



Ejercicio 1 Proyecto Mobile Money

MÓDULO 2

Ejercicio 1

Juega y Aprende

Duración estimada

10 min

Materiales

Dispositivo con acceso a Internet para aclarar dudas;
papel y lápiz

Instrucciones

Hay 5 preguntas sobre la seguridad online. Marca las respuestas correctas y revisa con la tercera página, si has acertado.



1. ¿Cuál es la forma más común de transmitir virus?

- A. Email
- B. Mensaje instantáneo
- C. Descarga por internet
- D. Medios portátiles

2. ¿Cuál de las siguientes sería la mejor contraseña?

- A. MySecret
- B. lw2c^tILV
- C. Abc123
- D. George1234

3. Recibes un correo electrónico con un salvapantallas que dice que te encantaría. ¿Qué debes hacer?

- A. Descargarlo en tu ordenador.
- B. Reenviar el mensaje a otros amigos para que lo compartan.
- C. Llama a alguien que te ayuda a instalarlo.
- D. Borrar el correo electrónico.

4. Cuando recibas un correo electrónico de un contacto desconocido que contenga un archivo adjunto, debes::

- A. Abrir el archivo adjunto para ver su contenido
- B. Eliminar el correo electrónico
- C. Reenviar el correo electrónico a alguien con más experiencia para que pueda abrir primero el archivo adjunto
- D. Imprimir el adjunto



1. **¿Cuál es la forma más común de transmitir virus?**

A. E-mail

El correo electrónico es el método de distribución de virus más común. Los ciberdelincuentes suelen utilizarlos como vector para distribuir programas maliciosos. Estos correos pueden parecer de fuentes fiables, lo que los hace especialmente peligrosos. Una vez que el destinatario abre el archivo adjunto o hace clic en el enlace, el virus se ejecuta en el dispositivo.

2. **¿Cuál de las siguientes sería la mejor contraseña?**

B. lW2c^tILV

Porque sigue los principios clave para crear una contraseña segura:

Complejidad: Incluye una mezcla de mayúsculas, minúsculas, números y caracteres especiales, lo que dificulta descifrarla.

Longitud: Es suficientemente larga, lo que añade otra capa de seguridad.

Las contraseñas más largas suelen ser más difíciles de descifrar.

Imprevisibilidad: La contraseña no incluye palabras o patrones fáciles de adivinar, que sean comunes, sencillos o relacionados con el usuario.

3 + 4. Recibes un correo electrónico con un salvapantallas que dice que te encantaría & Recibas un correo electrónico de un contacto desconocido que contenga un archivo adjunto ¿Qué debes hacer?

D. Borrar el mensaje.

Hay 4 grandes riesgos:

1. Algunos salvapantallas contienen virus.
2. Hacer clic en un enlace malicioso puede infectar un ordenador.
3. Las direcciones de correo electrónico pueden ser falsas, por lo que sólo porque el correo electrónico diga que es de alguien conocido, no puedes estar seguro de ello sin comprobarlo.
4. Algunos sitios web y enlaces parecen legítimos, pero en realidad son engaños diseñados para robar tu información.

¡Cuídate y disfruta del mundo digital!



Ejercicio 2 Proyecto Mobile Money

MÓDULO 2

Ejercicio 2 **¿Es un enlace seguro?**

Duración estimada

10 min

Materiales

Dispositivo con acceso a internet; papel y lápiz

Instrucciones

Le el texto

Piensa y decide por ti mismo

Repasamos todo conjuntamente



1. ¿Es seguro visitar este enlace?

Supongamos que recibes un correo electrónico de un banco pidiéndote que hagas clic en un enlace como el que aparece a continuación. El motivo del correo es que envíes datos personales, como nombre de usuario, contraseñas y datos de la tarjeta de crédito.

[http://url5423.eka.de/ls/click?
upn=V1OaWNMSPs2Lb0JqHpnyTLRIk2703ToIFpo2vd2MKt5gB6dYAUvw1B-
2FnC6T5iVsCdbcug7l6pkTad-2FBfACSlC-2BKw-3D-3DhmuAs-
OaWNMSPs2Lb0JqHpny-asDvdva](http://url5423.eka.de/ls/click?upn=V1OaWNMSPs2Lb0JqHpnyTLRIk2703ToIFpo2vd2MKt5gB6dYAUvw1B-2FnC6T5iVsCdbcug7l6pkTad-2FBfACSlC-2BKw-3D-3DhmuAs-OaWNMSPs2Lb0JqHpny-asDvdva)

No te apures, piénsatelo dos veces y decide si es seguro visitar este enlace.

Piensa en las razones.

La respuesta.

Este enlace **no** es seguro por varias razones:

- Utiliza http en lugar de https.
- El nombre del dominio no está relacionado con el nombre oficial del banco.
- El enlace es sospechosamente largo.
- El nombre de dominio del enlace es diferente del nombre de dominio de la dirección de correo electrónico del remitente.
- Un banco de verdad nunca pedirá nombres de usuario, contraseñas ni datos de tarjetas de crédito.



Ejercicio 3 Proyecto Mobile Money

MÓDULO 2

Ejercicio 3

Tu puntuación de seguridad en Internet

Duración estimada

10 min

Materiales

Dispositivo con acceso a internet; papel y lápiz

Instrucciones

El test puede realizarse individualmente o en grupo.

Las respuestas son SÍ y NO.



- ¿Utilizas la autenticación de dos factores en tus dispositivos? Por ejemplo, autenticación por huella dactilar y contraseña.
- ¿Utilizas un almacén de contraseñas? En ella se almacenan de forma segura todas las contraseñas de varias cuentas.
- ¿Utilizas la navegación privada cuando estás en línea?
- ¿Pones en privado la visibilidad de todas tus redes sociales?
- ¿Sueles publicar fotos en las redes sociales en las que compartes tu ubicación?
- ¿Compruebas regularmente tus transacciones bancarias para asegurarte de que no hay gastos de los que no eres consciente?
- Antes de introducir los datos de tu tarjeta de crédito cuando compras en Internet, ¿te aseguras de que hay un candado o una prueba de que el sitio web que estás visitando es seguro?
- ¿Tienes instalado en tu ordenador algún programa de seguridad, como antivirus, antispyware o cortafuegos?
- Si tu ordenador te pide que actualices el software, ¿lo harías de inmediato?
- ¿Utilizas una contraseña diferente para cada cuenta en la que tienes un inicio de sesión?

Enhorabuena.

Tu puntuación en seguridad online es ***** _____ *****

¡Seguridad de superestrella!