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

Escenario 1
Tecnología y TI

BRinging STEM into Active agINg – BRAIN

Erasmus+ 2020-1-PL01-KA204-081805

Nombre del socio: Foro de Formacion y Ediciones

Open Educational Resources

Este material se ha creado en el marco del proyecto BRAIN "BringING STEM into Active AgING" (CONVENIO DE SUBVENCIÓN 2020-1-PL01-KA204-081805. Este proyecto ha sido financiado con el apoyo de la Comisión Europea. Esta publicación refleja únicamente las opiniones del autor, y la Comisión no se hace responsable del uso que pueda hacerse de la información aquí difundida.

Akademia WSEI LUBLIN

Mine Vaganti NGO

FFE Foro de Formación y Ediciones S.L.

HORIZONT X PROCONSULT

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

Filtración de datos personales, creación de contraseñas seguras, organizadores de contraseñas

BRinging STEM into Active agINg – BRAIN

Erasmus+ 2020-1-PL01-KA204-081805

Nombre del socio: Foro de Formacion y Ediciones

Akademia WSEI
Mine Vaganti NGO
FFE Foro de Formación y Ediciones S.L.
Horizont X Proconsult

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

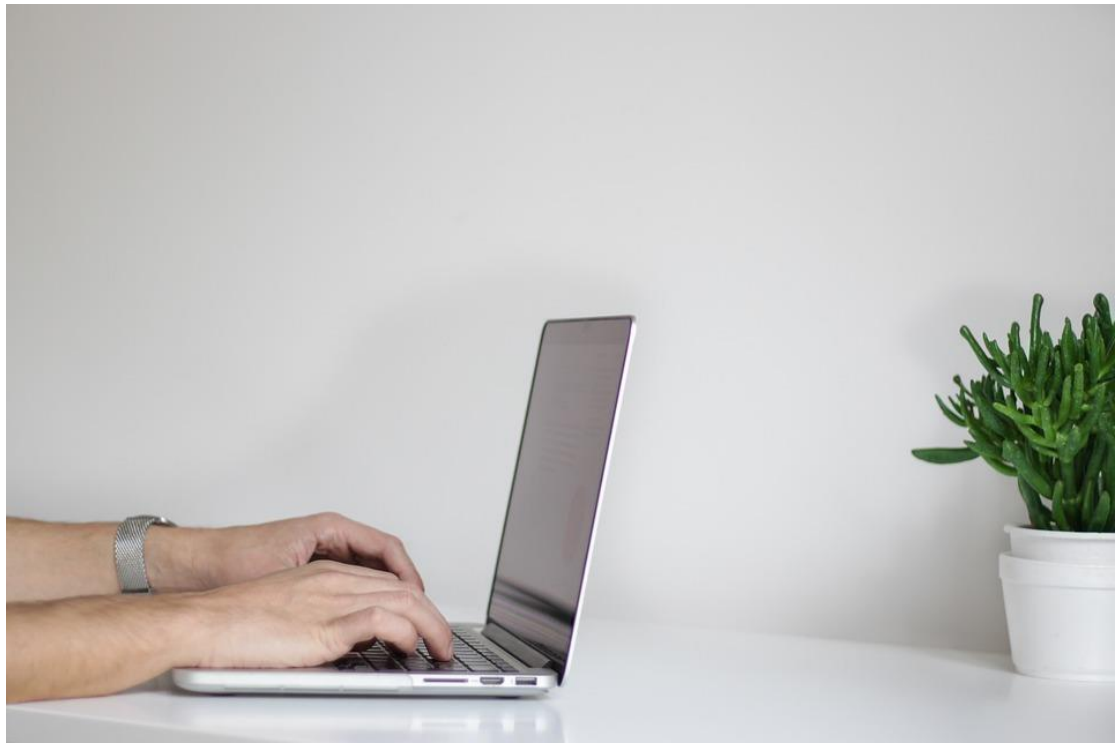
Ice Breaker

Pon al grupo en círculo. Empieza diciendo tu nombre y una palabra relacionada con las TI que empiece por la misma letra. Por ejemplo: Adam Application, Bartek Banner, Celine Cookies, Darek Domain, etc....
A continuación, la siguiente persona dice su nombre y el tuyo. A continuación, la tercera persona hace el suyo, el del segundo y el nombre del primero y una palabra relacionada con la informática. Se pueden hacer diferentes variaciones, pero es ideal para que el grupo se conozca y sepa los nombres.

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

Introducción

Internet se ha convertido en un factor determinante para el desarrollo de la sociedad actual. Se ha utilizado como principal medio para la interacción de personas y ordenadores, intercambiando información y fomentando la rápida transmisión de experiencias y conocimientos con independencia de la ubicación geográfica.



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

Introducción

Desde sus inicios en los años 60 hasta la actualidad, Internet ha sido un ingrediente fundamental para el desarrollo tecnológico, la educación, las comunicaciones, la medicina, la ciencia, el arte y prácticamente todas las disciplinas y profesiones. en un mundo globalizado. Aunque en un principio se pensó para uso militar, sus beneficios se extendieron radicalmente a prácticamente cualquier ámbito.

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

Introducción

El comercio es otro espacio en el que internet ha conseguido tener un impacto positivo, tanto para el vendedor como para el comprador. Los grandes supermercados y cadenas de tiendas, además de tener sus puntos de venta, han desarrollado plataformas para la venta online, consiguiendo abaratar algunos costes como el personal de ventas y las ubicaciones, por ejemplo. El comercio electrónico permite a las empresas cruzar fronteras sin necesidad de estar físicamente en un mismo lugar. Esto ha redundado en la eficiencia empresarial y ha abierto nuevas vías de comercio.

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

Introducción

Además, el comercio electrónico ya no es exclusivo de las grandes marcas. Su versatilidad ha permitido que pequeñas y medianas empresas también se aventuren en este negocio, y las redes sociales han contribuido de forma interesante a esta dinámica.

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

Introducción

Internet es hoy, por tanto, un medio de comunicación global que nos permite interactuar en diferentes espacios. Desde comunicarnos a través de una videollamada o un chat con otra persona a miles de kilómetros de distancia, acceder a una educación de calidad en institutos y universidades de diferentes partes del mundo, comprar productos o servicios online, leer periódicos, revistas o libros, escuchar música, ver películas o interactuar en las redes sociales. Esto, por mencionar sólo algunas de las muchas posibilidades que nos ofrece.

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

Introducción

Está en nuestras manos hacer un uso racional y objetivo de una herramienta tan poderosa como nos gustaría que fuera.

La forma en que Internet ha evolucionado desde su invención es fantástica y nos ha dejado ver que seguirá evolucionando tan rápido que no dejará de sorprendernos.

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

Noticias falsas: es decir, buscar en Internet y verificar la información proporcionada por los medios de comunicación. Rotafolios de noticias falsas

Materiales

teléfonos/tabletas/ordenadores portátiles con acceso a Internet, retroproyector, bolígrafos, rotuladores, rotafolios, notas adhesivas, hojas de papel A4

Cómo llegar

El presentador escribe el término "FAKE NEWS" en el centro del rotafolio. Distribuye 3 notas adhesivas a los participantes y pídeles que escriban sus asociaciones con el término y las peguen en el rotafolio. Lee las asociaciones escritas, agrupándolas si es posible. Discuta cada asociación y compárela con la definición de fake news (anexo).

Anexo

El término "Fake news

Las fake news son "noticias falsas, no veraces, generalmente difundidas por la prensa sensacionalista para causar sensación o difamar a alguien (normalmente un político)". El Diccionario de Cambridge dice que son (traducido) "historias falsas que parecen ser noticias, difundidas en Internet o a través de otros medios, generalmente creadas para influir en opiniones políticas o como broma".

Noticias falsas: es decir, buscar en Internet y verificar la información proporcionada por los medios de comunicación.
Rotafolios de noticias falsas

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

El término "fake news" (noticias falsas) es un neologismo y resulta difícil situarlo en un marco de definición. Denota noticias de los medios de comunicación que no son ni verdaderas ni falsas al mismo tiempo y que se basan en la desinformación, incluyendo a menudo partes verdaderas. Las noticias falsas suelen basarse en la desinformación o en una broma, y a menudo contienen elementos verdaderos. Las noticias falsas pueden simular ser información real, artículos, publicaciones en redes sociales, memes, etc. Pueden crearse con diversas intenciones, desde el engaño, a herramientas de propaganda, para crear sensacionalismo, a una broma.
Las noticias falsas son "una manipulación de los hechos, utilizada con avidez por periodistas cuyo objetivo, al preparar una publicación, es suscitar el mayor interés posible por el tema, y no su conformidad con la realidad". Internet es actualmente la fuente de comunicación más popular. Sin embargo, los contenidos que se publican en ella deben abordarse con cautela. El estudio de IAB "Desinformación en la Red. Análisis de la credibilidad de los canales de información" muestra que las redes sociales son líderes en la difusión de noticias falsas. En segundo lugar están los portales de Internet.

Tipos de noticias falsas:
falsedad total: la información facilitada es falsa y contradictoria,
la verdad es discutible - los hechos se presentan de forma selectiva o en el contexto adecuado, lo que da lugar a engañar al receptor,
Manipulación de citas - se coloca el enunciado en el contexto adecuado o se eliminan frases o sus fragmentos, lo que cambia el sentido del enunciado y, en consecuencia, apoya la tesis específica.

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

Noticias falsas: es decir, buscar en Internet y verificar la información proporcionada por los medios de comunicación.
Vídeos de noticias falsas

Materiales

teléfonos/tabletas/ordenadores portátiles con acceso a Internet, retroproyector, bolígrafos, rotuladores, rotafolios, notas adhesivas, hojas de papel A4

Cómo llegar

Utilizando un retroproyector, el presentador muestra cortometrajes sobre qué son las noticias falsas y cómo reconocerlas.
Cómo pueden difundirse las noticias falsas - Noah Tavlin (inglés, subtítulos disponibles en otros idiomas)
https://www.youtube.com/watch?v=cSKGa_7XJkg
Cómo elegir sus noticias - Damon Brown (inglés, subtítulos disponibles en otros idiomas)
https://www.youtube.com/watch?v=q-Y-z6HmRgI
Presentar al grupo los elementos gracias a los cuales se pueden reconocer las noticias falsas, distinguirlas de la información real (anexo a continuación).

Anexo

INTERPRETACIÓN DEL MATERIAL ORIGINAL:
- prestar atención al lenguaje emocional, a las descripciones brutales
- sea consciente de sus propios prejuicios
- hacer preguntas sobre el material (¿quién es el autor? ¿es coherente el mensaje? ¿confirman otras fuentes la información? etc.)

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

Noticias falsas: es decir, buscar en Internet y verificar la información proporcionada por los medios de comunicación.
Vídeos de noticias falsas

- prestar atención a si las imágenes utilizadas se sitúan en un contexto real
Comprobar la credibilidad del sitio web: si la URL es correcta y conduce al sitio web auténtico.
- comprobar la fecha y la actualidad de la información
- verificar al autor: si es creíble, cuáles son sus objetivos e intenciones, si ya ha publicado otros materiales en línea
- comprobar que las imágenes no tienen un aspecto extraño o no han sido manipuladas; esto puede hacerse, por ejemplo, utilizando la opción de búsqueda inversa de imágenes disponible en los motores de búsqueda

FAKE NEWS - NORMAS GENERALES:
En ellos predominan las imágenes/fotos y los textos breves.
El mensaje tiene una fuerte carga emocional: utiliza expresiones de odio, muestra escenas e imágenes violentas y conmovedoras.
A menudo pretende ser de primera mano.
Utilizan verdades y creencias generalmente conocidas.
A menudo muestran medias verdades, tergiversan los hechos de tal manera que es imposible saber dónde empieza y dónde acaba la información verificada. Se basan en el supuesto de que una verdad parcial confirma la verdad del todo.
A veces describen hechos reales pero cambian su contexto.
Casi siempre incluyen fotos o vídeos que ayudan a aumentar la cobertura rápidamente.
No comunican que la información facilitada puede no ser cierta.
Evitan los matices y los puntos de vista diferentes.

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

Hora de preguntar...

¿Qué puede decirme sobre la privacidad en Internet?

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

Hora de responder...

La definición de privacidad en línea es el nivel de protección de la privacidad que tiene un individuo mientras está conectado a Internet. Abarca el grado de seguridad en línea disponible para los datos personales y financieros, las comunicaciones y las preferencias. La privacidad en Internet es importante porque permite controlar la identidad y la información personal. Sin ese control, cualquiera con la intención y los medios puede manipular su identidad para servir a sus objetivos, ya sea venderle unas vacaciones más caras o robarle sus ahorros.

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

La importancia de las contraseñas

Las contraseñas son la llave que abre la puerta al uso de todos nuestros servicios. Si nuestras contraseñas quedan al descubierto, los ciberdelincuentes podrían utilizarlas para entrar en ellos y suplantar nuestra identidad, realizar pagos en nuestro nombre, cambiar o acceder a otro tipo de información o a otras personas, entre otras cosas, por lo que es recomendable tomar una serie de medidas para nuestra protección.

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

La importancia de las contraseñas

Una contraseña debe ser fuerte, con un mínimo de 8 caracteres y estar compuesta por:

-Mayúsculas (A, B, C...)

-Números (1, 2, 3...)

-Minúsculas (a, b, c...)

-Caracteres especiales ($, &, #...)

Es importante utilizar contraseñas que no sean fáciles de adivinar. Por ejemplo: "123456789", "qwerty", "aaaaa", nombres propios, cumpleaños, etc.

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

La importancia de las contraseñas

Las contraseñas no deben compartirse con nadie, una contraseña debe pertenecer exclusivamente al usuario que la crea y solo ser utilizada por él. Compartirla nos hará vulnerables y más si el medio por el que la compartimos es una red de mensajería como (WhatsApp, Telegram, Facebook), ya que la información se almacena en los servidores de estos servicios.

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

La importancia de las contraseñas

Intenta evitar a toda costa utilizar la misma contraseña para todos los servicios, ya que si un ciberdelincuente se hace con ella, podrá acceder a todos ellos.

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

La importancia de las contraseñas

Cambie las contraseñas periódicamente y no una permanente para siempre. Una buena forma de recordar cuándo debemos cambiar nuestras contraseñas es tener en cuenta las estaciones del año. Un cambio de contraseña para cada estación, por lo que siempre se actualizaría cada 3 meses.

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

La importancia de las contraseñas

Como consejo al gran número de contraseñas que habría que gestionar en caso de tener una por servicio, existen gestores de contraseñas que facilitan la vida a la hora de recordarlas todas.

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

Autenticación en 2 pasos

A veces, tener una contraseña no es suficiente, por muy segura que sea, o después de seguir todos los pasos anteriores.

Los ciberdelincuentes podrían hacerse con ellos a través de diferentes técnicas como el "phishing" o algunos virus diseñados para ello que veremos más adelante.

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

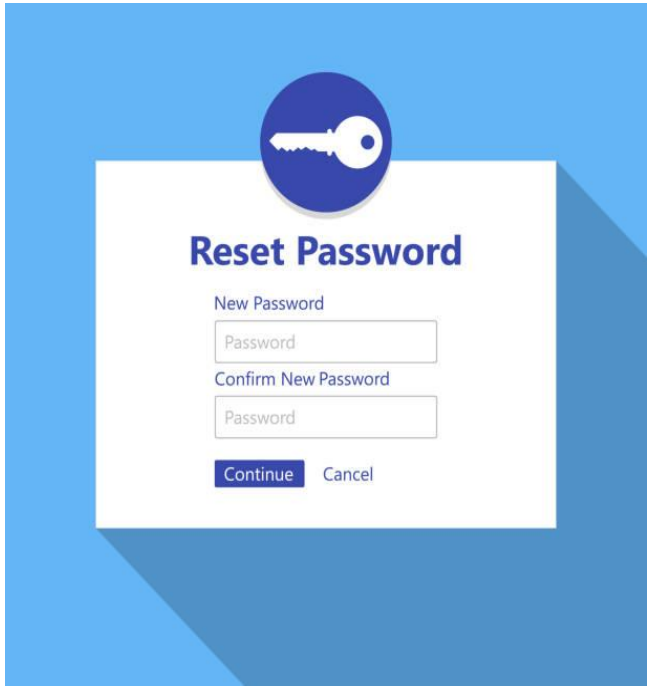
Autenticación en 2 pasos

Por eso muchos servicios ya ofrecen la autenticación en dos pasos. Con este método usaremos la contraseña de nuestro servicio de forma normal y luego nos pedirá que añadamos un segundo código. La forma más habitual de recibir este código es recibirlo en forma de SMS a nuestro Smartphone, aunque también puede ser una llamada telefónica a través de un contestador automático o disponiendo de una app de servicio que cambie activamente los códigos cada 5 minutos.

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

Autenticación en 2 pasos

Evidentemente, el servicio ha tenido que ser configurado previamente para vincular nuestro smartphone a él y recibir los códigos. De esta forma, aunque el ciberdelincuente obtenga tu contraseña, no podrá acceder al servicio ya que necesitará este segundo código para entrar.



Si en algún momento te encuentras con un intento de acceso a tu cuenta porque has recibido el código de doble autenticación y no eras tú, deberías plantearte cambiar la contraseña, ya que es muy probable que ya no sea una clave segura.

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

Hora de preguntar...

¿Qué es Spying / snooping?

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

Hora de responder...

Cuando usted está en línea, es espiado por una serie de rastreadores con diversos fines. Los rastreadores mantienen un registro de su historial de búsqueda y rastrean todas sus actividades en línea a través de diversos medios. Esto les proporciona una imagen clara de quién es usted y de sus intereses, lo que supone una violación de la política de privacidad en línea y le convierte en una propiedad pública. La mayoría de las veces, este rastreo sólo tiene fines publicitarios y permite a los anunciantes mostrar anuncios acordes con sus gustos e intereses. Pero a veces esta información es utilizada por ciberdelincuentes para llevar a cabo actividades no autorizadas e ilegales que ponen en peligro tu existencia en Internet.

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

Datos personales

Antes de facilitar sus datos personales, debe analizar quién se los pide... ¿para qué necesita esa información? La información que tendrá que facilitar, por ejemplo, para contratar una cuenta bancaria, no es la misma que para suscribirse a un sitio web de compras en línea. En el primer caso, la información requerida será sustancialmente amplia, pero en el segundo bastaría con el nombre, apellidos, dirección de entrega, datos de facturación y forma de pago.

Si alguien solicita tus datos personales, debes informarte sobre la finalidad, para qué los van a utilizar, así como su tratamiento y cuánto tiempo van a conservar tus datos. Es útil saber cómo ejercer sus derechos (Acceso, Rectificación, Oposición, Limitación del tratamiento y Portabilidad).

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

Phishing

El phishing es la suplantación de identidad de un servicio o empresa para intentar estafar a la gente. Por ejemplo, podría recibir un correo electrónico pidiéndole que actualice sus datos bancarios porque su tarjeta de crédito está a punto de caducar. En este correo electrónico viene un enlace para acceder a este servicio. Al abrirlo, aparece una página web que es una copia de la original, el usuario actualiza los datos de su cuenta bancaria y es entonces cuando ha caído en el engaño.

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

Phishing

Consejos para evitar ser víctima

1. Desconfíe de correos electrónicos que aparenten ser de entidades bancarias o servicios conocidos con mensajes del tipo:

a. Problemas técnicos de la entidad

b. Problemas de seguridad en la cuenta de usuario.

c. Recomendaciones de seguridad para evitar el fraude.

d. Cambios en la política de seguridad de la entidad

e. Promoción de nuevos productos

f. Vales de descuento, premios o regalos

g. Cese inminente o desactivación del servicio.

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

Phishing

2. Sospecha si hay errores gramaticales en el texto.

3. Si recibe comunicaciones anónimas dirigidas a "Estimado cliente" o "Notificación de usuario" es un indicio que debe alertarle.

4. Si el mensaje te obliga a tomar una decisión en pocas horas, es mala señal. Contrasta directamente si la urgencia es real o no con el servicio a través de otros canales.

5. Compruebe que el texto del enlace coincide con la dirección a la que apunta.

6. Un servicio de confianza utilizará sus propios dominios para las direcciones de correo electrónico corporativas. Si recibes la comunicación desde un buzón tipo @gmail.com o @hotmail.com, no es buena señal.

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

Phishing

Qué debe hacer si detectamos un caso de phishing

1. No responda a estos correos electrónicos bajo ningún concepto. Si tiene dudas, pregunte directamente a la empresa o servicio que representa.

2. No acceda a los enlaces proporcionados en el mensaje ni descargue ningún documento adjunto.

3. Borra el mensaje y alerta a tus contactos sobre el fraude.

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

Hora de preguntar...

¿Qué sabe sobre el tratamiento incorrecto de la información?

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

Hora de responder...

Hay varios sitios en Internet que necesitan tus datos personales para acceder a sus servicios. Estos sitios a menudo almacenan cookies y guardan su información personal para luego utilizarla con diversos fines. La mayoría de las veces esta información no está cifrada y cualquiera puede acceder a ella. Este mal uso de la información personal puede acarrear graves consecuencias. La tendencia moderna de los portales de banca y comercio electrónicos ha multiplicado los riesgos asociados a la privacidad en línea. Al compartir sus datos bancarios y archivos cruciales en Internet, está allanando el camino a los ladrones y haciéndose vulnerable a los ciberdelincuentes.

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

Filtración de datos personales, creación de contraseñas seguras, organizadores de contraseñas
Juego: Dos verdades y una mentira

Materiales

Teléfonos/tabletas/portátiles con acceso a Internet, proyector, hojas de papel, bolígrafos, cartulinas

Cómo llegar

Juego Dos verdades y una mentira. Los participantes reciben tres afirmaciones. Dos serán verdaderas y una será mentira. Los participantes deben identificar la mentira.

Anexo

A los participantes se les dan tres afirmaciones. Dos serán verdaderas y una será mentira. Los participantes deberán identificar la mentira. Todas las afirmaciones estarán relacionadas con temas de Internet.

Compras en línea:

1. La tarjeta de crédito es una de las formas más peligrosas de pagar en Internet
2. Nunca debe introducir sus datos de pago en una página a menos que haya una S después de HTTP
3. Si no dispone de tarjeta de crédito o débito, PayPal es una buena alternativa para pagar productos en Internet.

Malware:

1. El malware es un tipo de virus informático
2. Un gusano informático suele aprovecharse de ordenadores con software obsoleto.
3. Un paso importante para protegerse del ransomware son las copias de seguridad periódicas

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

Filtración de datos personales, creación de contraseñas seguras, organizadores de contraseñas

Juego: Dos verdades y una mentira

Phishing:

1. Si un correo electrónico se dirige a usted como "cliente", debe desconfiar especialmente de él
2. Una estafa de phishing que conoce datos personales pertinentes para el destinatario se denomina ataque de spear-phishing
3. Hacer clic en un enlace de un correo electrónico es correcto si procede de un banco en el que tiene una cuenta.

Privacidad en las redes sociales:

1. El único nivel de privacidad recomendado por defecto es SÓLO amigos y familiares.
2. Instalar aplicaciones de redes sociales (Facebook, Instagram, Twitter...) puede dar acceso a desconocidos a cierta información sobre ti.
3. Si bloqueo a alguien en Facebook o Twitter, esa persona no podrá ver nada de lo que haga o publique en mi cuenta.

Estafa en Facebook:

1. Añadir a un desconocido en Facebook le da acceso a mi ordenador
2. Añadir a un desconocido en Facebook podría poner en peligro a mis amigos
3. Añadir a un desconocido en Facebook podría conducir a un robo de identidad

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

Filtración de datos personales, creación de contraseñas seguras, organizadores de contraseñas
Juego: Dos verdades y una mentira

Estafas por correo electrónico:

1. Las estafas por correo electrónico consisten en engañar a la víctima para que envíe dinero con la promesa de un beneficio mucho mayor.
2. Abrir un archivo adjunto de correo electrónico que contenga un documento de Word puede ser peligroso.
3. Lo mejor que puedo hacer si recibo un correo electrónico fraudulento de un "príncipe nigeriano" es responder y decirles que dejen de enviarme correos electrónicos.

Ransomware

1. Si el ransomware infecta mi ordenador, un programa antivirus fiable y de buena reputación puede eliminarlo.
2. Los antivirus pueden revertir los efectos del ransomware
3. El ransomware es una de las amenazas online más prolíficas de 2017 y 2018

Después de estos ejemplos, los participantes tendrán que pensar en al menos uno más cada uno. A continuación, intentarán averiguar qué afirmación es incorrecta.

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

Filtración de datos personales, creación de contraseñas seguras, organizadores de contraseñas
Juego: Dos verdades y una mentira

Respuestas:

1

3

3

1

1

3

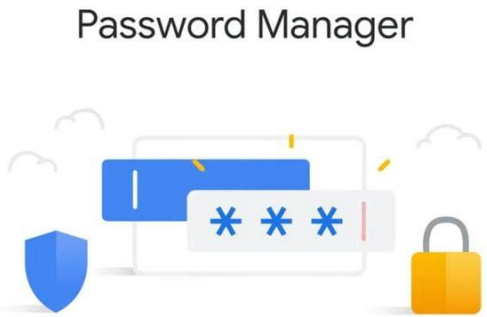
2

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

Gestores de contraseñas

Disponer de una versión gratuita de un gran gestor de contraseñas

siempre es mejor que no tener ninguno.



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

Gestores de contraseñas

1Password: gran opción familiar ➞ https://cnews.link/get-1password_7/

==========

Contras del plan gratuito:

✓ Comprobación de contraseñas comprometidas

✓ Asistencia por correo electrónico 24/7

✓ Usuarios ilimitados para una cuenta

✓ Opción de almacenamiento local

1Password

Limitaciones del plan gratuito:

✗ No hay asistencia por chat en directo

✗ No hay actualizaciones de contraseñas con un solo clic.

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

Gestores de contraseñas

NordPass: el gestor de contraseñas más versátil ➞ https://cnews.link/get-nordpass_46/

==========

Ventajas del plan gratuito:

Cifrado de última generación

Almacenamiento ilimitado de contraseñas

✓ Autenticación multifactor

✓ Fácil transferencia de bóvedas

✓ Atención al cliente por chat en directo

Limitaciones del plan gratuito:

✗ La mayoría de los artículos son de pago

✗ Carece de complementos para más navegadores.

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

Gestores de contraseñas

Dashlane: una experiencia segura y optimizada ➞ https://cnews.link/get-dashlane_39/

==========

Plan gratuito:

✓ Compartir contraseña con 5 usuarios

✓ Excelente reputación

✓ Soporte 2FA

✓ Almacena hasta 50 contraseñas

Limitaciones del plan gratuito:

❌ La cantidad máxima de contraseñas almacenadas es de 50.

❌ Falta la versión para iOS

❌ Limita el usuario a un solo dispositivo.

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

Gestores de contraseñas

Keeper: excelente herramienta de gestión de contraseñas ➞ https://cnews.link/get-keeper_10/

==========

Contras del plan gratuito:

✓ Gran compatibilidad

✓ Múltiples opciones de 2FA

✓ Aplicación de mensajería privada

KEEPER

Limitaciones del plan gratuito:

✕ Pocas opciones de exportación

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

Gestores de contraseñas

RoboForm ➞ https://cnews.link/get-roboform_10/

==========

Contras del plan gratuito:

Almacenamiento ilimitado de contraseñas

✓ Cómoda actualización de las contraseñas más débiles.

✓ Compartir contraseña por correo electrónico

✓ Vigilancia de la web oscura

Limitaciones del plan gratuito:

❌ Podría ser más fácil de usar

❌ Chat en directo solo para usuarios de pago

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

Hora de preguntar...

¿Puede decirme qué es el robo de identidad y algunas de las formas en que se lleva a cabo? (phishing, malware, pharming, ordenadores y teléfonos desechados...)

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

Hora de responder...

El robo de identidad y el fraude de identidad son términos utilizados para referirse a todos los tipos de delitos en los que alguien obtiene y utiliza indebidamente los datos personales de otra persona de alguna manera que implica fraude o engaño, normalmente para obtener un beneficio económico.

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

Filtración de datos personales, creación de contraseñas seguras, organizadores de contraseñas
Juego: ¿Con quién estás hablando?

Materiales

Teléfonos/tabletas/portátiles con acceso a Internet, proyector, hojas de papel, bolígrafos, cartulinas

Cómo llegar

Se supone que este juego simula cuando hablas con alguien por Internet y no sabes realmente quién está al otro lado de la pantalla, si dice la verdad o no, o si se está haciendo pasar por otra persona con un propósito oculto. A cada participante se le asigna un personaje y los demás tienen que averiguar quiénes son. Pero algunos no coincidirán con la verdad. Los que no tienen personaje en parejas o grupos (dependiendo de los participantes) tienen que adivinar a través de preguntas quién es la persona con la que están hablando (la que tiene el personaje asignado). Está pensado para un grupo de 15 personas, donde 5 tienen personaje y 10 en parejas intentarán averiguar quién es el personaje de los otros 5 y si es real o no. Se jugará en dos grupos de 15 participantes cada uno. Las personas con personajes asignados tienen que responder a las preguntas como si fueran los personajes. Las parejas sabrán que es posible que algunos de los personajes no sean quienes dicen ser. Las 5 parejas se harán preguntas unas a otras durante unos minutos y rotarán. Después de terminar con todos, cada pareja tiene que decir quién cree que es cada personaje y si realmente son quienes dicen ser.

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

Filtración de datos personales, creación de contraseñas seguras, organizadores de contraseñas
Juego: ¿Con quién estás hablando?

Personaje 1:
Chico de 20 años. Le gusta el fútbol, salir con sus amigos e ir a conciertos.

Personaje 2:
Chica de 25 años. Juega en un equipo de rugby y le gustan los deportes de montaña. Le gustan los animales y tiene un perro.

Personaje 3: (Personaje falso)
Respuestas como: Chica de 18 años. Participante en biología. Le gusta la naturaleza y las plantas. Es fan de Rosalía.
En realidad lo es: un hombre de 39 años.

Personaje 4: (Personaje falso)
Respuestas como: Chico de 23 años. Le gusta la música rock y el surf. Suele jugar a videojuegos.
En realidad lo es: Un hombre de 47 años.

Personaje 5:
Chico de 27 años. Juega al pádel. Le gustan los animales y tiene dos gatos. Trabaja como diseñador gráfico.

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

Filtración de datos personales, creación de contraseñas seguras, organizadores de contraseñas
Juego: ¿Con quién estás hablando?

¿Qué ocurre?

Se supone que este juego simula cuando hablas con alguien por Internet y no sabes realmente quién está al otro lado de la pantalla, si dice la verdad o no, o si se está haciendo pasar por otra persona con un propósito oculto.

A cada participante se le asigna un personaje y los demás tienen que averiguar quiénes son. Pero algunos de ellos no coincidirán con la verdad.

Las personas con personajes asignados tienen que responder a las preguntas como si fueran los personajes.

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

Escenario 2
Tecnología y TI

BRinging STEM into Active agINg – BRAIN

Erasmus+ 2020-1-PL01-KA204-081805

Nombre del socio: Foro de Formacion y Ediciones

Akademia WSEI
Mine Vaganti NGO
Foro de Formación y Ediciones S.L.
Horizont Proconsult

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

Problemas con las compras en línea y las transferencias de dinero

BRinging STEM into Active agINg – BRAIN

Erasmus+ 2020-1-PL01-KA204-081805

Nombre del socio: Foro de Formacion y Ediciones

Akademia WSEI
Mine Vaganti NGO
Foro de Formación y Ediciones S.L.
Horizont Proconsult

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

Ice Breaker

El grupo forma un círculo. Los participantes se lanzan una pelota. Cada uno da una asociación a la palabra anterior pronunciada por la persona de la que recibe la pelota. Se repite la actividad.

¿Qué ocurre?

Los rompehielos son actividades divertidas que ayudan a las personas a conocerse. Los instructores pueden utilizarlos para familiarizar a los participantes con el contenido y las expectativas del curso. Los rompehielos también pueden diseñarse para ayudar a calentar los espacios de aprendizaje en línea y orientar a los participantes sobre el entorno en línea.

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

Pagos por móvil

Las carteras digitales son un medio para almacenar varias tarjetas físicas de crédito o débito.

Aplicación bancaria que puede utilizarse con fines de autenticación cuando se realizan transacciones o para acceder a servicios bancarios. Normalmente, cada banco tiene su propia aplicación.

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

Ventajas de pagos móviles

Touch ID en forma de escáner de huellas dactilares o introducción de PIN las hace más seguras que las tarjetas de crédito o débito físicas,

Eliminación de la cartera física

La gente no puede ver qué tarjeta tienes (algunas tarjetas se proporcionan a clientes con límites bajos de puntuación crediticia. Algunas personas sienten vergüenza de mostrarla a otras personas).

Facilitar el pago a terceros en sitios web de comercio electrónico

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

Hora de preguntar...

¿Qué son las galletas? ¿Para qué sirven?

Akademia WSEI
Mine Vaganti NGO
FFE Foro de Formación y Ediciones S.L.
Horizont Proconsult

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

Hora de responder...

Las cookies son pequeños fragmentos de texto que los sitios web que visita envían a su navegador. Permiten a los sitios web recordar información sobre su visita, lo que puede facilitar que vuelva a visitarlos y hacerlos más útiles para usted. Son archivos temporales que pueden durar más o menos tiempo. Podemos configurarlos, utilizar herramientas para bloquearlos, borrarlos cuando queramos... El problema puede venir sobre todo cuando recogen datos personales sin avisar al usuario.

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

Problemas con Internet, compras con tarjeta y transferencias de dinero.

Compras seguras en línea

Materiales

Teléfonos/tabletas/portátiles con acceso a Internet, proyector, hojas de papel, bolígrafos, cartulinas

Cómo llegar

Los participantes se sentarán en círculo. El formador escribirá en la pizarra preguntas orientativas para ayudar a los participantes a elaborar normas para comprar en Internet de forma segura (véase el anexo).

Anexo

- utilizar un sitio web conocido
- utilizar una herramienta de evaluación de la seguridad de los nuevos sitios web
- buscar la cerradura
- no comparta sus datos sensibles con todo el mundo
- Utilizar Wi-Fi privado
- Crear contraseñas seguras
- No compre con tarjeta en lugares públicos

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

Monederos digitales

- **Ejemplos:**
- Apple Pay, Google Pay y Samsung Pay son probablemente tres de los monederos digitales más populares, pero hay bastantes más. Otros monederos digitales populares son PayPal y Venmo, ambos de carácter exclusivamente social, ya que permiten enviar dinero fácilmente a comercios y amigos.

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

Problemas con Internet, compras con tarjeta y transferencias de dinero.

Peligros del uso del dinero en el espacio digital

Materiales

Teléfonos/tabletas/portátiles con acceso a Internet, proyector, hojas de papel, bolígrafos, cartulinas

Cómo llegar

El presentador escribe el término "Peligros del uso del dinero en el espacio digital" en el centro del rotafolios. Distribuye notas adhesivas Post-it (de distintos colores) a los participantes y pídeles que escriban sus asociaciones con el término y las peguen en el rotafolios. Lea en voz alta las asociaciones escritas, agrupándolas si es posible. Discuta cada asociación e intente conocer los peligros en línea relacionados con el dinero (anexo siguiente).

Anexo

Peligros del uso del dinero en el espacio digital

1. La información de su tarjeta puede ser robada (IBAN, CVC, fecha de caducidad)

Su información personal puede ser robada (nombre completo, código de identificación, fecha de nacimiento, número de teléfono, contraseñas)

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

¿SON SEGURAS LAS CARTERAS DIGITALES?

De hecho, los monederos digitales son más seguros que las tarjetas físicas, ya que los pagos móviles están fuertemente encriptados y tokenizados, lo que significa que ninguno de los números reales de su tarjeta o cuenta se almacenan en el monedero digital.

Los monederos digitales van un paso más allá y añaden la tokenización, que toma los datos confidenciales encriptados y los sustituye por un equivalente digital no confidencial conocido como token. Estos tokens únicos se generan aleatoriamente cada vez que un usuario realiza un pago y solo la pasarela de pago del comerciante puede hacer coincidir este token para aceptar el pago.

No sólo su información está más segura gracias a esa tecnología, sino también mediante la verificación del usuario. Esta capa añadida de seguridad suele hacerse mediante huella dactilar, reconocimiento facial o PIN.

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

Apple y google pagan similitud

Ambos sistemas utilizan la tecnología NFC

Tanto Google Pay como Apple Pay pueden realizar compras en línea directamente desde una aplicación o un sitio web, gestionando automáticamente todo el proceso de pago con valores predeterminados y requiriendo únicamente la verificación del PIN o Touch ID para completar la transacción.

Ambas son más seguras que las tarjetas de débito y crédito físicas, porque el sistema no revela los datos de la tarjeta del usuario al vendedor.

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

Diferencias entre Apple y Google Pay

Apple pay permite la autenticación con Touch ID o Face ID, pero solo es compatible con los nuevos gadgets de hardware.

Google, por su parte, opta por un sistema de autenticación más tradicional basado en el PIN. Esto le permite funcionar en hardware más antiguo.

Puedes añadir cualquier tarjeta de crédito o débito a google pay. En apple pay solo puedes añadir tarjetas de crédito o débito que la empresa Apple tenga en contacto con bancos emisores de tarjetas físicas.

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

Hora de preguntar...

¿Sabes qué son los datos en la nube?

Akademia WSEI
Mine Vaganti NGO
FFE Foro de Formación y Ediciones S.L.
Horizont Proconsult

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

Hora de responder...

El almacenamiento en nube es un modelo de computación en nube que almacena datos en Internet a través de un proveedor de computación en nube que gestiona y opera el almacenamiento de datos como un servicio. Se suministra bajo demanda, con capacidad y costes "justo a tiempo", y elimina la necesidad de comprar y gestionar una infraestructura propia de almacenamiento de datos.

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

¿Seguridad de Google? ¿Cómo funciona?

1. Los datos de la tarjeta del usuario se facilitan una sola vez, durante la configuración inicial en los servidores de Google. (Google almacena los datos de la tarjeta en sus servidores)

2. Google guarda los datos de tu tarjeta en sus servidores.

3. La tarjeta virtual se emite en su dispositivo con cifrado de datos sensibles.

4. Al pagar el vendedor nunca ve los datos reales de tu tarjeta, que están protegidos con los servidores de google.

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

¿Seguridad Apple? ¿Cómo funciona?

Apple Pay

- Apple utiliza el sistema de tokenización.
  Pasos;
- Cuando el dispositivo recibe los datos de tu tarjeta, se pone en contacto directamente con el banco emisor. (Apple no almacena los datos de tu tarjeta)
- Cuando se confirma la tarjeta con el banco, éste recibe un token específico para el dispositivo y la tarjeta (relacionado) llamado Número de Cuenta del Dispositivo (DAN), que se almacena en un chip seguro en el dispositivo.
- El DAN se parece estructuralmente a un número de tarjeta de crédito y se transmite al comerciante cuando se realiza cualquier pago antes de ser autorizado por el banco.
- Apple Pay explicado en detalle:
  https://www.youtube.com/watch?v=mt5FEvoEHEk

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

Monederos criptográficos

Disponer de un monedero seguro de criptomonedas funciona de forma muy parecida a un monedero normal, salvo que las divisas y el contenido del monedero pueden ser pirateados a través de medios digitales. Además, disponer de un monedero puede permitir a los usuarios realizar varias transacciones sin perder de vista su saldo.

Algunos bancos en línea como Revolut, Wirex, Cryptopay, etc. permiten retirar criptomonedas de cajeros automáticos en euros/dólares de forma gratuita hasta un cierto límite.

Revolut

wirex

CRYPTOPAY

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

Tipos de criptocarteras

Monederos informáticos

Los monederos software son monederos calientes, ya que suelen estar conectados a Internet. Son monederos que funcionan con un programa específico que permite un fácil acceso. Algunos ejemplos de monederos software son:

- Monederos de sobremesa
- Monederos móviles
- Monederos en línea

Monederos electrónicos

Los monederos de hardware se diferencian de los monederos de software en que almacenan las claves privadas del usuario en un dispositivo de hardware, como una unidad flash. Su principal objetivo es almacenar sus datos fuera de línea para evitar la invasión de la privacidad. Su principal objetivo es almacenar sus datos fuera de línea para evitar la invasión de la privacidad.

Monederos de papel

Estos tipos de monederos incluyen un software particular que puede utilizarse para generar tus claves e imprimirlas. Sus otras funciones incluyen transferir tus fondos a la dirección y trasladar tus activos a tu monedero de escritorio. Para hacer esto último, los usuarios tendrán que introducir manualmente sus claves o escanear el código incluido en el monedero.

Akademia WSEI
Mine Vaganti NGO
FFE Foro de Formación y Ediciones S.L.
Horizont X Proconsult

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

Hora de preguntar...

¿Podría alguien explicarme qué es la ciberseguridad?

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

Hora de responder...

La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Estos ciberataques suelen tener como objetivo acceder a información sensible, modificarla o destruirla; extorsionar a los usuarios; o interrumpir los procesos empresariales normales.

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

Ventajas de los distintos tipos de criptocarteras

Monederos calientes/en línea/software

- Fines de gasto;
- No estoy dispuesto a pagar por una cartera.

Carteras frías/offline/Hardware

- Fines de inversión;
- Si está almacenando más criptomonedas, entonces está

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

Problemas con Internet, compras con tarjeta y transferencias de dinero.

Estafa en las compras en línea - vídeos

Materiales

Teléfonos/tabletas/portátiles con acceso a Internet, proyector, hojas de papel, bolígrafos, cartulinas

Cómo llegar

ELEMENTOS DE CREDIBILIDAD DEL SITIO WEB

Cómo detectar y evitar un sitio web fraudulento (en inglés): https://www.youtube.com/watch?v=3oEI0FCnI_Y

Consejos para comprar en Internet con seguridad (en inglés): https://www.youtube.com/watch?v=cWcNQgPiqhc

Pasos:

1. Antes de reproducir los vídeos anteriores, se pide a los participantes que los sigan y observen que no todos los elementos de credibilidad
2. Tras ver los vídeos, se pide a los participantes sentados en círculo que escriban en la pizarra elementos sobre cómo comprobar la credibilidad de un sitio web.
3. Cada escrito es discutido de inmediato por el participante y el formador (anexo).

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

Problemas con Internet, compras con tarjeta y transferencias de dinero.

Estafa en las compras en línea - vídeos

Anexo

Cómo comprobar la credibilidad de un sitio web:
Anuncios de pago: algunos estafadores utilizan anuncios de pago de Google para aparecer en las primeras posiciones de las búsquedas de Google.
Reseñas positivas falsas de usuarios: los sitios web falsos crean reseñas positivas para aumentar su credibilidad.
comentarios de usuarios positivamente falsos.
URL falsa - algunos sitios web falsos utilizan letras de diferentes alfabetos para imitar sitios web legítimos.
PadLock y HTTPS - muestran que los datos que tendrá en el sitio web están encriptados. (Terceros no pueden ver sus contraseñas, correos electrónicos, etc.)
Certificado: compruebe la fecha de caducidad del certificado del sitio web y quién lo emitió.
Dirección de la empresa. derechos de autor y contactos - la dirección de la empresa no se encuentra en google maps o está en un lugar extraño (bosque, desierto, etc.)
Derechos de autor, estatuto de explotación/trabajo: deben estar actualizados.
Correos electrónicos falsos - mejor entrar en los enlaces de su navegador que de los correos electrónicos, ya que puede consistir en datos de spyware para recopilar datos sensibles.

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

Tarjeta de débito

Las tarjetas de débito son **emitidas por su banco y funcionan como una combinación de tarjeta de cajero automático y tarjeta de crédito**. Sin embargo, a diferencia de una tarjeta de crédito, una tarjeta de débito está vinculada directamente a su cuenta bancaria, utilizando el dinero que tiene depositado para pagar su compra o retirar dinero del cajero de forma digital.

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

Tarjetas de débito

Pros

- Prevenir la deuda
- Sin cuota anual
- Bueno para compras pequeñas
- Fácil de conseguir

Contras

- Disponen de fondos limitados
- Cobrar comisiones por descubierto
- Complicado para artículos caros

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

Hora de preguntar...

¿Alguien sabe cómo crear una contraseña segura?

Akademia WSEI
Mine Vaganti NGO
FFE Foro de Formación y Ediciones S.L.
HORIZONT X PROCONSULT

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

Hora de responder...

Las principales claves para crear una contraseña segura son que debe tener al menos 12 caracteres, mezclando mayúsculas y minúsculas, números y un símbolo. También es necesario utilizar contraseñas diferentes para cada sitio y cambiarlas de vez en cuando.

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

Tarjetas de crédito

Las tarjetas de crédito le ofrecen una línea de crédito que puede utilizar **para hacer compras, transferencias de saldo y/o anticipos en efectivo** y que le exigen devolver el importe del préstamo en el futuro. Al utilizar una tarjeta de crédito, tendrás que realizar al menos el pago mínimo cada mes antes de la fecha de vencimiento del saldo.

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

Tarjetas de crédito

Pros

- Tiempo para detectar errores
- Puede crear crédito
- Ofrecer recompensas
- Tienen límites elevados

Contras

- Puede perder no mucho dinero
- Puede perjudicar al crédito
- Posible exceso de gasto

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

Hora de preguntar...

¿Qué es una VPN?

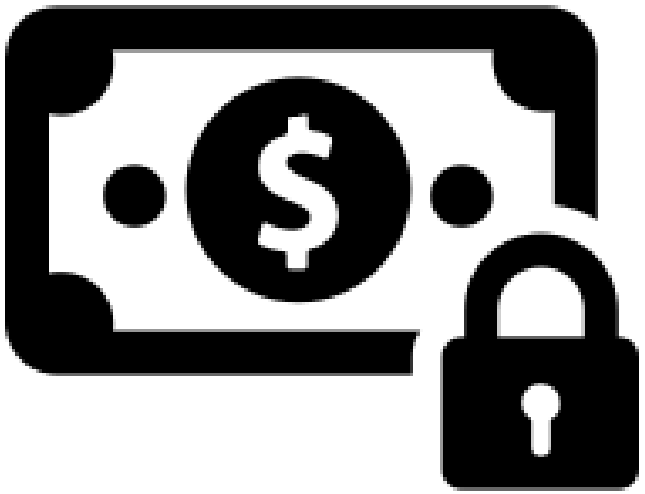
Co-funded by the
Erasmus+ Programme
of the European Union

Hora de responder...

VPN son las siglas de "red privada virtual", un servicio que le ayuda a mantener la privacidad en Internet. Una VPN establece una conexión segura y cifrada entre su ordenador e Internet, proporcionando un túnel privado para sus datos y comunicaciones mientras utiliza redes públicas.

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

Cómo utilizar con seguridad su tarjeta de débito o crédito en Internet



Busque el candado: Asegúrate de que estás comprando en un sitio web seguro, sobre todo cuando llegue el momento de introducir el número de tu tarjeta. Busca el icono del candado cerrado en tu navegador y presta atención a cualquier advertencia de seguridad que aparezca.

Controla tu cuenta: Siempre es una buena idea controlar tu dinero, y es especialmente importante si compartes la información de tu cuenta en Internet. Revisa tus cuentas con regularidad: una vez al mes como mínimo, aunque es mejor hacerlo más a menudo. Y configura alertas en tu cuenta para saber cuándo sale dinero.

Utilice conexiones seguras: Los dispositivos móviles y la conexión Wi-Fi gratuita facilitan las cosas. Pero nunca se sabe lo seguro que es un punto de acceso público. Si vas a acceder a cuentas financieras o a teclear números de tarjetas, deja esas tareas para cuando estés en casa o en el trabajo y sepas que tu tráfico es seguro.

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

Utilice sitios web conocidos

- Empieza por un sitio de confianza. Los resultados de las búsquedas pueden estar amañados para llevarte por mal camino, sobre todo cuando pasas de las primeras páginas de enlaces. Si conoces el sitio, es menos probable que sea un timo. Todos sabemos que Amazon.com tiene de todo; asimismo, casi todos los grandes comercios tienen una tienda online, desde Target a Best Buy, pasando por Home Depot. Tenga cuidado con los errores ortográficos o los sitios que utilizan un dominio de nivel superior diferente (.net en lugar de .com, por ejemplo). Sí, las ventas en estos sitios pueden parecer tentadoras, pero así es como le engañan para que facilite sus datos.

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

Hora de preguntar...

¿Sabe cómo se rastrea a los usuarios en los motores de búsqueda (historial de búsqueda, cookies, direcciones IP, historial de clics)?

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

Hora de responder...

Un motor de búsqueda puede rastrearle a través de sitios web si los sitios web que visita contienen los propios scripts de rastreo del motor de búsqueda como parte de la página. Lo que busca deja un rastro de información sobre usted. Esta información revela lo que le interesa, lo que le despierta curiosidad e incluso lo que piensa sobre esas cosas.

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

Busque el candado

- Nunca compre nada por Internet con su tarjeta de crédito en un sitio que no tenga instalado el cifrado SSL (secure sockets layer), como mínimo.
- Sabrá si el sitio tiene SSL porque la URL del sitio empezará por HTTPS, en lugar de sólo HTTP. Aparecerá el icono de un candado cerrado, normalmente a la izquierda de la URL en la barra de direcciones o en la barra de estado de abajo; depende de tu navegador.
- HTTPS es estándar ahora incluso en sitios no comerciales, lo suficiente como para que Google Chrome marque cualquier página sin la S extra como "no segura". Así que un sitio sin ella debería destacar aún más.

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

Redes sociales: gestión segura de imágenes e información en línea
Nuestra seguridad en línea y la protección de nuestra intimidad

Materiales

Ordenador portátil con acceso a Internet para el presentador, retroproyector, bolígrafos, rotuladores, rotafolio, notas adhesivas, hojas de papel A4, pelota de tenis.

Cómo llegar

El presentador divide a los participantes en grupos de 4-5 personas y les pide que piensen y escriban en tarjetas las respuestas a la pregunta: ¿qué podemos hacer para cuidar Nuestra seguridad en Internet y proteger nuestra privacidad? A continuación, pide a los representantes de los grupos que lean las respuestas y las anoten en la pizarra o el rotafolio. Tras anotar todas las respuestas, el presentador pide a los participantes que elijan la regla que les parece más importante. Los voluntarios explican a los demás participantes por qué la han elegido. Véase a continuación:

Además: Resumen del instructor de la clase, debate sobre el impacto de los medios sociales en nosotros, las oportunidades y los riesgos de utilizar los medios sociales de forma incorrecta, qué podemos hacer para aumentar nuestra seguridad.
Visionado conjunto de la totalidad o partes del vídeo de You Tube "La verdad sobre las redes sociales"
https://www.youtube.com/watch?v=DU3655oQexw

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

Redes sociales: gestión segura de imágenes e información en línea
Nuestra seguridad en línea y la protección de nuestra intimidad

Anexo

- Si no está seguro de con quién está hablando, no dé ninguna información sobre sí mismo.
- No reveles tus contraseñas a otras personas. Organiza unas que sean difíciles de adivinar (¡no puede ser tu fecha de nacimiento ni tu nombre!). La contraseña no debe contener menos de 8 caracteres, incluidos números y mayúsculas. Utiliza contraseñas distintas en servicios diferentes.
- No permita que su navegador recuerde las contraseñas del correo electrónico y los servicios que utiliza. Cierre la sesión cuando haya terminado.
- Si utilizas redes sociales, asegúrate de que tienes la configuración de privacidad adecuada. Cuanta menos información compartas con extraños, mejor.
- En foros de debate o blogs, utilice un apodo (seudónimo), no su nombre. Evita publicar información sobre ti en Internet.
- No utilices la posibilidad de "etiquetarte" automáticamente donde estés.
- Preste atención a los mensajes que aparecen al descargar juegos y aplicaciones para móviles y smartphones. Por ellos puedes saber a qué datos tuyos solicita acceso el servicio descargado. Ten cuidado con lo que aceptas.
- Proporcione sólo los datos necesarios para crear una cuenta.
- En lugar del seguimiento de Facebook, utiliza boletines y canales RSS.

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

No comparta más de la cuenta

- Ningún comercio electrónico de compras en línea necesita tu número de la Seguridad Social o tu fecha de cumpleaños para hacer negocios.
- Sin embargo, si los estafadores se hacen con ellos y con su número de tarjeta de crédito, pueden hacer mucho daño. Cuanto más sepan los estafadores, más fácil les resultará robarte la identidad.
- Siempre que sea posible, facilite la menor cantidad posible de datos personales. Los sitios más importantes sufren infracciones constantemente.

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

Hora de preguntar...

¿Conoces algún truco para evitar que rastreen tu información?

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

Hora de responder...

Cambia la configuración para bloquear rastreadores, usa el modo incógnito, usa VPN, usa navegadores privados. Search Encrypt utiliza el cifrado para ocultar su historial de búsqueda de otras personas que puedan utilizar su dispositivo después de buscar.

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

Problemas con Internet, compras con tarjeta y transferencias de dinero.

Uso seguro de tarjetas de crédito y débito

Materiales

Teléfonos/tabletas/portátiles con acceso a Internet, proyector, hojas de papel, bolígrafos, cartulinas

Cómo llegar

Los participantes se sentarán en círculo. El formador escribirá en la pizarra preguntas orientativas para ayudar a los participantes a elaborar normas para utilizar las tarjetas de crédito y débito de forma segura (véase el anexo).

Anexo

- Utilizar mejor la aplicación de pago por móvil
- Utilice los dispositivos de seguridad proporcionados por el emisor de la tarjeta.
- Si pierde su tarjeta, informe inmediatamente al banco
- No muestre su tarjeta en público.

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

No use la tarjeta, use el teléfono

Hoy en día, pagar con el smartphone es bastante habitual en las tiendas físicas y, de hecho, es incluso más seguro que utilizar la tarjeta de crédito.

El uso de una aplicación de pago móvil como Apple Pay genera un código de autenticación de un solo uso para la compra que nadie más podría robar y utilizar.

Además, evitarás que te roben la tarjeta. Ni siquiera tendrás que llevar la tarjeta de crédito si sólo vas a sitios que acepten pagos por teléfono.

¿Qué importancia tiene esto para las compras en línea? Muchas aplicaciones de teléfono aceptan ahora pagos con Apple Pay y Google Pay. Solo necesitas tu huella dactilar, tu cara o tu código para hacerlo al instante.

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

Crear contraseñas seguras

- Asegúrese de utilizar contraseñas indescifrables. Nunca es más importante que cuando se realizan operaciones bancarias y compras en línea. Nuestros viejos consejos para crear una contraseña única pueden resultar útiles en una época del año en la que ir de compras probablemente signifique crear nuevas cuentas en sitios de comercio electrónico.
- Ni siquiera tu contraseña perfecta es perfecta. Lo más inteligente: utiliza un gestor de contraseñas que cree contraseñas indescifrables por ti. El gestor las registrará y las introducirá para que no tengas que pensar en ellas.

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

Filtración de datos personales, creación de contraseñas seguras, organizadores de contraseñas
Juego: Nunca jamás...

Materiales

Teléfonos/tabletas/portátiles con acceso a Internet, proyector, hojas de papel, bolígrafos, cartulinas

Cómo llegar

- Todos los participantes se colocan de pie formando un círculo. Se dicen frases que empiecen por "Yo nunca he..." y los participantes que hayan hecho esta frase deben avanzar un paso. Después vuelven a su sitio. Aquí hay algunos ejemplos, pero los participantes también pueden decir cualquier afirmación que deseen.
- Nunca he comprado por Internet
- Nunca me han estafado en Internet.
- Nunca he hablado con alguien por Internet sin conocerle
- Nunca he olvidado mis contraseñas
- Nunca he recibido un correo spam
- Nunca he sido atacado por malware
- Nunca he recibido un correo electrónico pidiéndome toda mi información personal
- Nunca he intentado averiguar la contraseña de alguien
- Nunca había sospechado que alguien hubiera entrado en una de mis cuentas.
- Nunca he encontrado en mi teléfono un anuncio de algo que acababa de buscar.
- Nunca he sospechado que me espiaran por Internet
- Nunca he acosado a nadie
- Nunca he sufrido ciberacoso

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

Filtración de datos personales, creación de contraseñas seguras, organizadores de contraseñas

Juego: Nunca jamás...

- Nunca he acosado cibernéticamente a nadie
- Nunca he accedido a sitios web sospechosos
- Nunca he descargado un virus mientras intentaba descargar otra cosa
- Nunca he tenido que cambiar todas mis contraseñas
- Nunca he tenido que cambiar mi tarjeta de crédito porque se hubieran filtrado sus datos.
- Nunca me he hecho pasar por otra persona en Internet.
- Nunca he ignorado las normas para mantener una contraseña segura.
- Nunca he participado en un falso sorteo en internet
- Nunca he perdido todo mi trabajo ni nada importante por no tener una copia de seguridad.
- Nunca había hecho clic en un banner que dijera que había ganado un premio.
- Nunca he navegado por la Deep web
- Nunca he compartido información privada en las redes sociales
- Nunca he compartido imágenes embarazosas en internet
- Nunca he publicado comentarios ofensivos en internet
- Nunca he recibido comentarios ofensivos en Internet
- Nunca he intentado averiguar la información privada de alguien
- Nunca he utilizado la autenticación en dos pasos
- Nunca he utilizado una VPN
- Nunca me he sentido inseguro en Internet

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

Filtración de datos personales, creación de contraseñas seguras, organizadores de contraseñas
Juego: Nunca jamás...

¿Qué ocurre?

Juego Nunca jamás. Sobre temas de Internet.
Todos los participantes se colocan en círculo. Se dicen frases que empiecen por "Nunca jamás..." y los participantes que hayan hecho esta frase deben avanzar un paso. Después vuelven a su sitio. Hay algunos ejemplos, pero también pueden decir cualquier afirmación que se les ocurra.

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

Privatice su Wi-Fi

- Si vas a comprar a través de un punto de acceso público, limítate a redes conocidas, aunque sean gratuitas, como las que se encuentran en Starbucks o en las tiendas Barnes & Noble.
- Cualquiera de los proveedores de nuestra lista de las redes Wi-Fi nacionales gratuitas más rápidas suele ser de confianza, pero probablemente también deberías utilizar una red privada virtual (VPN) para estar seguro (aquí te explicamos por qué).

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

Noticias falsas: es decir, buscar en Internet y verificar la información proporcionada por los medios de comunicación.

Test CRAAP - Presentación

Materiales

teléfonos/tabletas/ordenadores portátiles con acceso a Internet, retroproyector, bolígrafos, rotuladores, rotafolios, notas adhesivas, hojas de papel A4

Cómo llegar

Presentación de la herramienta de verificación de la información (prueba CRAAP), para qué sirve y cómo utilizarla (anexo a continuación) junto con la Presentación.

Anexo

El test CRAAP es una prueba de la fiabilidad objetiva de las fuentes de información en diversas disciplinas científicas. CRAAP es un acrónimo que significa actualidad, relevancia, autoridad, exactitud y finalidad. La prueba CRAAP está diseñada para ayudar a profesores y participantes a determinar si sus fuentes son fiables. Al utilizar la prueba al evaluar las fuentes, el investigador puede reducir la probabilidad de utilizar información poco fiable. La prueba CRAAP, desarrollada por Sarah Blakeslee y su equipo de bibliotecarios de la Universidad Estatal de California, Chico (CSU Chico), es utilizada principalmente por bibliotecarios de educación superior. Es uno de los diversos enfoques de la crítica de fuentes.

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

Noticias falsas: es decir, buscar en Internet y verificar la información proporcionada por los medios de comunicación.

Test CRAAP - Presentación

Puede resultar tentador utilizar en tu artículo cualquier fuente que parezca estar de acuerdo con tu tesis, pero recuerda que no toda la información es buena información, especialmente en un entorno en línea. Desarrollado por bibliotecarios de la Universidad Estatal de California-Chico, el test CRAAP es una lista de comprobación útil para evaluar un recurso en línea (o CUALQUIER recurso). La prueba proporciona una lista de preguntas para hacerse a la hora de decidir si un recurso es lo suficientemente fiable y digno de confianza como para ser utilizado en un trabajo de investigación.
La prueba CRAAP es un acrónimo de: Actualidad, Relevancia, Autoridad, Precisión y Finalidad.
No es fácil determinar si una fuente es fiable y puede utilizarse como herramienta de investigación. La prueba ahorra el tiempo y la energía necesarios para evaluar los contenidos disponibles en Internet.

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

Noticias falsas: es decir, buscar en Internet y verificar la información proporcionada por los medios de comunicación.

Test CRAAP - Presentación

Los recursos deben pasar por cinco etapas de verificación.

Actualidad de la información

La hora de publicación o envío de la información, si la información está actualizada o corregida y si el enlace funciona o no.

Pertinencia - la relevancia de la información

Comprueba si la información está relacionada con el tema, si el recurso es pertinente y si puede utilizarse en un trabajo académico.

Autoridad

Genera confianza proporcionando detalles sobre el autor, el editor antes de confiar en la información y el sitio web.

Precisión

Preste atención a la exactitud del contenido. La información debe basarse en pruebas presentadas a la audiencia. Hay que comprobar el tono del lenguaje, los errores gramaticales y otros errores tipográficos.

Finalidad de la información

Determinar los fines de la información: informar, enseñar, vender, entretener o persuadir.

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

Noticias falsas: es decir, buscar en Internet y verificar la información proporcionada por los medios de comunicación.

Test CRAAP - Prueba

Materiales

teléfonos/tabletas/ordenadores portátiles con acceso a Internet, retroproyector, bolígrafos, rotuladores, rotafolios, notas adhesivas, hojas de papel A4

Cómo llegar

Divida al grupo en equipos de unas 4 personas. Pide a cada equipo que busque un artículo sobre un tema de su elección. Elige un tema que se adapte al grupo (anexo siguiente). Distribuye las pruebas de craap impresas (anexo) y repártelas a cada persona. Pide a los participantes que lean el artículo y, a continuación, que analicen todo el texto a la luz de las preguntas incluidas en el test. En la parte derecha tienen espacio para reflexiones/conclusiones/respuestas. A partir del test, determinarán el grado de fiabilidad del artículo. No hay escala de calificación ni número de puntos. Las personas trabajan "en línea" sobre el material recibido, lo que significa que pueden realizar un análisis en profundidad del material: conocer todo el artículo, examinar su fuente con más detalle, verificar los datos utilizados, aprender algo sobre el autor, etc. Es importante que comprueben, utilizando los criterios dados en la prueba de craap, si el material es creíble, qué elementos indican credibilidad y cuáles la socavan. Los participantes también pueden anotar sus reflexiones, lo que facilitará el debate. Pide a cada grupo que exponga brevemente los resultados de su análisis.

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

Noticias falsas: es decir, buscar en Internet y verificar la información proporcionada por los medios de comunicación.

Test CRAAP - Prueba

Anexo

Temas para grupos:
Clima
Coronavirus
Refugiados
Vacunas
Famosos
Deportes
Unión Europea

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

Noticias falsas: es decir, buscar en Internet y verificar la información proporcionada por los medios de comunicación.

Test CRAAP - Prueba

		Notas / respuestas
Moneda puntualidad información	¿Cuándo se publicó la información?	
	¿Se ha actualizado la información (si no es nueva)?	
	¿El caso para el que está revisando esta información requiere datos más recientes y actualizados, o puede basarse en material más antiguo?	
	¿Funcionan los enlaces (si los hay) publicados en la información?	
Relevanc materialidad de la información en relación con sus necesidades	¿La información está relacionada con el tema que está tratando o responde a una pregunta importante para usted?	
	¿Para quién se preparó la información? ¿Para qué grupo destinatario?	
	¿Está la información a un nivel adecuado para sus necesidades? ¿Es demasiado básica y general o demasiado avanzada y detallada?	
	¿Comprobó otras fuentes de información antes de decidirse por ésta?	

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

Noticias falsas: es decir, buscar en Internet y verificar la información proporcionada por los medios de comunicación.

Test CRAAP - Prueba

Autoridad origen de la información	**¿Quién es el autor, editor, fuente o patrocinador de la información?**	
	¿Cuáles son las credenciales del autor de la información? ¿A qué organización, entidad o institución pertenece?	
	¿Está el autor cualificado para escribir sobre este tema?	
	¿Puede encontrar información de contacto, por ejemplo, nombre del editor, dirección de correo electrónico, etc., junto a la información?	
	¿La dirección del sitio web donde apareció la información dice algo sobre el autor o el remitente (por ejemplo, la URL termina en .com, .edu, .gov)?	
Precisión fiabilidad, veracidad y exactitud de la información	¿De dónde procede la información?	
	¿La información facilitada está respaldada por pruebas?	
	¿La información ha sido revisada por pares o citada (se aplica principalmente a los artículos científicos)?	
	¿Puede confirmar al menos parte de la información facilitada en otra fuente o utilizando sus conocimientos?	
	¿El lenguaje o la pronunciación de toda la información indican imparcialidad y están desprovistos de coloración emocional?	
	¿Hay errores ortográficos, gramaticales o de estilo en la situación?	

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

Noticias falsas: es decir, buscar en Internet y verificar la información proporcionada por los medios de comunicación.

Test CRAAP - Prueba

Propósito objetivo de la información, la razón por la que se creó	¿Para qué se creó la información? ¿Educar, informar, entretener, persuadir?
	¿Ha dejado claro el autor o la persona que financia la creación de la información cuál es el propósito de la misma?
	¿Es la información una cita o descripción de hechos, presenta una opinión o tiene carácter propagandístico?
	¿Da el punto de vista presentado en la información la impresión de imparcialidad y objetividad?
	¿Ve elementos en la información que indiquen parcialidad, adopción de una postura determinada, en temas relacionados con la política, la religión, la visión del mundo o, por ejemplo, que presente la perspectiva de una sola institución o persona?