**Proyecto del Curso de Ingeniería Social**

**Elaboración de Escenario de Pretexting**

**Instrucciones:** Para realizar la siguiente tarea siga los siguientes pasos:

1. Identifique un posible objetivo (***TARGET***) (el objetivo puede ser una persona, una empresa, una compañía, un servicio Web, etc.).
2. Haciendo uso de las siguientes herramientas realice una búsqueda de información sobre su objetivo:
   1. Visite los portales de Facebook, Twitter, LinkedIn y otras redes sociales.
   2. Recolecta imágenes.
   3. Estudie los gustos y preferencias del objetivo.
   4. Investigue amigos y hobbies.
   5. Open Source INTelligence (OSINT) Reference Sheet - <https://tpia.com/resources/Pictures/2019%20CPE%20files/OSINT%20Resources.pdf>
   6. Open Source Intelliegence Tools and Resources Handbook- <https://i-intelligence.eu/uploads/public-documents/OSINT_Handbook_June-2018_Final.pdf>
3. Vaya creando un Folder o un archivo (file), sobre los datos que vaya consiguiendo del objetivo:
   1. Screenshots, fotos, etc.
   2. Una vez recopilado la información, utilice la plantilla (Apéndice B) para ir preparando el informe sobre los resultados de la búsqueda de información.
   3. Provea las fuentes en donde encontró la información.
4. Con los datos de su objetivo y conociendo sus vulnerabilidades, proceda a diseñar un ataque de pretexting:
   1. Utilice la plantilla adjunta (Apéndice A) para crear el escenario.
   2. Ensaye su ataque.
   3. Grabe su ataque en un video: recuerde que los escenarios más efectivos son los que tienen al menos 3 a 4 de los principios de SE incorporados en el ataque.

APÉNDICE A

Plantilla de Pretexting

**Este ejemplo es realizado con un objetivo y nombres ficticios**

|  |
| --- |
| Nombre del Pretexto: Adeudo pendiente en cuenta empresarial.  Nombre del Cliente: Powerably INC.  Nombre del Proyecto: Validación de medidas anti-phishing. |

|  |
| --- |
| Nombre del Personaje: Andrés Olivas  Datos demográficos del Personaje:   * Español, algunas personas se abren más a un extranjero. * 30-35 años de edad.   Antecedentes del Personaje:   * Especialista en banca. * Trabaja en el área de cobranza. * Es manager del área, por lo que tiene “autoridad” |

|  |
| --- |
| Nombre del Objetivo: Jorge Cortéz  Datos demográficos de Objetivo:   * Mexicano. * 47 años de edad. * Reside en la ciudad Aguascalientes. * Padre de familia, tiene 2 hijos que no viven con él. * Acceso a internet desde computadora y teléfono. * Trabaja como supervisor de inventarios en distribución de alimentos en VFF Foods.   Resultados del OSINT:   * Redes sociales:   + <https://www.facebook.com/jorge.cortez123/>   + <https://twitter.com/jorgecortez1234>   + <https://www.linkedin.com/in/jorgecortez1234/> |

Script

|  |
| --- |
| **Introducción**  Asunto: URGENTE - Aviso de cobranza de BancoMéxico Referencia 1234  **Contexto**  Este es un mensaje importante para Jorge Cortez, Supervisor de Inventarios en VFF Foods. Si usted no es esta persona por favor ignora este mensaje y elimínalo.  Estimado,  Este es un recordatorio de que su cuenta en BancoMéxico aparece con un sobregiro. De acuerdo a nuestros registros, tiene un adeudo por $2,350.00 a Proveedor de Software S.A. de C.V. por concepto de licencia mensual InventarioMatic. Apreciamos que de ser posible haga su pago dentro de las próximas 24 horas para evitar intereses moratorios a través de [este enlace](https://www.youtube.com/watch?v=dQw4w9WgXcQ).  **CLOSING**  Si tiene alguna duda al respecto puede comunicarse al 01 800 123456 para aclararla.  Gracias por ser un valioso cliente de BancoMéxico.  **Palabras Claves**   1. **Urgente.** 2. **Deuda.** 3. **24 horas.** 4. **Jorge Cortez.** 5. **VFF Foods.** 6. **Supervisor de Inventarios.** 7. **BancoMéxico** |

**Apéndice B**

**Proyecto de Pretexting**

**Dossier Target**

**Target:**

**Jorge Cortez**

**Tabla de Contenidos**

[Resumen del Objetivo 3](#_heading=h.gjdgxs)

[Descripción de la Empresa/Persona 4](#_heading=h.30j0zll)

[Herramientas Utilizadas para la búsqueda 4](#_heading=h.1fob9te)

[Oportunidades/Vulnerabilidades 5](#_heading=h.3znysh7)

[Escenario de Pretexting 5](#_heading=h.2et92p0)

# Resumen del Objetivo

Jorge Cortez es un hombre mexicano, de 47 años de edad con educación media-superior concluida, se desempeña como supervisor de inventarios en VFF Foods. Lleva 2 meses en este empleo y de acuerdo a sus redes sociales aún está en periodo de prueba; según sus fotos tiene acceso a los sistemas de inventario, al cliente de correo electrónico y se hace a cargo de algunos pagos a proveedores.

Es divorciado, padre de familia de 2 hijos quienes ya no viven con él, ocasionalmente los ve los fines de semana y tiene un perro como mascota. Conduce un vehículo modelo Atos, año 2010 con los rótulos de VFF Foods.

# Descripción de la Empresa/Persona

VFF Foods es una empresa familiar que tiene 3 años en el mercado, cuenta con solo 6 empleados lo cual indica que cada persona es cercana a la familia propietaria teniendo acceso a información sensible y métodos de pago.

Fuentes:

https://www.facebook.com/vfffoods/

https://www.facebook.com/jorge.cortez123/

https://twitter.com/jorgecortez1234

https://www.linkedin.com/in/jorgecortez1234/

# Herramientas Utilizadas para la búsqueda

Ejemplos:

1. Google
2. Metagoofil
3. Facebook
4. LinkedIn
5. Twitter
6. Reddit.com
7. Netcraft
8. YouTube

# Oportunidades/Vulnerabilidades

Vulnerabilidades:

* Es una empresa familiar con poca cultura de tecnología.
* Accesos a sistemas de pagos están delegados.
* El objetivo es bastante activo en redes sociales.
* Existen diversos distractores en el lugar de trabajo.
* El personal de la empresa ha demostrado pasar llamadas telefónicas sin dificultad.

# Escenario de Pretexting

1. Se llamará por teléfono al objetivo durante la mañana en las primeras horas de trabajo.
2. Se le explicará que la llamada proviene de Proveedor de Software S.A. de C.V. con motivo de una factura vencida de pago.
3. Posteriormente se indicará que este pudo ser un error pero se revisará.
4. Después de la hora de comida se enviará email al objetivo con un email tracker para saber cuando lo haya abierto.
5. En el momento que abra el mail se le llamará por teléfono con otro motivo diferente como ventas de línea telefónica o algún otro tipo para distraerlo.
6. Minutos después se le llamará por parte de BancoMéxico explicando el mail que recibió y que puede llamar al número del mail o escribir a otra dirección para aclarar dudas/recibir indicaciones.
7. Se evaluará la velocidad en que el objetivo realiza algunas de estas acciones para definir el éxito del ataque.