OBJETOS DE APRENDIZAJE

2019

LÍNEA 2

MATERIALES DE FORMACIÓN PARA ESTUDIANTES DE GRADO DE LA COMPETENCIA DIGITAL

4. Seguridad: 4.1. Protección de dispositivos:

4. Cuestionario

crue Universidades Españolas

Red de Bibliotecas REBIUN

Colección Objetos de Aprendizaje, 2019

MATERIALES DE FORMACIÓN PARA ESTUDIANTES DE GRADO DE LA COMPETENCIA DIGITAL

4. Seguridad: 4.1. Protección de dispositivos:

4. Cuestionario

REBIUN Línea 2 (3er. P.E.) Grupo de Competencia Digital

.

crue Universidades Españolas Red de Bibliotecas REBIUN

REBIUN_COMP_DIG_4.1_Cuestionario

Área 4. Seguridad

Competencia 4.1 Protección de dispositivos

1. ¿A cuál de los siguientes aspectos debemos prestar atención para proteger nuestros dispositivos?
   [Selecciona la respuesta correcta]
   a. Sistema operativo
   b. Conexiones inalámbricas
   c. Aplicaciones y programas
   d. **Todas son correctas**

2. Son sistemas de protección de acceso a los dispositivos…
   [Selecciona la/s respuesta/s correcta/s. Puede haber más de una]
   a. Fondo de pantalla
   b. **Código PIN**
   c. Bluetooth
   d. **Contraseña**

3. ¿Cuál de los siguientes sistemas de protección de acceso es más recomendable?
   [Selecciona la respuesta correcta]
   a. Huella dactilar
   b. Código PIN de 4 dígitos
   c. **Contraseña alfanumérica de 8 caracteres**
   d. Patrón de puntos

4. Para poder contar con los últimos parches de seguridad para nuestro dispositivo es recomendable…
   [Selecciona la respuesta correcta]
   a. Instalar aplicaciones de mensajería
   b. Conectar el dispositivo a una red de telefonía
   c. **Actualizar el sistema operativo**
   d. Desactivar la localización del dispositivo

5. Señala las amenazas de seguridad que pueden afectar a un dispositivo personal
   [Selecciona la/s respuesta/s correcta/s. Puede haber más de una]
   a. **Malware**
   b. Webmail
   c. Freeware
   d. **Spam**

6. Indica la opción correcta para cada afirmación. [Verdadero/Falso]
    a. Se recomienda utilizar datos personales en las contraseñas para dificultar que pueda ser descubierta en un ataque **[falso]**
    b. Las contraseñas son un método de protección que usamos para limitar el acceso a la información y los archivos contenidos en nuestros dispositivos y cuentas personales **[verdadero]**
    c. En el caso de utilizar un gran número de contraseñas diferentes, es recomendable anotarlas en un papel **[falso]**
    d. Los gestores de contraseñas son herramientas que nos permiten almacenar las claves de acceso a múltiples servicios, sin necesidad de tener que memorizarlas **[verdadero]**

7. Qué tipo de ataques se realizan para descubrir contraseñas
   [Relaciona cada tipo de ataque con sus características]

Ataque	Características
1 Fuerza bruta **[D]**	A. Es una técnica de engaño que simula o suplanta la interfaz de un servicio en línea, como la banca electrónica, para que introduzcamos nuestras claves y obtenerlas así fácilmente.
2 Phising **[A]**	B. Se trata de un software malicioso de tipo spyware que captura todas las pulsaciones del teclado, incluidas las contraseñas.
3 Keylogger **[B]**	C. Un software se encarga de intentar obtener la contraseña de forma automática, probando con combinaciones de letras y palabras.
4 Ataque de diccionario **[C]**	D. Consiste en adivinar la contraseña a base de ensayo y error. Los ciberdelincuentes prueban distintas combinaciones hasta que dan con el patrón correcto.

8. Son medidas de buenas prácticas en la creación de contraseñas
   [Selecciona la/s respuesta/s correcta/s. Puede haber más de una]
    a. Utilizar datos personales como contraseña
    b. **Elegir una contraseña con un mínimo de 8 caracteres de longitud**
    c. Repetir el mismo caracter en la contraseña
    d. **Combinar letras mayúsculas y minúsculas, con números y caracteres especiales**

9. Son medidas de buenas prácticas en el uso de contraseñas
   [Selecciona la/s respuesta/s correcta/s. Puede haber más de una]
    a. **Elegir una contraseña fácil de recordar**
    b. Compartir contraseñas o difundirlas por medios electrónicos
    c. **Cambiar la contraseña periódicamente**
    d. Usar la misma contraseña en cada servicio

10. El uso de un gestor de contraseñas es recomendable para:
    [Selecciona la/s respuesta/s correcta/s. Puede haber más de una]
    a. **Generar de forma aleatoria contraseñas robustas**
    b. Mantener actualizadas las aplicaciones y programas instalados
    c. **Almacenar múltiples contraseñas, asociadas a diferentes servicios**
    d. Simular o suplantar la interfaz de un servicio en línea

11. Ventajas e inconvenientes del uso del sistema de autentificación de acceso usuario y contraseña
    [Relaciona cada característica con una opción]

Característica	Opción
1 Sirve para proteger nuestra información personal **[A]**	A Ventaja
2 Garantiza la privacidad de contenidos **[A]**	B Desventaja
3 Existe dificultad para memorizar múltiples contraseñas complejas **[B]**	
4 Evita accesos no deseados a dispositivos o cuentas personales **[A]**	
5 Presenta vulnerabilidades frente a las técnicas de robo de contraseñas utilizadas por ciberdelincuentes **[B]**	

12. Programa diseñado para mostrar publicidad no deseada
    [Selecciona la respuesta correcta]
    a. Keylogger
    b. **Adware**
    c. Gusano

13. Medidas para garantizar la seguridad de las conexiones inalámbricas
    [Selecciona la/s respuesta/s correcta/s. Puede haber más de una]
    a. Conectar Bluetooth siempre que usemos WiFi
    b. **No conectar los dispositivos a redes WiFi públicas abiertas**
    c. Conectar a WiFi públicas únicamente cuando debamos sincronizar archivos en la nube.
    d. **Deshabilitar las conexiones inalámbricas (WiFi, Bluetooth, NFC…)**

14. Formas de proteger los dispositivos
    [Selecciona la/s respuesta/s correcta/s. Puede haber más de una]
    a. **Establecer un código de acceso**
    b. **Mantener actualizadas las aplicaciones y programas instalados**
    c. **Deshabilitar los servicios de localización**
    d. No instalar aplicaciones desde repositorios oficiales

15. Son herramientas de protección específicas frente a las amenazas en línea:
    [Selecciona la/s respuesta/s correcta/s. Puede haber más de una]
    a. Botnet
    b. Ransomware
    c. **Antivirus**
    d. **Cortafuegos o firewall**

16. El protocolo seguro de navegación web HTTPS [Verdadero/Falso]
    a. Incorpora un canal de cifrado que garantiza la seguridad del tráfico de datos sensibles [**verdadero]**
    b. Únicamente funciona en navegadores móviles **[falso]**
    c. Incorpora un certificado de seguridad que se puede verificar a través del navegador **[verdadero]**
    d. Se debe evitar si vamos a utilizar servicios de intercambio de información privada como correo electrónico, redes sociales o banca electrónica **[falso]**

17. Indica la opción correcta para cada afirmación. [Verdadero/Falso]
    a. El uso de copias de seguridad reduce el daño que pueda ocasionar un ataque peligroso con previsible pérdida de información **[verdadero]**
    b. Es recomendable estar informado a través de canales oficiales especializados para mantener la seguridad de nuestros dispositivos y obtener formación en ciberseguridad. **[verdadero]**
    c. Es aconsejable utilizar métodos de acceso al dispositivo como el deslizado de pantalla para desbloquear el aparato **[falso]**
    d. Se debe contar con medidas de protección independientemente del sistema operativo utilizado por el dispositivo **[verdadero]**

18. Amenazas en el entorno digital
    [Relaciona cada amenaza con su descripción]

Amenaza	Descripción
1 Botnet **[B]**	A. Método de engaño utilizado por ciberdelincuentes para obtener datos personales como contraseñas de acceso o datos de tarjetas de crédito.
2 Phising **[A]**	B. Red de dispositivos que han sido infectados con un malware que se encarga de reclutarlos para efectuar acciones maliciosas sin consentimiento o conocimiento del usuario.
3 Spam **[C]**	C. Mensajes no solicitados que muestran publicidad sin consentimiento del usuario procedentes de envíos automatizados que sea realizan de forma masiva y aleatoria..

19. Tipos de malware
[Relaciona cada amenaza con su característica]

Malware	Característica
1 Troyano **[D]**	A. Lanza ventanas emergentes desde aplicaciones o páginas web con publicidad no deseada.
2 Virus **[C]**	B. En su versión más temible, cifra todo el contenido del dispositivo, impidiendo el acceso a archivos y carpetas, y exige un rescate económico para recuperar el acceso.
3 Adware **[A]**	C. Infecta archivos y carpetas replicándose a sí mismo sin conocimiento del usuario, llegando a modificar o borrar datos y aplicaciones
4 Ransomware **[B]**	D. De apariencia útil y legítima, aprovecha los privilegios concedidos para saltarse los métodos de seguridad y ejecutar de forma oculta acciones maliciosas.

20. Para evitar el correo no deseado o spam se recomienda:
[Selecciona la/s respuesta/s correcta/s. Puede haber más de una]
    a. **Crear filtros de correo personalizados**
    b. Abrir mensajes previamente categorizados como spam
    c. Utilizar la cuenta de correo principal para servicios de suscripción
    d. **No abrir ni contestar mensajes cuyo remitente nos resulte sospechoso o desconocido**

crue Universidades Españolas
Red de Bibliotecas REBIUN