

“Proyecto del Curso de Ingeniería Social”

Elaboración de Escenario de Pretexting

APÉNDICE A

Nombre del Pretexto: **Acceso exclusivo a Platzi Expert por 3 meses gratis.**

Nombre del Cliente: **PlatziNautas (víctimas objetivo de la campaña de phishing).**

Nombre del Proyecto: **Validación de medidas de seguridad contra phishing y ataques de ingeniería social.**

Nombre del Personaje: **Freddy Vega (Co-fundador de Platzi)**

Datos demográficos del Personaje: **(Edad: 30-40 años, Nacionalidad: Colombiano Ocupación: CEO y cofundador de Platzi)**

Antecedentes del personaje: **Freddy Vega es una figura pública muy activa en la comunidad tecnológica y educativa. Tiene un gran número de seguidores en redes sociales y es conocido por su participación en eventos educativos y tecnológicos. En este ataque de pretexting, se podría hacer uso de su imagen y autoridad para ofrecer de manera "confidencial" los tres meses gratuitos de acceso a Platzi, una oferta que parecería legítima debido a su alto perfil y conexión con la plataforma.**

Nombre del Objetivo: **PlatziNautas (Usuarios de Platzi)**

Datos demográficos de Objetivo: **(Personas de 18 a 40 años, Interesados en educación online y el desarrollo de habilidades tecnológicas, Usuarios de redes sociales como Twitter, Facebook y LinkedIn, Activos en comunidades digitales y tecnológicas)**

Resultados del OSINT:

- **Información general disponible sobre los seguidores de Freddy Vega y Platzi en redes sociales como LinkedIn, Twitter y Facebook.**
- **Información sobre las ofertas y campañas anteriores de Platzi publicadas en diversas plataformas.**
- **Comentarios y conversaciones en redes sociales donde los usuarios mencionan el interés en becas, ofertas especiales y suscripción gratuita a cursos.**

“Proyecto del Curso de Ingeniería Social”

Script:

Introducción:

Asunto: ¡3 meses gratis de Platzi Expert solo para ti!

Contexto

Hola, soy Freddy Vega, cofundador de Platzi. Te ofrezco 3 meses gratis de acceso a nuestra suscripción Platzi Expert, pero es un regalo que quiero mantener en secreto. Solo tú y unos pocos estudiantes tienen acceso a esta promoción especial.

Inicia sesión ahora mismo en el enlace de abajo para activar tu suscripción. No compartas esta oferta con nadie, ya que es personal y no quiero que el equipo de Platzi se entere. ¡Apúrate, sólo tienes unas pocas horas!

CLOSING

Haz clic aquí para obtener tus 3 meses gratis:
[\[https://erickddp.github.io/platzi-expert-login-phishing/\]](https://erickddp.github.io/platzi-expert-login-phishing/).

Una vez inicies sesión, tu suscripción se activará automáticamente. Esta es una oportunidad exclusiva, ¡no la dejes pasar!

Palabras Claves

- [3 meses gratis](#)
- [Freddy Vega](#)
- [Iniciar sesión ahora](#)
- [Acceso limitado](#)
- [Oferta secreta](#)
- [Platzi Expert](#)



“Proyecto del Curso de Ingeniería Social”



Términos y Condiciones:

El acceso a esta oferta es exclusivo y temporal, sujeto a disponibilidad de pases gratuitos y al cumplimiento de las políticas de Platzi. Esta oferta no es visible para todos los usuarios, solo para aquellos invitados a través de este acceso especial. Platzi no se hace responsable por problemas técnicos o pérdida de acceso. Para cualquier consulta, contáctanos en sopORTEEXCLUSIVO@platzi.com.

APÉNDICE B

Tabla de Contenidos

| | |
|--|----------|
| Resumen del Objetivo: | 4 |
| Descripción de la Empresa/Persona: | 4 |
| Herramientas Utilizadas para la búsqueda: | 4 |
| Oportunidades/Vulnerabilidades: | 5 |
| Escenario de Pretexting: | 5 |

“Proyecto del Curso de Ingeniería Social”

Objetivo del expediente

Usuarios de Platzi que desean acceder a una suscripción gratuita de 3 meses de Platzi Expert, confiando en la figura pública de Fredy Vega

Resumen del Objetivo:

El objetivo principal es atacar a los usuarios de Platzi (conocidos como "Platzinautas") mediante una página de phishing que promete 3 meses gratis de suscripción a cursos. El ataque se basa en explotar el deseo de las personas por acceder a contenido educativo gratuito y su confianza en la marca Platzi.

Descripción de la Empresa/Persona:

- **Fredy Vega**, Co-fundador de Platzi, es la figura que el ataque de pretexting simula. En este escenario, Fredy estaría ofreciendo una promoción secreta de 3 meses gratis a Platzi, a espaldas del equipo.
- **Platzinautas**: Los Platzinautas son los usuarios de la plataforma, personas interesadas en mejorar sus habilidades a través de cursos en línea. Muchos de ellos frecuentan foros, redes sociales, y otros espacios donde buscan ofertas y descuentos para acceder a cursos de manera gratuita o a precios reducidos.

Herramientas Utilizadas para la búsqueda:

- **Google**: Para investigar sobre la comunidad de Platzi y encontrar foros donde los Platzinautas interactúan.
- **Redes Sociales**: Facebook, Twitter, LinkedIn, YouTube, y Telegram para identificar plataformas donde los usuarios de Platzi son activos.
- **OSINT Tools**: Metagoofil y Netcraft para obtener correos electrónicos, información personal, y otros datos disponibles en la web de los usuarios de la plataforma.
- **Foros de Platzi y Grupos de Piratería**: Espacios donde los usuarios buscan contenido gratuito, siendo este un lugar idóneo para distribuir el enlace de phishing.

“Proyecto del Curso de Ingeniería Social”

Oportunidades/Vulnerabilidades:

- **Confianza en la Marca:** Los Platziusuarios confían en la marca y en sus fundadores, lo que facilita el engaño si el ataque parece venir de Fredy Vega.
- **Falta de Conocimiento en Ciberseguridad:** Muchos usuarios de Platzi pueden no tener formación en ciberseguridad, lo que aumenta su vulnerabilidad a este tipo de ataques.
- **Interés en Contenidos Gratuitos:** Los usuarios son altamente susceptibles a caer en la trampa debido a su deseo de acceder a contenido educativo gratuito.
- **Amplia Presencia en Plataformas:** Platzi tiene presencia en múltiples plataformas y comunidades, lo que aumenta el alcance del ataque.

Escenario de Pretexting:

- **Difusión del Enlace:** Se compartiría un enlace de phishing en foros de Platzi, grupos de Telegram, redes sociales y sitios donde los usuarios buscan ofertas. Se utiliza un perfil falso de Fredy Vega para darle legitimidad.
- **Página de Phishing:** La página imita el sitio oficial de Platzi y solicita al usuario iniciar sesión para reclamar su oferta de 3 meses gratis.
- **Robo de Credenciales y Malware:** Al iniciar sesión, se roban las credenciales de los usuarios y, adicionalmente, se descarga un troyano en sus dispositivos que compromete su información personal, incluyendo potencialmente datos bancarios.
- **Mensajes Personalizados:** Los usuarios más activos podrían recibir correos personalizados, supuestamente de Fredy Vega, para aumentar la credibilidad del ataque.
- **Educación y Alerta:** Al final del escenario, se alerta sobre los riesgos de caer en ofertas extremadamente atractivas en línea, reforzando la importancia de verificar la legitimidad de los mensajes y páginas que solicitan datos personales.