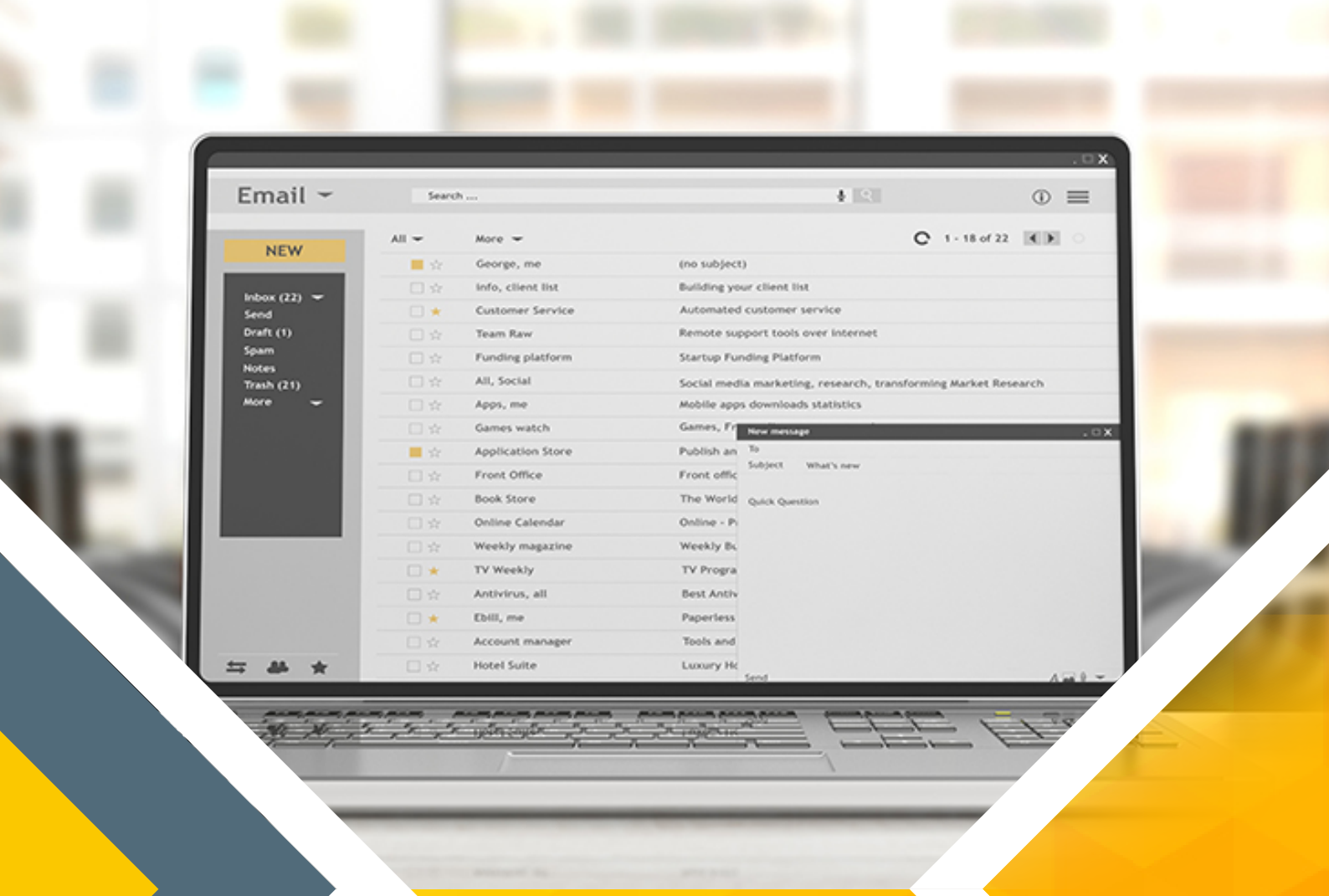


TEST DE EVALUACIÓN

EL CORREO ELECTRÓNICO

Principales fraudes y riesgos.

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. El *phishing* es un tipo de correo electrónico malicioso:

a) Cuyo objetivo, generalmente, es infectar los equipos de las víctimas con malware.

b) Cuyo objetivo es ofrecer información falsa.

c) Que suplanta a una empresa o entidad fiable y cuyo objetivo es generalmente hacerse con claves de acceso o información sensible.

d) Que hará que el dispositivo de la víctima funcione de manera anómala e imposibilitando realizar cualquier tarea con él.

2. Las campañas de sextorsión generalmente consisten en correos electrónicos que extorsionan al destinatario:

a) Por medio de un supuesto video privado, que no existe, solicitando un pago en criptomonedas para no hacerlo público.

b) Por medio de un video privado creado utilizando inteligencia artificial y solicitando un pago en criptomonedas para no hacerlo público.

c) Por medio de un video privado obtenido previamente mediante un acceso fraudulento al dispositivo o sistema que lo aloja y solicitando un pago en criptomonedas para no hacerlo público.

d) Por medio de un supuesto video privado, que no existe, solicitando instalar un determinado software malicioso de control remoto para no hacerlo público.

3. Las campañas de envío de software malicioso o malware que realizan los ciberdelincuentes por correo electrónico generalmente se realizan utilizando una de las siguientes técnicas:

a) Malware incrustado en el propio correo que en el momento de ser abierto infecta el equipo.

b) Documentos adjuntos maliciosos.

c) Enlaces maliciosos a páginas web.

d) La «b» y la «c».

4. Comprobar el remitente de los correos electrónicos es una de las mejores formas para diferenciar si una comunicación es fraudulenta o no. Ante un correo enviado por una supuesta entidad bancaria llamada Lesan Bank, ¿cuál de los siguientes remitentes sería más sospechoso de ser fraudulento?

a) no-reply@lesanbank.es

b) contact@lesanbank.es

c) no-reply@clientes.lesanbank.es

d) contact@lesanbank.es.banking.es

5. Ante una comunicación por correo electrónico cuyo remitente parece legítimo pero existen sospechas sobre su legitimidad, la mejor forma de proceder es:

a) Acceder a lo que solicita el correo, pero esto solamente si es abrir un archivo adjunto ya que los enlaces son más peligrosos.

b) Comprobar las cabeceras del correo con una herramienta especializada y ante la menor duda no interactuar con el correo de ninguna manera. Además es recomendable borrarlo directamente para evitar futuras situaciones peligrosas.

c) Acceder a lo que solicita el correo, pero esto solamente si solicita abrir un enlace o responder a la propia comunicación ya que los archivos adjuntos son más peligrosos.

d) Ninguna de las anteriores.

6. La ingenieria social consiste en:

a) Intentar forzar a la víctima a realizar una determinada acción que beneficie al ciberdelincuente como revelar información confidencial, abrir un enlace o descargar y ejecutar un archivo adjunto.

b) Suplantar a una entidad conocida, como a un banco, cambiando su página web.

c) Realizar campañas masivas de envío de correos electrónicos fraudulentos.

d) Enviar correos electrónicos de spam.

7. Con cual de las siguientes afirmaciones es falsa:

a) Cualquier documento adjunto en un correo electrónico debe ser una señal de alerta.

b) Las entidades legítimas por norma no envían enlaces en sus comunicaciones oficiales y solicitan al usuario que acceda al sitio web, utilizando su navegador web o la aplicación específica.

c) Los ciberdelincuentes utilizan técnicas de ingeniería social para engañar a sus víctimas y que realicen acciones, como abrir un adjunto malicioso o acceder a una web ilegítima.

d) El malware no puede venir en ficheros Excel ni en ficheros .zip, solo en ficheros .exe.

8. En el supuesto de haber descargado un archivo, bien sea en un adjunto de correo o por medio de una página web y tener dudas sobre si este puede ser malicioso o no, la mejor forma de proceder es:

a) Ejecutarlo, pero antes haber actualizado el antivirus ya que así ante un posible malware el equipo estará protegido.

b) Analizarlo con una herramienta especializada como VirusTotal y en caso de duda, no ejecutarlo y borrarlo.

c) Analizarlo con una herramienta especializada como VirusTotal y después ejecutarlo, ya que esta habrá eliminado todo rastro de malware en caso de existir.

d) Borrarlo sin realizar ninguna comprobación.

9. Cuando hay que enviar un correo a múltiples destinatarios, estos se deben añadir utilizando la opción:

a) CC o Carbon Copy.

b) En el campo Para.

c) En el campo CCO o Blind Carbon Copy.

d) No se puede hacer ya que la LOPDGDD puede llegar a sancionar a la empresa destinataria por considerar los correos como spam.

10. Cuando se recibe un correo electrónico sospechoso, para verificar si es fraudulento nos fijaremos en

a) En el remitente que puede estar falseado, para ver si es conocido y si está bien escrito.

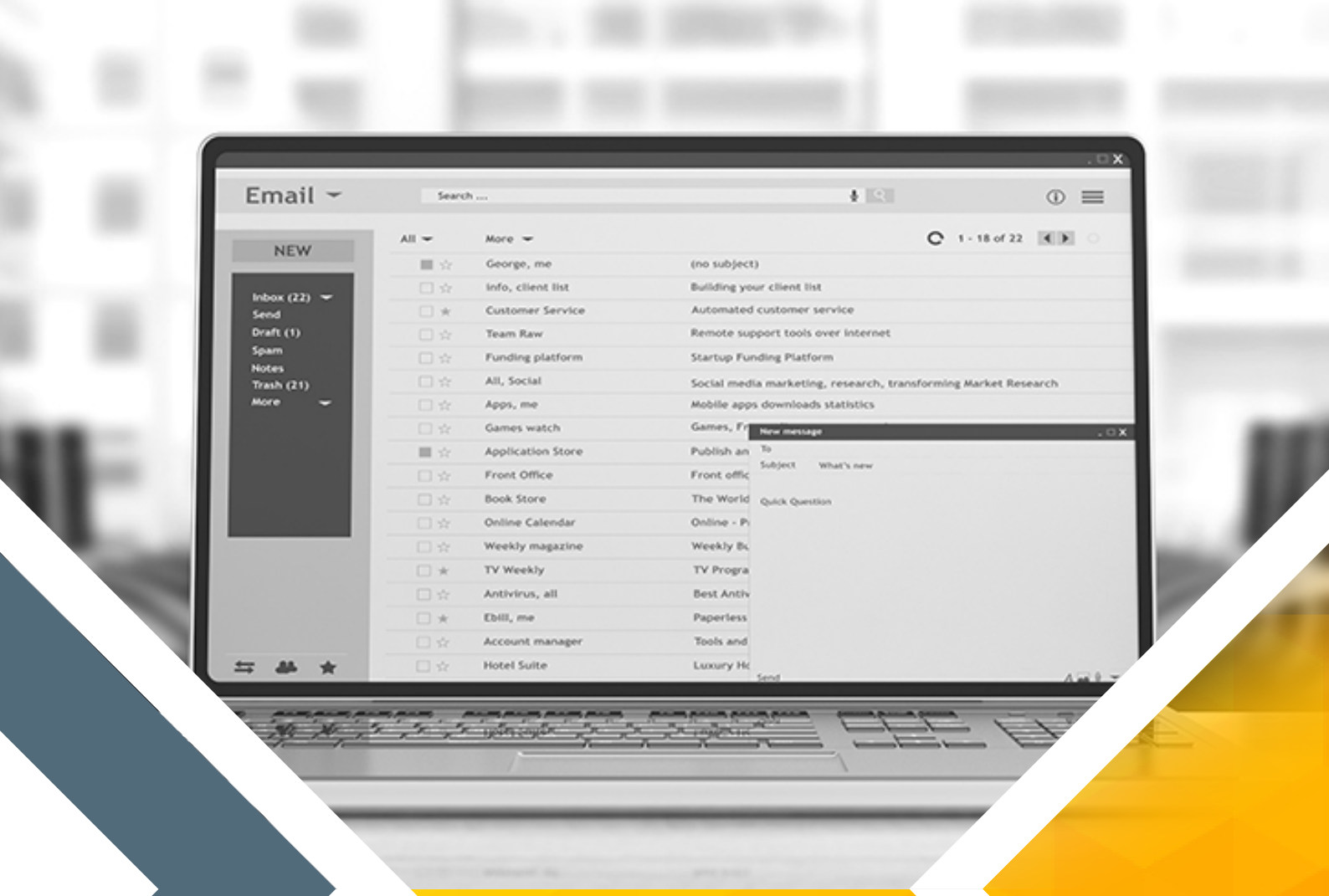
b) En el remitente que puede estar falseado, en el cuerpo y asunto para detectar posibles engaños, en los adjuntos que pueden ser maliciosos y en los enlaces que pueden estar falseados.

c) En el cuerpo para ver si están bien escritos, si se dirige a nosotros de manera impersonal y si nos insta a realizar una descarga o visitar una web.

d) En los adjuntos que pueden ser maliciosos y en si lleva enlaces que pueden estar falseados.

SOLUCIONES

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



TEST DE EVALUACIÓN

EL CORREO ELECTRÓNICO

Principales fraudes y riesgos.

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