog /wiki
- Cualquier otro formato

Nota: Esta es nuestra recomendación, pero decide tú qué formato es más adecuado.

Criterios de evaluación

Las siguientes recomendaciones son sólo sugerencias y se proporcionan como guía de apoyo.

Presentación pública (20%)

Puedes utilizar la tabla del ***Apéndice A*** al final de este documento que contiene criterios para ayudarte en la evaluación de competencias de presentación.

Trabajo en equipo (20%)

Puedes utilizar la tabla del ***Apéndice B*** al final de este documento que contiene criterios para ayudarte en la evaluación de competencias de presentación.

Resolución del reto (60%). Puede ser 10% por ítem.

1. El equipo identifica y agrupa al menos 3 riesgos físicos y tres virtuales.

Posibles respuestas del alumnado (listado no exhaustivo):

Riesgos físicos	**Riesgos virtuales**
Dejar el dispositivo desatendido, que el dispositivo pueda ser sustraído	No tener un anti-virus en el dispositivo
Que el agua dañe el dispositivo	No actualizar el software (parcheado)
Darle tu contraseña personal a alguien	Credenciales de seguridad débiles (contraseña, PIN, etc.)

Sobrecalentamiento del dispositivo	Instalación de aplicaciones sin certificados/credenciales de seguridad

2. El equipo describe una estrategia para prevenir verse comprometido.

Aspectos que se ***deberían*** incluir en la estrategia (para el usuario/a del dispositivo):

- Restringir el acceso al dispositivo requiriendo la autentificación del usuario/a (esto debería incluir un énfasis sobre el PIN, medios biométricos (por ejemplo, huella digital), contraseñas seguras, autenticación en dos pasos (2FA) (por ejemplo, e-mail y SMS enviado al móvil).
- Actualizar el sistema operativo del dispositivo con los últimos parches de seguridad.
- Realizar back-ups de datos.
- Usar Webs encriptadas/seguras cuando sea posible
- Desactivar servicios mientras no estén en uso (Bluetooth, Wi-Fi…).
- Ser crítico/a y saber reconocer el Phishing
- Instalar y/o actualizer software anti-malware, etc

3. El equipo instala/actualiza un software anti-malware en el dispositivo

Puede tratarse de la instalación de nuevo software anti-malware o asegurarse de que el software anti-malware actual es la versión más reciente. En NIST.org existe un listado sobre anti-malware disponible:- https://www.nist.org/news.php?extend.45.11

También incluye un servicio gratuito donde se puede subir cualquier archivo para su escaneado remoto: https://www.virustotal.com/gui/home/upload. Esto puede ser útil en caso de que no se pueda realizar un escaneado de forma local en el dispositivo.

4. El equipo genera y testea contraseñas seguras

El equipo ***puede*** usar los links siguientes (incluidos en la sección de recursos) para:

- Generar una contraseña –
  - https://passwordsgenerator.net
- Testar la seguridad de las contraseñas generadas –
  - https://howsecureismypassword.net/
  - https://www.roboform.com/how-secure-is-my-password
    https://lastpass.com/howsecure.php

5. El equipo identifica vulnerabilidades potenciales del dispositivo y posibles mecanismos para su protección.

Se deberían identificar al menos 3 vulnerabilidades potenciales y sus posibles mecanismos de protección, tales como:

Vulnerabilidades potenciales	**Mitigación**
El nuevo dispositivo viene sin autenticación	Habilitar la autenticación en el dispositivo
Los servicios como Wi-Fi y Bluetooth vienen automáticamente activados y pueden comprometer la seguridad.	Desconectar los servicios cuando no se estén usando.

Descarga de apps que pueden contener malware.	Descargar sólo de sitios recomendados. Asegurarse de que hay software anti-malware instalado y actualizado.

6. El equipo identifica datos sensibles y posibles ataques dependiendo de la naturaleza de los datos.

Aquí algunos ejemplos:

Plataforma / área	Tipo de datos	Vector de ataque
Redes sociales	Información personalmente identificable (PII)	Social engineering, Phishing, etc.
Banca on-line	PII, financieros	Social engineering, Phishing etc
Descarte de correo antiguo a la papelera	PII, financieros	Dumpster diving (urgar en la basura)
e-mail	Imágenes, PII, financieros	Esteganografía (ocultación de información a través de imágenes). Técnica muy usada para transmitir mal-ware (ver: http://www.mejor-antivirus.es/noticias/el-regreso-del-troyano-zeus.html)

Apéndice A

Evaluación de la presentación

Criterios	Excelente	Muy bien	Bien	Suficiente	Sin hacer	Comentarios/sugerencias:
Introducción oral: introducción, captación de atención de la audiencia,	4	3	2	1	0	
Lenguaje: Fácil de seguir y entender, información certera y completa.	4	3	2	1	0	
Resumen: Breve, claro y se proporcionan conclusiones.	4	3	2	1	0	
Actuación: Se muestra una pronunciación correcta, expresiones correctas, naturalidad, contacto visual con la audiencia, tono de voz alto y claro, poca dependencia de textos	4	3	2	1	0	
Conocimiento: El/la participante es capaz de responder a las preguntas de la audiencia	4	3	2	1	0	
Atención de la audiencia: Se mantiene la atención de la audiencia durante la presentación	4	3	2	1	0	
Fuentes: Se muestran las fuentes usadas al final de la presentación	1	0	0	0	0	

Apéndice B

Objetivos						
Los objetivos no están claros o se entienden poco, de forma que hay poco compromiso hacia ellos.	1	2	3	4	5	Los objetivos son claros, entendidos y hay total compromiso por parte de los miembros del equipo.
Apertura						
Los miembros del equipo no debaten sus ideas	1	2	3	4	5	Los miembros del equipo expresan sus ideas de forma abierta y libre y se debate.
Confianza						
Los miembros del equipo no confían los unos en los otros.	1	2	3	4	5	Los miembros del equipo del equipo confían los unos en los otros.
Actitudes sobre las diferencias						
Los miembros del equipo evitan hablar de diferencias para no enturbiar el ambiente de trabajo	1	2	3	4	5	Los miembros del equipo confrontan sus diferencias y trabajan para solucionarlas y alcanzar acuerdos.

Apoyo						
Los miembros del equipo no piden ayuda aunque la necesiten	1	2	3	4	5	Los miembros del equipo se muestran abiertos a pedir ayuda y admitir propuestas.
Participación						
La discusión las dominan unos pocos miembros.	1	2	3	4	5	Todos los miembros se involucran activamente en las discusiones.
Toma decisiones						
Las decisiones las toman unos pocos.	1	2	3	4	5	Todos los miembros participan en la toma de decisiones.
Flexibilidad						
El grupo se ciñe a reglas establecidas y procedimientos que son difíciles de cambiar.	1	2	3	4	5	Los miembros están dispuestos a cambiar su forma de trabajar.

Uso de los recursos personales del equipo						
No se utilizan de forma adecuada los conocimientos, habilidades y competencias de los miembros del equipo.	1	2	3	4	5	Se utilizan completamente los conocimientos, habilidades y competencias de los miembros del equipo.