DIGITAL ACCESS

DIGITAL SKILLS FOR PEOPLE LIVING IN THE 3RD AGE
Effective Digital Access to Public Services

Erasmus+

PROYECTO DIGITAL ACCESS

MÓDULO DIDÁCTICO

Conocimientos básicos de seguridad online

Preparado por: AKLUB
Septiembre 2018

Este proyecto ha sido financiado con el apoyo de la Comisión Europea. Esta publicación refleja únicamente los puntos de vista de los autores, y la Comisión no puede ser responsable de cualquier uso que pueda hacerse de la información contenida en el mismo.

Contenido

HORAS DE APRENDIZAJE: [TODAS LAS UNIDADES HORAS DE APRENDIZAJE]

CARGA DE TRABAJO: [TODAS LAS UNIDADES HORAS DE APRENDIZAJE + TIEMPO TOTAL PARA LOS EJERCICIOS]

Resumen

Este módulo está diseñado para ofrecer el conocimiento básico al usuario sobre la seguridad online para un usuario principiante de Internet. Los objetivos principales de la unidad es enseñar al usuario cómo mantener la información personal segura, asegurando que sus datos online y sus activos digitales no se vean comprometidos.

Palabras clave

Seguridad online, información personal, contraseña, ciberacoso, caja fuerte de contraseñas

OBJETIVOS DEL MÓDULO

Acciones/logros		
Adquirir un entendimiento de las actividades delictivas basadas en Internet dirigidas a los individuos y la adquisición de las habilidades para identificar y evitar estas actividades.		
Conocimiento	**Habilidades**	**Competencias**
Seguridad online	Comprender la seguridad online Comprender los tipos de riesgos online La comprensión de las palabras clave básicas	Entender por qué es importante la seguridad online y cuáles son los riesgos online.
Información personal	¿Cuál es mi información personal Divulgar información personal online ¿Qué podría suceder si comparto mi información personal online ¿Cómo puedo proteger mi información personal	Ser capaz de entender cuáles son los datos personales, cuáles son los riesgos en el entorno online y ser capaz de proteger sus datos personales.

Contraseñas	Elegir la mejor contraseña Mantenimiento de sus contraseñas Acciones a tomar para proteger su autoprotegerse	Comprensión de la importancia de tener contraseñas fuertes. Crear y administrar contraseñas y cuentas de usuario.
La configuración de privacidad	Identificar el ciberacoso Estrategias El uso de almacenes de contraseñas Administración de cuentas de usuario	Comprensión de la importancia de tener contraseñas fuertes. Crear y administrar contraseñas y cuentas de usuario.

UNIDAD 1: seguridad online

Resultado

Entender por qué es importante la seguridad online y cuáles son los riesgos online.

Introducción

10 reglas básicas de seguridad online

1. Mantenga la información personal profesional y controladaa

Nadie necesita saber su estado personal o su domicilio. Pueden necesitan saber acerca de su experiencia y antecedentes profesionales, y de cómo ponerse en contacto con usted. Si no entregarías información puramente personal a individuos extraños, no la entregues a millones de personas online.

2. Mantenga su configuración de privacidad en ON

A los vendedores les encanta saber todo sobre usted, y también lo hacen los hackers. Ambos pueden aprender mucho de su navegación y su uso de medios sociales. Pero usted puede tomar el control de su información. Tanto los navegadores web como los sistemas operativos móviles, tienen configuraciones disponibles para proteger su privacidad online. Los principales sitios web como Facebook también tienen disponibles configuraciones de mejora de la privacidad. Estas configuraciones son a veces (deliberadamente) difíciles de encontrar porque las empresas quieren su información personal por su valor de mercado (marketing). Asegúrese de que ha habilitado estas salvaguardas de privacidad y manténgalas habilitadas.

3. Practique la navegación segura

Si no elegirías caminar por un barrio peligroso, no visites vecindarios peligrosos online. Los ciberdelincuentes utilizan el contenido lúdico como cebo. Saben que a veces las personas son tentadas por el contenido dudoso y pueden bajar la guardia cuando lo buscan. El submundo de Internet está lleno de trampas difíciles de ver, donde un clic descuidado podría exponer datos personales o infectar su dispositivo con malware. Al resistir el impulso, evitas dar una oportunidad a los hackers.

4. Asegúrese de que su conexión a Internet es segura

Cuando se está online en un lugar público, por ejemplo, mediante el uso de una conexión Wi-fi pública, no se tiene ningún control directo sobre su seguridad. Los expertos corporativos de ciberseguridad se preocupan por los "endpoints", los lugares donde una red privada se conecta al mundo exterior. Su punto de enlace vulnerable es su conexión a Internet local. Asegúrate de que t

u dispositivo esté seguro y, en caso de duda, espera un mejor momento (es decir, hasta que puedas conectarte a una red Wi-Fi segura) antes de proporcionar información como tu número de cuenta bancaria. Usted, aprenderá más sobre esto en el módulo intermedio.

5. Tenga cuidado con lo que descarga

Un objetivo principal de los ciberdelincuentes es engañarle para que descargue malware, programas o aplicaciones que llevan malware o intentan robar información. Este malware puede ser disfrazado como una aplicación: cualquier cosa, desde un juego popular a algo que informe del tráfico o del clima. No descargue aplicaciones que parecen sospechosas o provienen de un sitio en el que no confía.

6. Elija contraseñas seguras

Las contraseñas son uno de los puntos débiles más grandes en toda la estructura de seguridad de Internet, pero actualmente no hay manera de evitarlo. Y el problema con las contraseñas es que las personas tienden a elegirlas fáciles de recordar (como "contraseña" y "123456"), que también son fáciles de adivinar para los ladrones cibernéticos. Seleccione contraseñas seguras que sean más difíciles de descifrar para los ciberdelincuentes. El software de administrador de contraseñas puede ayudarte a administrar varias contraseñas para que no las olvides. Una contraseña segura es aquella que es única y compleja — al menos 15 caracteres de largo, mezclando letras, números y caracteres especiales. Hablaremos de esto más adelante en esta lección.

7. Haga compras online de sitios seguros

Cada vez que realice una compra online, debe proporcionar información de la tarjeta de crédito o de la cuenta bancaria, justo lo que los ciberdelincuentes están más ansiosos por tener en sus manos. Solo proporcione esta información a sitios que proporcionen conexiones seguras y cifradas. Como puede identificar sitios seguros buscando una dirección que comience con *https:* (el S significa *seguro*) en lugar de simplemente *http:* también pueden ser marcados por un icono de candado junto a la barra de direcciones.

8. Tenga cuidado con lo que publique

Internet no tiene una tecla de borrado. Cualquier comentario o imagen que publique online puede permanecer online para siempre porque eliminar el original (digamos, de Twitter) no elimina ninguna copia que otras personas hayan hecho. No hay forma de "recuperar" una observación que desearías no haber hecho. No pongas nada online que no quieras que tus parientes u otras personas vean.

9. Tenga cuidado con quien conoce online

Las personas que se reúnen online no siempre son quienes afirman ser. De hecho, puede que ni siquiera sean reales. Los perfiles FAKE (falsos) de redes sociales son una forma popular que usan los hackers para atrapar a los usuarios Web desprevenidos y coger sus monederos cibernéticos. Sea tan cauteloso y sensato en su vida social online como usted está lo es en su vida social en persona.

10. Mantenga su programa antivirus actualizado

El software de seguridad de Internet no puede protegerle contra cada amenaza, pero detectará y eliminará la mayoría del malware, aunque debe asegurarse de que esté actualizado. Asegúrese de mantenerse al día con las actualizaciones de su sistema operativo y las actualizaciones de las aplicaciones que utiliza. Proporcionan una capa vital de seguridad.

Ten en cuenta estas 10 reglas básicas de seguridad de Internet y evitarás muchas sorpresas desagradables que acechan online para los descuidados. En las próximas lecciones y módulos vamos a proporcionar más detalles para enseñarte cómo aplicar esas reglas en la práctica.

UNIDAD 2: información personal

Resultado

Ser capaz de entender cuáles son los datos personales, cuáles son los riesgos en el entorno online son y ser capaces de proteger sus datos personales.

¿Cuál es mi información personal?

Su información personal puede incluir:

Nombre completo
Dirección
Los números de teléfono
Escuela
Fecha de nacimiento
Dirección de correo electrónico
Nombre de usuario y contraseña
Datos bancarios y de tarjetas de crédito.

Divulgar información personal online

Muchos servicios online requieren que los usuarios proporcionen cierta información personal para poder usar su servicio. Antes de proporcionar información personal, debe pensar en lo que se puede hacer con su información personal y evaluar si todavía está contento de transmitir estos detalles. Además del uso inapropiado o ilegal de la información, divulgar información personal online puede afectar su reputación digital.
Hay varias actividades online que usted debe tener en cuenta que puede requerir un nivel de divulgación de información personal. Estos incluyen:

Compras: para verificar la identidad del comprador, para procesar los pagos o para la entrega de bienes.

Suscribirse o registrarse: un nombre de pantalla o identificación y una dirección de correo electrónico son a menudo requisitos mínimos, pero otra información solicitada puede incluir: edad, sexo, dirección, Foto y gustos personales o disgustos (un asterisco rojo (*) generalmente identifica los campos obligatorios que se necesitan para registrarse).

Concursos, premios y recompensas: a menudo requieren que los usuarios proporcionen datos personales extensos, incluidos los intereses personales y los detalles demográficos, a menudo utilizados por los vendedores para promocionar productos y servicios.

Juegos online y mundos virtuales: estos pueden requerir que los usuarios se registren antes de que puedan empezar a jugar.

¿Qué podría suceder si comparto mi información personal online?

El spam, las estafas, el robo de identidad y el fraude son solo algunos de los problemas más serios que podrías enfrentar si compartes información personal online.

¿Cómo puedo proteger mi información personal

Es importante comprender cómo se utiliza la información personal online y cómo proteger su información y su reputación digital.

Los siguientes consejos son una gran base para proteger su información personal online:

Solo divulgar información financiera en sitios Web seguros. Busque una dirección que comienza con https://y un símbolo de candado ' bloqueado ' en la parte inferior de la pantalla, lo que indica que los datos se cifran.

Si tiene dudas sobre la legitimidad de un sitio web, llame a la organización que pretende representar. El sitio web de SCAMwatch proporciona más consejos sobre cómo identificar y reportar posibles estafas.

Las instituciones bancarias nunca enviar por correo electrónico a las personas pidiendo su nombre de usuario o contraseña. Si recibe un correo electrónico de una organización que afirma representar a una institución bancaria, informe el correo electrónico al Banco y a SCAMwatch. No responda y no haga clic en ningún enlace proporcionado.

Leer acuerdos de usuario y políticas de privacidad. Muchas organizaciones utilizan la información con fines de marketing y pueden venderla a otras empresas de marketing. Si la información se publica en sitios web que venden información a los vendedores, las personas pueden recibir correos electrónicos promocionales de spam que pueden ser difíciles de detener.

Reduzca el spam protegiendo sus datos. El spam puede reducirse:

limitar la divulgación de direcciones de correo electrónico y números móviles

instalar y utilizar el software de filtrado de spam

comprobar los términos y condiciones al comprar productos, participar en concursos o registrarse para servicios o boletines informativos por correo electrónico

no permitir que los datos de contacto se utilicen con fines de marketing (asegurándose de que usted marque la casilla de exclusión)

aumentar la seguridad online para limitar el spam.

Comprenda que la información compartida online puede ser permanente: es posible que los usuarios no tengan control sobre quién ve o accede a su información personal.

Seleccione las contraseñas cuidadosamente. Al crear contraseñas hay algunos dos y no hacer, estos incluyen:

hacer

usar ocho caracteres o más
usar una combinación de palabras que no son predecibles
usar la autenticación de dos factores en cuentas que contengan información personal.

No
usar nombres de mascotas, fechas de nacimiento, nombres de familiares o amigos
usar una combinación predecible de palabras (p. ej. ' ilovehiking '), una palabra específica del contexto (por ejemplo. ' Google ') o caracteres secuenciales repetidos (p. ej. ' Aaaaaa ' o ' 123456 ')
compartir contraseñas con otros, incluso con amigos

almacenarlos en su dispositivo, a menos que sea a través de un administrador de contraseñas que los almacena en una base de datos cifrada. estafas de hreat y extorsión incluyen ' ransomware ', ' malware ' y ' hit man ' estafas. Ransomware y estafas de malware pueden implicar software dañino que se coloca en su ordenador. Esto puede dar acceso a los delincuentes a su información personal, lo que puede resultar en la pérdida de datos o impedir el acceso a sus programas y archivos. Los estafadores entonces exigen el pago antes de permitirle acceder a su ordenador de nuevo.

UNIDAD 3: Contraseñas

Resultado

Conocer los fundamentos de creación y mantenimiento de contraseñas.

Introducción

Sus contraseñas son la forma más común de probar su identidad cuando se utilizan sitios web, cuentas de correo electrónico y su propio ordenador (a través de cuentas de usuario). Por lo tanto, el uso de contraseñas seguras es esencial para proteger su seguridad e identidad. La mejor seguridad en el mundo es inútil si una persona maliciosa tiene un nombre de usuario legítimo y contraseña.

Las contraseñas se utilizan comúnmente junto con su nombre de usuario. Sin embargo, en sitios seguros también se pueden utilizar junto con otros métodos de identificación, como un PIN separado y/o información memorable. En algunos casos, también se le pedirá que introduzca solo ciertos caracteres de su contraseña, para mayor seguridad.

El riesgo de usar contraseñas débiles y no tener una contraseña separada para su cuenta de correo electrónico

Personas que se hacen pasar por cometer fraudes y otros delitos, entre ellos:
Acceder a su cuenta bancaria
La compra de artículos online con su dinero
Haciéndose pasar por usted en redes sociales y sitios de citas
Enviar correos electrónicos a su nombre
Acceder a la información privada que se mantiene en su ordenador

Elegir las mejores contraseñas

Qué HACER:

Utilice siempre una contraseña.

Utilice una contraseña fuerte y separada para su cuenta de correo electrónico.

Para crear una contraseña segura, simplemente elija tres palabras aleatorias. Los números, los símbolos y las combinaciones de mayúsculas y minúsculas se pueden utilizar si usted cree que necesita crear una contraseña más fuerte, o si la cuenta para la que está creando una contraseña requiere más que sólo letras.

Hay alternativas, sin reglas duras y rápidas, pero podrías considerar las siguientes sugerencias:
Elige una contraseña con al menos ocho caracteres (más si puedes, ya que las contraseñas más largas son más difíciles de adivinar o romper por los delincuentes), una combinación de letras mayúsculas y minúsculas, números y símbolos de teclado como @ # $% ^ & * () _ +. (por ejemplo, SP1D3Rm @ n – una variación de Spiderman, con letras, números, mayúsculas y minúsculas). Sin embargo, tenga en cuenta que algunos de estos signos de puntuación pueden ser difíciles de introducir en los teclados extranjeros. También Recuerde que el cambio de letras a números (por ejemplo, E a 3 y I a 1) son técnicas bien conocidas por los delincuentees.

Una frase de una canción que otras personas no asociarían contigo.

El apellido de soltera de la madre de otra persona (no el apellido de soltera de tu madre).

Escoge una frase conocida para ti, por ejemplo 'vagabundos como nosotros, nacimos para correr ' "y tomar el primer carácter de cada palabra para conseguir ' VCN, NPC '

NO HACER:

No utilice lo siguiente como contraseñas:
Nombre de usuario o nombre de empresa.

Nombres de miembros de la familia o mascotas.

Cumpleaños de tu familia.

Equipo de fútbol favorito o de F1 u otras palabras fáciles de conseguir con un poco de conocimiento de base.

La palabra "Password".

Secuencias numéricas.

Una sola palabra del diccionario común, que podría ser descubierta por los programas de piratería corrientes.

Al elegir códigos de acceso numéricos o PIN, no utilice números ascendentes o descendentes (por ejemplo 4321 o 12345), números duplicados (como 1111) o patrones de teclado fácilmente reconocibles (como 14789 o 2580).

¿Estás buscando tus contraseñas

Nunca divulgue sus contraseñas a nadie más. Si cree que alguien más conoce su contraseña, cámbiela inmediatamente.
No ingrese su contraseña cuando otros puedan ver lo que escribe.
No se recomienda el cambio rutinario de contraseñas, a menos que las cuentas a las que se apliquen hayan sido hackeadas, en cuyo caso deben cambiarse inmediatamente. Esto también se aplica si se ha hackeado otra cuenta o sitio web para el que utilizas los mismos datos de acceso.

Utilice una contraseña diferente para cada sitio Web. Si usted tiene sólo una contraseña, un delincuente simplemente tiene que romperlo para obtener acceso a todo.
No Recicle las contraseñas (por ejemplo, password2, password3).
Si debe escribir las contraseñas para recortarlas, encriptelas de una manera que le resulte familiar, pero que las haga indescifrables por otros.
Una alternativa a la escritura de contraseñas es usar un almacén de contraseñas online o seguro. Busque recomendaciones sobre esos almacenes y asegúrese de que el que elija sea seguro y de buena reputación.
No envíe su contraseña por correo electrónico.

El hecho de que usted deba utilizar diferentes contraseñas para cada una de sus cuentas puede hacer que sean muy difíciles de recordar. Considere usar uno de los muchos almacenes de contraseñas disponibles en Internet, pero lea las reseñas y obtenga recomendaciones.

Cajas fuertes de contraseñas.

Hay una serie de almacenes de contraseñas (también conocidos como cajas de contraseñas - password vaults) disponibles para su uso -algunas de pago, algunas de gratuitas. Estos le permiten almacenar todas sus contraseñas en una ubicación de fácil acceso para que no tenga que recordarlas todas, o escribirlas. Sólo tiene que recordar un conjunto de detalles de inicio de sesión.

Debe leer opiniones u obtener recomendaciones personales antes de introducir sus contraseñas en un almacén de contraseñas. Cualquiera que usted elija, nuestra recomendación es que cuente con la autenticación de dos factores (2FA)-en otras palabras, envía un código a su teléfono móvil u otro dispositivo, que necesita para entrar en el almacén de contraseñas con el fin de obtener acceso, al igual que cuando se confirma una pago bancario online.

Controlar cuentas de usuario

Todos los que usan un equipo deben tener asignada su propia cuenta de usuario para que solo ellos puedan acceder a sus archivos y programas. Cada cuenta de usuario debe ser accesible sólo introduciendo un nombre de usuario y contraseña con el fin de salvaguardar la privacidad de los usuarios.

No utilice una cuenta con privilegios de administrador para el uso diario, ya que el malware podría asumir derechos de administrador. Incluso si eres el único usuario, configura una cuenta de administrador para usarla cuando necesites realizar tareas como instalar programas o cambiar la configuración del sistema, y otra cuenta de "usuario estándar" como cuenta normal. Si no ha iniciado sesión como administrador, se le solicitará que introduzca una contraseña de administrador al instalar un nuevo controlador de dispositivo o programa.

UNIDAD 4: Configuración de privacidad

Resultado

Ayudar a un usuario gestionar sus perfiles de privacidad.

La privacidad del ordenador

Eche un vistazo a la configuración de privacidad ofrecida en su navegador (generalmente se encuentra en el menú herramientas) para ver si puede afinar para mantener el bien y bloquear el mal. Cuando usted trabaja online, los sitios web instalan cookies en su ordenador que rastrean sus movimientos. Algunas cookies pueden ser beneficiosas, como las que recuerdan sus nombres de usuario o artículos en su carrito de compras online. Pero algunas cookies están diseñadas para recordar todo lo que haces online, crear un perfil de tu información personal y hábitos, y vender esa información a los anunciantes y otras empresas.

Ejemplo de configuración de Internet Explorer

Para proteger su equipo de intrusiones o de virus que podrían dañar su sistema, debe saber cómo cambiar la configuración de privacidad en Internet Explorer. Al cambiar la configuración de privacidad, decide a qué tipos de sitios puede acceder Internet Explorer y de qué tipos de sitios desea proteger su equipo.

1. Abra Internet Explorer, elija Herramientas → Opciones de Internet y haga clic en la pestaña privacidad.

2. Arrastre la barra deslizante hacia arriba y hacia abajo para ver los diferentes niveles de configuración de seguridad.

   En cada nivel, Internet Explorer le dará información sobre esa configuración de seguridad específica.

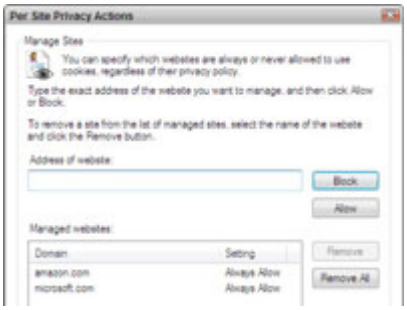
3. Lea las opciones y seleccione un ajuste que le convenga.

   Si no sabes qué elegir, Medium es una buena opción para empezar. Si eso no parece bloquear lo suficiente, siempre se puede aumentar el nivel de seguridad.

4. Haga clic en el botón sitios para especificar sitios que siempre deben o nunca deben estar autorizados a usar cookies.

   Se abre el cuadro de diálogo acciones de privacidad por sitio, que le permite invalidar la configuración general que eligió con el control deslizante.

Introduzca un sitio en el cuadro dirección del sitio web y haga clic en bloquear o permitir.



Haga clic en permitir para sitios en los que sepa que siempre puede confiar, y haga clic en bloquear para sitios que sepa que nunca puede confiar (como www.ComputerDemolishingDownloads.com).

5. Haga clic en Aceptar para guardar la nueva configuración.

Volverá al cuadro de diálogo Opciones de Internet.

6. Ajuste el bloqueador de elementos emergentes y haga clic en Aceptar cuando termine.

Puede activar y desactivar el bloqueador de ventanas emergentes desde aquí, y puede permitir que ciertas ventanas emergentes de sitios web aparezcan, a través del bloqueador haciendo clic en el botón configuración. Agregue sitios aquí de la misma manera que agregó sitios en el cuadro de diálogo acciones de privacidad por sitio.

Privacidad smartphone

La configuración de los smartphones varía, pero puedes reforzar la privacidad con estas precauciones:

Desactive los servicios de ubicación. Lo que impide que las aplicaciones rastreen su ubicación.

No permita que las aplicaciones compartan datos. Algunas aplicaciones quieren usar la información almacenada en su teléfono (su lista de contactos, por ejemplo). Diga que no.

Habilite la configuración de privacidad en las aplicaciones que descargue. Asegúrese de que está utilizando la configuración de privacidad estricta en servicios tales como Instagra o myFacebook.

Tenga cuidado con los inicios de sesión sociales. Cuando inicie sesión en un sitio con su Facebook o Google (nombre de usuario y contraseña), puede estar permitiendo que la aplicación pueda acceder a cierta información de su perfil. Lea la letra pequeña para saber lo que está compartiendo.

Ejercicios

¿Qué es su Privacy IQ? ¡Rellene nuestro cuestionario y averiguelo!

https://blog.avast.com/2014/01/27/what-is-your-privacy-iq-take-our-quiz-and-find-out-2/

Juego online de ciberseguridad

NOVA ha unido fuerzas con expertos en ciberseguridad para crear su laboratorio de ciberseguridad. Este es un juego en el que los jugadores descubren cómo pueden mantener su vida digital segura. El juego ayuda a los jugadores a desarrollar una comprensión de las amenazas cibernéticas comunes que existen online y sus defensas.

https://www.pbs.org/wgbh/nova/labs/lab/cyber/

La peor lista de contraseñas

MÁS LECTURAS Y RECURSOS

Los términos que debe conocer

https://www.lifewire.com/top-internet-terms-for-beginners-2483381

planificación de seguridad en Internet para personas mayores

(descarga en PDF)

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=18&cad=rja&uact = 8 & ved = 2ahUKEwiz8LGAjNjdAhVSGsAKHbISB8QQFjARegQIBxAC & URL = https% 3A% 2F% 2Fvict imserviceslanark. CA% 2Fphotos% 2Fcustom % 2FVSLG% 2FResources% 2FSafetyPlanningForSe niors English. pdf & USG = AOvVaw3WNu9papw-5PbHbhKSxVFi

Las reglas de seguridad de Internet

https://usa.kaspersky.com/resource-

center/preemptive-safety/top-10-internet-safety-

rules-and-what-not-to-do-online

Cómo mantenerse seguro online para las personas mayores – video de YouTube

https://www.youtube.com/watch?v=HGHxRNT6PjU

Seguridad online para personas mayores https://www.connectsafely.org/seniors/

Más información de seguridad online

https://www.protectseniorsonline.com/resources/