VIRUS
TROYANOS
PHISHING

APRENDA CÓMO ESTAR PROTEGIDO

Conozca cuáles son los vectores de ataques más utilizados por los ciberdelincuentes para robar dinero e información personal y confidencial

Durante la charla aprenderá cómo identificar un ataque de phishing dirigido a usted, cómo proteger de manera más segura su cuenta y cómo evitar que tomen control de su smartphone de forma remota

Mail: **info@isglatam.com** / WhatsApp: **+595 972 156975** /

ISG LATAM
https://www.isglatam.com
+595 972 156975
info@isglatam.com

[Calidad en Seguridad Informática]

Ciberataques a Usuarios

ISG LATAM
https://www.isglatam.com
+595 972 156975
info@isglatam.com

[Calidad en Seguridad Informática]

Presentación de la charla

La charla de concientización a todo público busca demostrar los principales peligros de los cibercriminales a los que se exponen día a día todas las personas, ya que actualmente todos somos usuarios de la tecnología, desde nuestro inseparable Smartphone, que se ha convertido en la puerta principal de entrada ilegal a nuestra información confidencial, hasta las PC de nuestras casas y/o de nuestro lugar de trabajo.

Los cibercriminales están constantemente buscando nuevas formas de acceder a información sensible y confidencial, por lo que el área de la ciberseguridad, como respuesta a estas nuevas formas, está en constante cambio y es más que conveniente que todos estemos en conocimiento de estas nuevas tendencias. Sin embargo, actualmente, el 99% de las personas no conocen estos peligros y, por ende, mucho menos cómo protegerse y qué hacer en caso de ser víctimas. Por eso, comprender las motivaciones, el proceso y la anatomía de un ciberataque puede resultar de gran ayuda a la hora de protegerse de estos ataques.

Para ello, la charla está dividida en 3 etapas. Durante la primera se tratan los aspectos de seguridad y la protección de datos e información sensible que los usuarios deben considerar cuando utilizan dispositivos móviles. En este punto es importante destacar que en la actualidad el ataque dirigido a dispositivos móviles, sobre todo a Smartphone, ha tenido un aumento exponencial y representa hoy en día una de las mayores amenazas para todas las personas.

La segunda etapa trata de las medidas de seguridad que el usuario debe considerar cuando realiza uso de un ordenador. Y en la tercera etapa, se explicará cómo proceder en caso de ser víctima de un ciberataque. Las 2 primeras etapas de la capacitación cuentan con demostraciones en vivo de situaciones reales del día a día de una persona, de cómo son realizados los ciberataques y cuáles son las recomendaciones a tener en cuenta para evitar los mismos, es decir, cómo protegerse de los ciberataques.

Una de las cosas interesantes que se verá en la charla, es la realización de demostraciones de técnicas de ciberataques en donde usaremos un dispositivo (mini-ordenador) preparado por nosotros especialmente para la charla. El dispositivo posibilita la demostración de distintos vectores de ataque a los que se exponen diariamente los usuarios. A continuación, la foto del dispositivo:

Este mini-ordenador permite la obtención de información, por ejemplo, la obtención de la agenda de contactos para los usuarios iOS que se conecten por bluetooth para escuchar música, aunque el ataque más riesgoso podría ser la copia completa de todo el sdcard del teléfono, incluyendo la base de datos de WhatsApp, o incluso peor, el copiado de recursos confidenciales que eventualmente estuviesen almacenados en la memoria.

ISG LATAM
https://www.isglatam.com
+595 972 156975
info@isglatam.com

[Calidad en Seguridad Informática]

Temario de la charla de concientización

Etapa 1 – Dispositivos Móviles:

- ✓ Ing. Social. ¿Qué es y cuáles son las técnicas más utilizadas para engañar al usuario?
- ✓ Desde un simple e-mail a tomar control de tu cuenta de Google y tu AppleID.
- ✓ El peligro de tener los asistentes habilitados (Siri y Google Assistant).
- ✓ El peligro de conectarse a dispositivos remotos desconocidos (Bluetooth y Wifi).
- ✓ Instalación de aplicaciones y navegación segura desde tu Smartphone.
- ✓ Virus, troyanos y Ransomware, cómo protegernos.
- ✓ Seguridad en las transacciones bancarias desde tu Smartphone.
- ✓ Backup y cifrado de datos.
- ✓ Recomendaciones generales para la protección de los dispositivos móviles.

Etapa 2 - Dispositivos de escritorio/notebook:

- ✓ Robo de Identidad.
- ✓ El peligro de conectar un pendrive encontrado en algún lugar.
- ✓ Los antivirus. ¿Qué tan confiable son?
- ✓ Instalación de nuevo software y navegación segura en Internet.
- ✓ Manejo de contraseñas robustas.
- ✓ Factor de doble autenticación.
- ✓ Seguridad en los cajeros automáticos.
- ✓ Seguridad al momento de pagar con tarjetas físicas.
- ✓ Seguridad en los pagos online realizados.
- ✓ Recomendaciones para evitar caer los diferentes tipos de ataques.

Etapa 3 - ¿Cómo proceder ante un ciberataque?

Instructores

Ing. Víctor David Casares, cuenta con las certificaciones de C|EH y OSCP, ha dictado cursos de Ethical Hacking para varios países de Latinoamérica, escribió el libro: Test de Intrusión Experiencias y Demostraciones Prácticas. Realiza test de intrusión Web| Mobile| Infraestructura| ATPs entre otros para empresas de primera línea. Participa activamente en conferencias internacionales como disertante, la última conferencia impartida fue en el DragonJar 2017 bajo la temática Pentesting a Plataflormas IoT.

Lic. Esteban Florentin, analista y desarrollador de sistemas web, en los lenguajes PHP y c# orientado a la seguridad informática y el desarrollo seguro de sistemas desde el inicio del mismo. Posee una Certificación Internacional en Auditoria de Seguridad de Sistemas en la universidad de Deloitte. Es consultor para importantes entidades en el ámbito educativo (a nivel nacional e internacional), instituciones del sector público y privado, brindando soluciones e implementaciones de sistemas Web y aplicaciones seguras, con más de 8 años de experiencia en el campo.