Detectando correos sospechosos

Nombre: _____

Fecha: _____

Puntaje: _____

1.

¿Qué es el phishing?

1. Un tipo de virus informático
2. Un correo electrónico fraudulento que busca obtener información personal
3. Un método para acelerar Internet

Respuesta correcta:
B.

Un correo electrónico fraudulento que busca obtener información personal

2.

¿Cuál de las siguientes es una señal de que un correo puede ser phishing?

1. El remitente es conocido
2. El correo tiene faltas de ortografía
3. El correo incluye enlaces que usan HTTPS
4. El correo viene de un amigo

Respuesta correcta:
B.

El correo tiene faltas de ortografía

3.

¿Qué debes hacer si recibes un correo sospechoso que pide tu contraseña?

1. Responder con tu contraseña
2. Hacer clic en el enlace para verificar
3. No hacer clic y reportarlo
4. Reenviarlo a tus amigos

Respuesta correcta:
C.

No hacer clic y reportarlo

4.

¿Qué es una URL engañosa?

1. Una dirección web que parece legítima pero redirige a un sitio falso
2. Una dirección web que no tiene el candado de seguridad
3. Una dirección web que usa el protocolo HTTPS
4. Una dirección web que termina en .com

Respuesta correcta:
A.

Una dirección web que parece legítima pero redirige a un sitio falso

5.

El tipo de fraude que utiliza correos electrónicos falsos se llama _____.

Respuesta: _____

Respuesta correcta:

phishing

6.

¿Cuál de estos NO es un signo típico de phishing?

1. Saludo genérico como 'Estimado cliente'
2. Urgencia para actuar rápido
3. Archivo adjunto inesperado
4. El remitente es tu mejor amigo

Respuesta correcta:
D.

El remitente es tu mejor amigo

7.

Si un correo dice 'Ganaste un premio, haz clic aquí', ¿qué deberías pensar?

1. Es verdad, debes reclamarlo
2. Es probablemente una estafa
3. Es una oportunidad única

Respuesta correcta:
B.

Es probablemente una estafa

8.

¿Qué significa que un correo tenga un remitente falso?

1. Que el correo fue enviado desde una dirección que no existe
2. Que el nombre del remitente está mal escrito
3. Que la dirección de correo parece real pero ha sido falsificada
4. Que el remitente está de vacaciones

Respuesta correcta:
C.

Que la dirección de correo parece real pero ha sido falsificada

9.

La técnica de manipulación psicológica para obtener información secreta se conoce como _____.

Respuesta: _____

Respuesta correcta:

ingeniería social

10.

¿Qué debes hacer antes de hacer clic en un enlace de un correo?

1. Pasar el ratón sobre el enlace para ver la URL real
2. Hacer clic inmediatamente
3. Copiar el enlace y pegarlo en un navegador
4. Ignorarlo siempre

Respuesta correcta:
A.

Pasar el ratón sobre el enlace para ver la URL real

11.

¿Qué es un archivo adjunto peligroso?

1. Un archivo .txt con información útil
2. Un archivo .exe o .zip inesperado que podría contener malware
3. Un archivo .pdf de un amigo
4. Un archivo .jpg de una foto

Respuesta correcta:
B.

Un archivo .exe o .zip inesperado que podría contener malware

12.

¿Cuál es la mejor acción si un correo sospechoso pide tu número de teléfono?

1. Proporcionarlo para que te llamen
2. No responder y marcarlo como spam
3. Llamar al número de teléfono del correo

Respuesta correcta:
B.

No responder y marcarlo como spam

13.

¿Qué característica tiene un correo de phishing típico?

1. Usa tu nombre correctamente
2. Contiene errores gramaticales
3. Ofrece ayuda genuina
4. Proviene de una empresa que conoces

Respuesta correcta:
B.

Contiene errores gramaticales

14.

La falsificación de la dirección de correo del remitente se llama _____.

Respuesta: _____

Respuesta correcta:

spoofing

15.

¿Cuál es una práctica segura al manejar correos?

1. Usar la misma contraseña para todo
2. Abrir todos los archivos adjuntos
3. Verificar la dirección del remitente antes de actuar
4. Compartir tu correo en foros públicos

Respuesta correcta:
C.

Verificar la dirección del remitente antes de actuar

16.

¿Qué debes hacer si accidentalmente hiciste clic en un enlace sospechoso?

1. Nada, si no pasó nada
2. Cambiar tus contraseñas y ejecutar un antivirus
3. Esperar a que el correo te pida más datos
4. Ignorar el incidente

Respuesta correcta:
B.

Cambiar tus contraseñas y ejecutar un antivirus

17.

¿Qué significa que un correo tenga un 'saludo genérico'?

1. Que el remitente no sabe tu nombre
2. Que es un correo muy formal
3. Que es un correo de un amigo

Respuesta correcta:
A.

Que el remitente no sabe tu nombre

18.

¿Cuál de los siguientes elementos NO debe compartirse por correo electrónico?

1. Tu nombre
2. Tu contraseña
3. Tu correo electrónico
4. Tu edad

Respuesta correcta:
B.

Tu contraseña

19.

El protocolo que muestra un candado en la barra de direcciones y comienza con 'https' se llama _____.

Respuesta: _____

Respuesta correcta:

HTTPS

20.

¿Cuál es el primer paso si sospechas que un correo es phishing?

1. Hacer clic en el enlace para confirmar
2. Contactar al remitente por otro medio
3. Reenviarlo a todos tus contactos
4. Eliminarlo sin pensar

Respuesta correcta:
B.

Contactar al remitente por otro medio

Respuestas

1. **B.**

   Un correo electrónico fraudulento que busca obtener información personal

2. **B.**

   El correo tiene faltas de ortografía

3. **C.**

   No hacer clic y reportarlo

4. **A.**

   Una dirección web que parece legítima pero redirige a un sitio falso

5. phishing

6. **D.**

   El remitente es tu mejor amigo

7. **B.**

   Es probablemente una estafa

8. **C.**

   Que la dirección de correo parece real pero ha sido falsificada

9. ingeniería social

10. **A.**

    Pasar el ratón sobre el enlace para ver la URL real

11. **B.**

    Un archivo .exe o .zip inesperado que podría contener malware

12. **B.**

    No responder y marcarlo como spam

13. **B.**

    Contiene errores gramaticales

14. spoofing

15. **C.**

    Verificar la dirección del remitente antes de actuar

16. **B.**

    Cambiar tus contraseñas y ejecutar un antivirus

17. **A.**

    Que el remitente no sabe tu nombre

18. **B.**

    Tu contraseña

19. HTTPS

20. **B.**

    Contactar al remitente por otro medio