TEST DE EVALUACIÓN

DISPOSITIVOS MÓVILES Y TELETRABAJO

Riesgos y protección

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CIBERSEGURITY INSTITUTE

www.incibe.es

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

TEST

Selecciona para cada pregunta la respuesta correcta.

1. ¿Los dispositivos móviles, como smartphones y tablets, pueden infectarse con malware?

a) No, están diseñados para no infectarse.

b) Sí, todos los dispositivos pueden infectarse.

c) Solamente los dispositivos basados en Android.

d) Sí, pero solamente si se descargan aplicaciones de tiendas no oficiales.

2. ¿Los correos maliciosos de tipo phishing afectan a los dispositivos móviles?

a) Sí, además debido al reducido tamaño de la pantalla, en el caso de los *smartphones* su detección se hace más compleja.

b) Sí, pero la protección que ofrece el sistema operativo en este tipo de dispositivos evita la mayoría de los ataques.

c) No, ya que este tipo de ataque está solamente enfocado a usuarios de ordenadores.

d) La «b», pero los navegadores de dispositivos móviles son capaces de detectar y avisar al usuario sobre si un sitio web es fraudulento o no.

3. Utilizar redes wifi de lugares públicos es:

a) Una práctica recomendable, ya que así se reduce el consumo de datos de la tarifa móvil.

b) Una práctica recomendable y segura, ya que actualmente debido al cifrado implementado en este tipo de redes es imposible espiar las comunicaciones.

c) Una práctica desaconsejable, ya que la red puede estar bajo el control de un ciberdelincuente y toda la información que se envía y recibe puede ser espiada.

d) Una práctica desaconsejable, pero si la conexión es lo suficientemente ágil los ciberdelincuentes no tendrían tiempo de espiar las comunicaciones.

4. El robo o pérdida es el principal riesgo al que se enfrentan los dispositivos móviles. Para evitar accesos no autorizados en caso de producirse, ¿cuál es el mejor sistema de control de acceso?:

a) Código PIN.

b) La «c» y la «d».

c) Contraseña.

d) Biometría.

5. Modificar los controles de seguridad impuestos por el fabricante, como hacer «root» en Android o «Jailbreak» en iOS, es:

a) Una práctica desaconsejable ya que ante un incidente de seguridad, como infección por malware, las consecuencias serían peores.

b) Una práctica desaconsejable, pero solamente si no se cuenta con los suficientes conocimientos técnicos.

c) Una buena práctica, sobre todo si el dispositivo se usa tanto para labores personales como de trabajo.

d) Ninguna de las anteriores.

6. Habilitar la función «recordar contraseña» con la que cuentan los navegadores web es:

a) Recomendable, ya que así se agiliza enormemente el flujo de trabajo.

b) Desaconsejable, ante un acceso fraudulento al dispositivo el ciberdelincuente podrá acceder a los servicios en los que está habilitada esta función.

c) Desaconsejable, ya que los controles de seguridad de este tipo de funciones suelen ser débiles.

d) Recomendable, ya que de esta forma se pueden establecer contraseñas únicas para cada servicio sin riesgo a que se olviden.

7. Los dispositivos móviles deben:

a) Contar con cifrado.

b) Tener un sistema de control de accesos robusto.

c) Estar actualizados a la última versión disponible.

d) Todas las respuestas son ciertas.

8. Una VPN permite:

a) Aumentar la velocidad de descarga de Internet.

b) Proteger el dispositivo contra las infecciones por malware.

c) Establecer una conexión segura y cifrada entre dos puntos cuando se usa una red insegura, como las redes wifi públicas.

d) Todas las respuestas son ciertas.

9. Cuando un dispositivo móvil corporativo se pierde o es robado se debe:

a) Informar a la empresa y a las FCSE si ha sido robado.

b) Bloquear el dispositivo, geolocalizarlo si es posible y en última instancia borrarlo remotamente si la recuperación del mismo no es posible.

c) Geolocalizar el dispositivo e intentar recuperarlo, en caso de no ser posible habilitar el borrado remoto.

d) La «a» y la «b».

10. La práctica del BYOD en el entorno empresarial:

a) Mejora la conciliación laboral pero también aumenta el riesgo de accesos no autorizados a información empresarial.

b) Aumenta los costes para la empresa.

c) Es una práctica desaconsejable que pone en riesgo la seguridad de la empresa y del propio empleado.

d) Aumenta el nivel de seguridad en la organización ya que son los propios empleados quienes gestionan los dispositivos.

SOLUCIONES

PREGUNTA	RESPUESTA
1	B
2	A
3	C
4	B
5	A
6	B
7	A
8	C
9	D
10	A

TEST DE EVALUACIÓN

DISPOSITIVOS MÓVILES Y TELETRABAJO

Riesgos y protección

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CIBERSEGURITY INSTITUTE

www.incibe.es

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD