INDICACIONES PARA TRABAJAR EN EL AULA

Jornada de ciberseguridad 2018

1. Auto-protección

Los dispositivos tecnológicos y aplicaciones en red deben protegerse para ayudarnos a salvaguardar nuestra información personal (datos personales, gustos y aficiones, imágenes, creaciones originales, etc.). Esa protección inicial (puerta de entrada) la logramos usando contraseñas robustas. Pero al igual que queremos evitar que alguien "entre" en nuestros sistemas debemos asegurarnos que cerramos bien la puerta cuando dejamos de usarlo mediante el cierre de sesión (¡especialmente en el correo electrónico y redes sociales en ordenadores compartidos!)

1.1 ¿Cómo reconocer una buena contraseña?

- Usan letras mayúsculas y minúsculas, números y otros caracteres
- Tienen al menos 8 caracteres de longitud
- No contienen información personal como tu nombre, fecha de nacimiento, etc.
- Cada servicio importante que uses (correo, red social…) deberá tener una contraseña diferente
- Si son pines numéricos, no poner números seguidos ni números relativos a fechas que me puedan relacionar como mi año de nacimiento

1.2 ¿Cómo recordar una buena contraseña?

Usando una "frase de contraseña":

1. Crea una frase
2. Toma una letra o sílaba de cada palabra (primera o última)
3. Transforma algunas en mayúsculas (impares, pares)
4. Transforma algunas letras en símbolos o números (usa siempre la misma regla de transformación)

Me gusta la Coca Cola Zero = MegulaCoCoZe => MegulaCoCo0 => M3gul@CoCo0

1.3 Principales amenazas de seguridad y su significado

1. Adware: software no autorizado que permite el envío de publicidad a mi dispositivo

2. Encriptación: método de codificación o cifrado que oculta la información a ojos curiosos usando códigos para ocultarla o una clave
3. Firewall: aplicación dentro de una red que permite bloquear y filtrar el tráfico que sale o entra a una red o equipo
4. Keylogger: malware que captura las pulsaciones del teclado y movimientos del teclado sin que el usuario se de cuenta para robarle información
5. Malware: programa informático que tiene efectos no deseados o maliciosos y que suele utilizar herramientas de comunicación populares para transmitirse como el correo electrónico o los pinchos USB
6. Phising: suplantación de la identidad de alguien conocido para obtener información
7. Ransomware: software que nos secuestra una parte de nuestro disco duro para que no podamos acceder a sus datos y nos pide un rescate económico para recuperarlo
8. Spam: también se le llama correo basura. Son mensajes idénticos enviados a muchas personas que generalmente no han pedido que los envíen. Se usan mucho como canal de transmisión de malware y para realizar phising
9. Spyware: software que espía al usuario de un dispositivo y manda su información y comportamiento a otras personas
10. Virus: software que altera el funcionamiento normal de un dispositivo sin conocimiento de su dueño

1.4 Buenas prácticas aprendidas en la lección

- Elige contraseñas robustas y emplea una frase de contraseña para recordarlas
- No compartas contraseñas con nadie ni las dejes a la vista
- Cada servicio importante que uses (correo, red social...) deberá tener una contraseña diferente
- No reutilices contraseñas cuando tengas que cambiarlas
- Cerrar la sesión siempre (especialmente en ordenadores compartidos)

1.5 Ampliaciones

- Completa la información de recuperación de cuenta por si alguna vez pierdes o tratan de robar tu contraseña
- Aplicar la función de bloqueo de pantalla en dispositivos móviles para proteger la información personal. Mejor un PIN que un patrón (no uses series consecutivas)
- Investiga que es la autenticación en dos pasos y úsala en las aplicaciones más críticas: contraseña y envío de mensaje al móvil

- Evitar descargas potencialmente dañinas: asegúrate de saber quien está detrás de la aplicación que te quieres descargar y cuál es su verdadero propósito
- Desconfía de las aplicaciones gratis. Nada es gratis, analiza que te pedirán a cambio: anuncios, datos, etc.
- Sospecha de los permisos que te solicitan a la hora de instalar: "¿necesita una linterna acceder a tus contactos?"
- Protege los dispositivos con las actualizaciones del sistema
- Aprende a diferenciar entre las redes de WiFi públicas y privadas, y cómo utilizarlas de manera segura: no deberías usar una red WiFi pública por ejemplo para entrar a tu banco, a tu correo o hacer pagos

2. Identidad personal

La actividad en Internet deja un rastro denominado huella digital que nos acompaña incluso en el futuro. Es preciso ser consciente de lo que ello supone y de cómo nuestra actividad en redes nos hace reconocibles como individuos. Es imprescindible que los alumnos se pregunten antes de compartir algo lo siguiente: "¿me puede perjudicar en el futuro?".

La información personal es algo muy valioso. En Internet es lo más valioso que tenemos y mucha gente quiere obtener información (legal o ilegalmente). Tenemos que ser consciente y protegerla. Si cuidamos nuestras pertenencias y las protegemos, tenemos que hacer lo mismo con nuestra identidad personal.

2.1 ¿Público o privado?

Saber diferenciar que se puede y que no se puede compartir les puede ahorrar problemas en el presente y en el futuro (huella digital). Tanto las imágenes como los contenidos/opiniones vertidas en la red pueden convertirse en virales (para bien o para mal). Lo importante es que una vez publicado en la red, perdemos el control absoluto sobre el contenido, y sobre las personas que pueden verlo. Algunas indicaciones para practicar sobre la idoneidad de publicar y compartir en redes:

- No subas imágenes al momento de tomarlas (desde tu teléfono). Pueden dar información sobre donde te encuentras (metadatos de geoposición) y además siempre es bueno tomarse un tiempo para pensar si se debe compartir algo
- No deberías subir imágenes en las que se te identifique a tí (recuerda que con menos de 14 años necesitas permiso de tus padres) ni a terceras personas
- No subas fotos o escribas comentarios que te puedan perjudicar en el futuro. Piensa en lo siguiente "¿si algún día soy presidente del gobierno o voy a buscar trabajo podrán utilizar esto en mi contra?"

- Pide permiso a las personas que salen en tus fotos antes de compartirlas y, en cualquier caso, intenta compartir las imágenes solo entre las personas que salen
- Nunca publiques fotos con poca ropa. Si nos vas al colegio desnud ¿por qué tienes que desnudarte en Internet que te puede ver más gente?

2.2 Buenas prácticas aprendidas en la lección

- Todo lo que hacemos en Internet deja una huella que perdura en el tiempo. Piensa antes de publicar
- Nuestra información personal es muy valiosa. Tenemos que aprender a diferenciar que forma parte de nuestra vida pública y privada
- Al compartir una foto (o un comentario) en Internet perdemos el control absoluto. Aunque lo borremos siempre habrá gente que haya podido realizar una captura o una descarga y podrá modificar y manipular la imagen para hacernos daño (bulos, memes, etc.)

2.6 Ampliaciones

- Compórtate con corrección cuando comentes en redes sociales. No eres anónimo y la Ley y el respeto aplica igual que en el "mundo real"
- Dedica tiempo a comprender las opciones de privacidad en tus cuentas: puedes elegir con quien compartes tu información

3. Confianza online

Las nuevas generaciones de jóvenes han crecido y se han educado con Internet como fuente principal, casi única, de información. Esto da lugar a la creación de informaciones y mensajes poco veraces que pueden ser compartidos muy rápidamente si no se tiene el criterio suficiente para discernir si el contenido es verídico o no.

3.1 Fakes

Este uso (redes sociales, WhatsApp, sitios web dudosos) y la propagación a través de la compartición de contenidos, han hecho que hoy por hoy existan gran cantidad de contenidos de dudosa credibilidad (fakes) que **siempre son creados con alguna intencionalidad: como la estafa o la manipulación de la opinión.**

¿Son conscientes realmente los jóvenes de que todo lo que se publica o comparte en Internet no tiene porque ser verídico?

- En el caso de los correos electrónicos que puedas recibir fíjate siempre en la dirección de correo del remitente y en los posibles enlaces que existan. ¿Procede de una dirección oficial (playstation.com vs pleystation.com). Una empresa o un comunicado oficial nunca usarán correos gratuitos tipo gmail o hotmail
- Desconfía de los correos electrónicos que te solicitan datos, especialmente aquellos alarmistas o que ofrecen regalos/beneficios
- En el caso de noticias, analiza la fuente (elmundo.es vs elmundotoday.com) de la noticia. Si desconfías de su contenido, busca otras fuentes (otros periódicos online, Google, periódicos de papel, telediarios, radio...)
- Recuerda la clase de lengua que hablaba del texto periodístico y analiza las noticias: título, subtítulo, firma del periodista, etc.
- En los mensajes que te lleguen por WhatsApp y similar párate a pensar antes de compartirlo: ¿ofrece el mensaje fuentes de información contrastada? ¿Puedo contrastar la información? No te fíes solo del destinatario.

3.2 Buenas prácticas aprendidas en la lección

- Antes de compartir información analiza su veracidad: ¿es fiable la fuente? ¿he comprobado en otro sitio que es real?
- Crear perfiles falsos o identidades digitales ficticias es muy fácil. Desconfía si no estás seguro
- Si alguien te molesta o acosa por Internet denuncia: habla con tus padres y profesores. Policía nacional y Guardia Civil están de tu parte y tienen cuerpos especializados en el cibercrimen
- Bloque o ignora las peticiones de amistad o los mensajes de remitentes desconocidos

3.3 Ampliaciones

- Aprende cómo activar las opciones de bloqueo de contactos en tu correo, servicio de mensajería o red social

Por último un consejo: en el mundo virtual deberíamos seguir el mismo criterio que usamos en el mundo real y sobre todo, aplicar el sentido común.