¿Estáis preparados?

Descripción del Reto 4: ingeniería social

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL

Índice

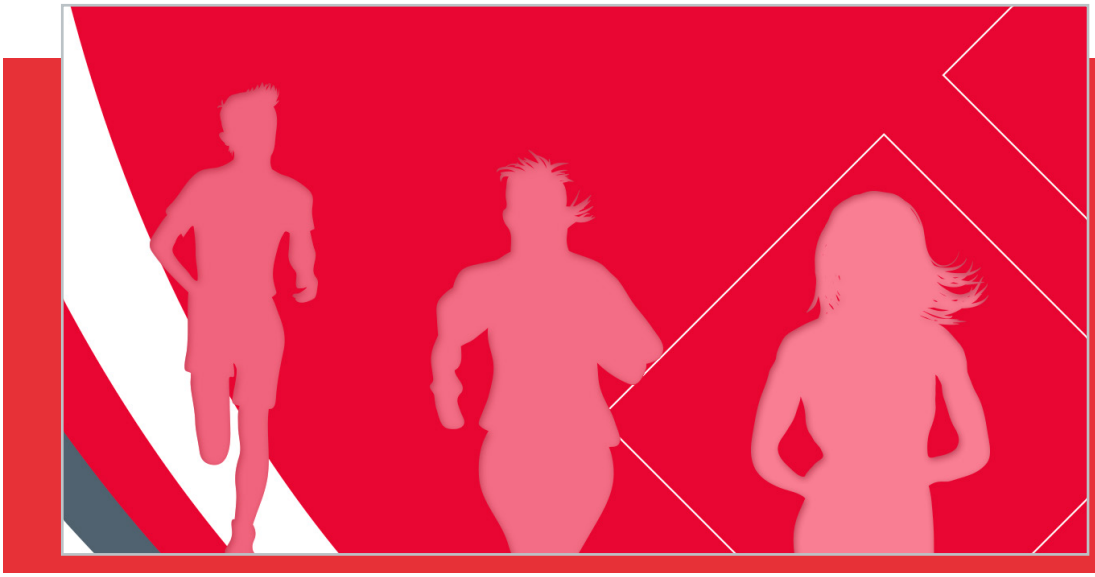
Ingeniería Social

R.4 Descripción del ataque por ingeniería social

Este es el material que se ha de entregar al equipo para debatir sobre el incidente con ayuda de la presentación.

1.1 Escenario

- Formáis parte de un negocio que tiene una oficina con algunos ordenadores, una red con wifi y conexión a internet.
- En vuestra empresa, la información se emplea para contactar con clientes y proveedores, mantener la página web de la tienda online, elaborar las facturas, intercambiar datos con la gestoría (RRHH, impuestos,...).
- Para vuestra actividad tenéis contratada una conexión a internet, los servicios de una gestoría y el soporte informático.
- Los empleados tienen un horario comercial.
- Los clientes contactan por teléfono, correo electrónico o presencialmente.



¿Respuesta a incidentes?

1.2 ¿Qúe ha pasado?

- Tras regresar de vacaciones, y al revisar los extractos bancarios de las operaciones de la empresa en la última semana, observáis que hay una serie de cargos extraños que no han sido autorizados ni justificados. Las órdenes de pago se han realizado fuera del horario comercial.
- Os ponéis en contacto con el banco para verificar estos movimientos. Os han informado que han sido realizados de forma correcta con las credenciales de facturación de la empresa.
- Preguntáis a los empleados que manejan la cuenta de facturación si habían notado algo extraño. En este caso, uno de ellos comenta que esos cargos los habría ordenado él jefe, pues hace unos días les había enviado un correo electrónico pidiendo las credenciales. En efecto, hay un correo dónde el jefe dice que está de vacaciones, que necesitaba realizar una transacción urgente y que no llevaba consigo las credenciales. Evidentemente no había sido él.
- Como el mensaje venía a su nombre, y no era la primera vez que las pedía, se las enviaron. No se fijaron que la dirección del remitente era falsa.

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL