Fundamentos de seguridad en línea

Nombre: _____

Fecha: _____

Puntaje: _____

1.

¿Cuál de las siguientes es una característica de una contraseña débil?

1. Usar mayúsculas y minúsculas
2. Incluir números y símbolos
3. Tener menos de 8 caracteres
4. Usar una frase larga

Respuesta correcta:
C.

Tener menos de 8 caracteres

2.

¿Qué capa adicional de seguridad proporciona la autenticación de dos factores (2FA)?

1. Solo requiere una contraseña
2. Combina algo que sabes con algo que posees
3. Es una contraseña más larga
4. Usa biometría únicamente

Respuesta correcta:
B.

Combina algo que sabes con algo que posees

3.

Recibes un correo de un banco pidiendo tu contraseña urgente. ¿Qué debes hacer?

1. Responder con la contraseña
2. Hacer clic en el enlace para verificar
3. Ignorar y reportar como phishing
4. Llamar al número del correo

Respuesta correcta:
C.

Ignorar y reportar como phishing

4.

¿Qué indica el candado en la barra de direcciones del navegador?

1. Que la página es segura (HTTPS)
2. Que la página es rápida
3. Que tiene certificado caducado
4. Que no hay conexión

Respuesta correcta:
A.

Que la página es segura (HTTPS)

5.

¿Qué nombre recibe la técnica de engaño para obtener información personal haciéndose pasar por una entidad confiable?

Respuesta: _____

Respuesta correcta:

phishing

6.

¿Qué es un administrador de contraseñas?

1. Un programa que genera, almacena y autocompleta contraseñas seguras
2. Un programa que cambia automáticamente tu contraseña cada semana
3. Un complemento del navegador que muestra todas tus contraseñas en texto plano
4. Un software que bloquea el uso de contraseñas débiles

Respuesta correcta:
A.

Un programa que genera, almacena y autocompleta contraseñas seguras

7.

¿Por qué es importante mantener actualizado el software?

1. Para tener nuevas funciones
2. Para corregir vulnerabilidades de seguridad
3. Para que se vea mejor
4. No es importante

Respuesta correcta:
B.

Para corregir vulnerabilidades de seguridad

8.

¿Es seguro usar una red Wi-Fi pública sin protección?

1. Sí, siempre
2. No, porque otros pueden interceptar tus datos
3. Sí, si no compartes archivos
4. Solo si usas VPN

Respuesta correcta:
B.

No, porque otros pueden interceptar tus datos

9.

¿Cuál es la función principal de un firewall?

1. Acelerar la conexión
2. Bloquear accesos no autorizados a la red
3. Detectar y eliminar virus
4. Filtrar sitios web por contenido

Respuesta correcta:
B.

Bloquear accesos no autorizados a la red

10.

¿Qué sigla se utiliza para referirse a la red privada virtual que cifra tu conexión?

Respuesta: _____

Respuesta correcta:

VPN

11.

¿Con qué frecuencia se recomienda hacer copias de seguridad de datos importantes?

1. Nunca
2. Una vez al año
3. Regularmente (diario/semanal)
4. Solo cuando hay virus

Respuesta correcta:
C.

Regularmente (diario/semanal)

12.

¿Cuál de los siguientes NO es un tipo de malware?

1. Virus
2. Gusano
3. Navegador

Respuesta correcta:
C.

Navegador

13.

¿Qué nombre recibe el código malicioso que se replica a sí mismo sin necesidad de infectar un archivo?

Respuesta: _____

Respuesta correcta:

gusano

14.

¿Qué es la ingeniería social?

1. Un método para cifrar datos
2. Manipulación psicológica para obtener información confidencial
3. Un tipo de antivirus
4. Un lenguaje de programación

Respuesta correcta:
B.

Manipulación psicológica para obtener información confidencial

15.

¿Qué medida de seguridad agrega un segundo factor como un código SMS o una huella digital?

Respuesta: _____

Respuesta correcta:

autenticación de dos factores

16.

¿Para qué se usan las cookies en los sitios web?

1. Para recordar sesiones y preferencias del usuario
2. Para instalar virus
3. Para ralentizar el navegador
4. Para enviar spam

Respuesta correcta:
A.

Para recordar sesiones y preferencias del usuario

17.

¿Qué es el modo incógnito?

1. Navegación que no guarda historial ni cookies locales
2. Navegación anónima total
3. Modo de alta velocidad
4. Modo de seguridad máxima

Respuesta correcta:
A.

Navegación que no guarda historial ni cookies locales

18.

¿Cuántos caracteres se recomienda como mínimo para una contraseña segura?

1. 4
2. 8
3. 12
4. 6

Respuesta correcta:
B.

8

19.

¿Qué tipo de software malicioso se presenta como programa legítimo, pero ejecuta acciones dañinas?

Respuesta: _____

Respuesta correcta:

troyano

20.

¿Qué debes hacer si tu sistema operativo te pide reiniciar para instalar actualizaciones de seguridad?

1. Ignorar el mensaje
2. Posponer indefinidamente
3. Reiniciar lo antes posible
4. Desinstalar las actualizaciones

Respuesta correcta:
C.

Reiniciar lo antes posible

Respuestas

1. **C.**

   Tener menos de 8 caracteres

2. **B.**

   Combina algo que sabes con algo que posees

3. **C.**

   Ignorar y reportar como phishing

4. **A.**

   Que la página es segura (HTTPS)

5. phishing

6. **A.**

   Un programa que genera, almacena y autocompleta contraseñas seguras

7. **B.**

   Para corregir vulnerabilidades de seguridad

8. **B.**

   No, porque otros pueden interceptar tus datos

9. **B.**

   Bloquear accesos no autorizados a la red

10. VPN

11. **C.**

    Regularmente (diario/semanal)

12. **C.**

    Navegador

13. gusano

14. **B.**

    Manipulación psicológica para obtener información confidencial

15. autenticación de dos factores
16. **A.**

    Para recordar sesiones y preferencias del usuario
17. **A.**

    Navegación que no guarda historial ni cookies locales
18. **B.**

    8
19. troyano
20. **C.**

    Reiniciar lo antes posible