CYBECRIME AS A SERVICE (CAAS)

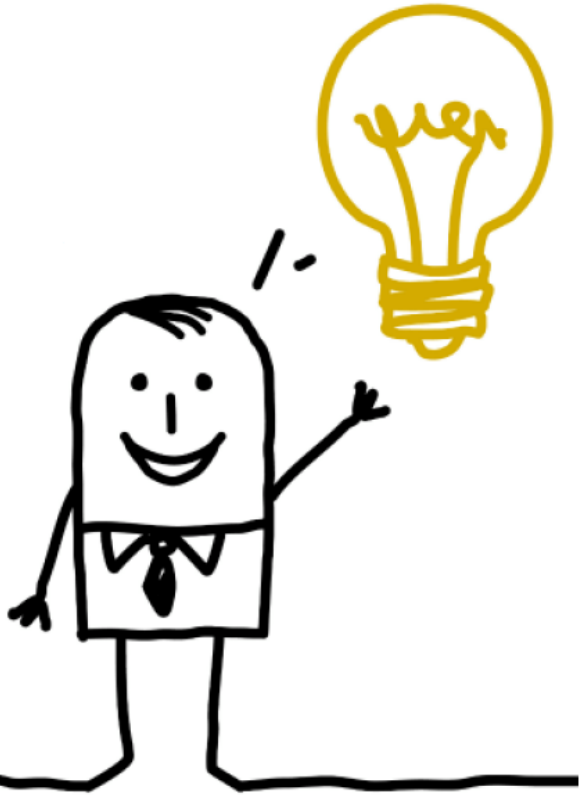
-investigando los tipos de estafas que involucran tecnología, phishing, drive by pharming, ransonware, estafas con tarjetas de crédito, rastreo de emails-

Cibercrimen » ciberdelitos conceptos

- "una definición universal de ciberdelito sigue siendo difícil, cada vez está menos claro si el **delito cibernético se refiere a** aspectos legales, sociológicos, tecnológicos o legales del delito…" (fuente: International Journal of Cyber Criminology, Vol 9 Issue 1 January – June 2015)
- pero siempre debemos basarnos en el principio: **"nullum crimen sine lege" » "ningún delito, ninguna pena sin ley previa" » conducta típica, antijurídica y culpable**
- **cibercrimen » actividades criminales perpetradas en el entorno digital** (incluye dispositivos electrónicos, computadoras, redes lan, wan, cloud computing, internet de las cosas…)

pero cibercrimen **no necesariamente involucra nuevos delitos**, es más **la mayoría son delitos bastante antiguos**» fraude, extorsión, divlugación de información privada, corrupción de menores, explotación sexual, estafas...

¿hay algun delito nuevo?



Módulo 3 – **Ciberestafas más comunes hoy**

- engaño del covid-19
- fraude del ceo
- ud ha sido hackeado
- estafa de black friday y mercados online
- phishing
- drive by pharming
- sextorsión
- ransonware
- estafas con trajetas de crédito
- troyanos de acceso remoto

Módulo 3 – **Cybecrime as a Service (CaaS)**

- la ciberdelincuencia de hoy dejo de **lado la intimidad y la soledad** para pasar a formar **grandes y pequeñas células de delincuencia organizada**.
- **factores** → globalización, hipercomunicacion, inacción judicial, inacción policial…

- tienen **especializaciones muy variadas**, estan los que hacen **ransonware**, lo **sextorsionadores**, los **skimmers**, los **clonadores**, los que toman control de **botnets**, los que **desarrollan malware**, los que los **venden en mercados online** …

Módulo 3 – **Cybecrime as a Service (CaaS)**

- esta variedad **de grupos dedicados a la ciberdelincuencia** está creando toda **una nueva economía** conocida como **'cybercrime as a service'**, caas
- tienen roles, funciones y jerarquías **bien definidas y organizadas:** a partir de esta estructura básica, el funcionamiento de la comunidad de ciberdelincuentes **no se diferencia mucho de cualquier otra estructura**

Módulo 3 – **Cybecrime as a Service (CaaS)**

funcionamiento del carrito de mercado online del cibercrimen: (fuente buguroo.com)

- **autenticación** → los delincuentes se **registran** y se les asigna una **identificación** única
- **motores de búsqueda** → pueden hacer comentarios y buscar los realizados por otros delincuentes, de tal forma que se genera un **sitio de interacción de confianza.**
- **reputación online** → en relación con esto, es posible establecer un sistema de **"puntos de reputación",** estos puntos pueden influir en el estatus del delincuente igual que cualquier mercado online.
- **administración confiable→ hay moderadores que administran y supervisan** estas comunicaciones. este sistema de regulación resulta básico para el buen funcionamiento del mercado.

Módulo 3 – **Cybecrime as a Service (CaaS)**

los servicios que se ofrecen:

- **data**: donde el servicio que se ofrece es el **intercambio de datos robados**: tarjetas de crédito, contraseñas, direcciones de correo electrónico…
- **hacking**: que consiste precisamente en poner un **hacker de sombrero negro a disposición de lo que necesite** el cliente.
- **translation**: es un servicio de **traducción y adaptación del lenguaje** para mejorar las campañas de phishing y que así parezcan más creíbles, en algunos casos, este servicio puede ser **complementario al diseño y clonado de webs** para que parezcan como auténticas.

Módulo 3 – **Cybecrime as a Service (CaaS)**

los servicios que se ofrecen:

- **money laundering:** en relación con lo anterior, el phishing **necesita una estructura de lavado de dinero,** para lo cual se suele requerir de la participación de las llamadas "mulas" que son seleccionadas y aportadas por este servicio, junto con todo el **proceso financiero de blanqueo de capitales**
- **malware**: precisamente consiste en diseñar, construir y poner en marcha **malwares para terceras personas.** este tipo **de servicios se ofrecen con multitud de "extras":** diseños a medida, garantía de infección, versiones premium, servicio técnico postventa…

Módulo 3 – **cibercrimen vectores de ataque**

- **ingeniería social**: es la herramienta más usada por los delincuentes → **enviar correos electrónicos, sms o generar cadenas virales por redes sociales con enlaces maliciosos** para descargar archivos o rellenar formularios con los que obtener información sensible de usuarios o datos de acceso

- **'spyware'**: es un 'malware' cuyo objetivo principal es **obtener información que poder utilizar o vender** posteriormente, generalmente información médica y financiera.

Módulo 3 – **cibercrimen vectores de ataque**

- **troyano**: el objetivo de este 'malware' **es tomar control de los dispositivos** → pueden utilizarlos para hacer operaciones fraudulentas con direcciones ip inocentes o para construir 'botnets' entre otras funciones.

- **'ransomware'**: este 'malware' **cifra los dispositivos con una clave desconocida** para el usuario, **pide un rescate** para poder descifrar y recuperar la información

Módulo 3 – ojo con los recomendadores de siempre

El crecimiento de las estafas románticas

Factores como la crisis económica y el auge de las redes sociales han hecho crecer este tipo de estafas notablemente. Por eso debemos tener precaución de cualquier extraño, por mucho que nos atraiga.

Este tipo de estafadores se aprovechan de la crecie[illegible]bre-exposición que existe en las redes sociales. Subimos demasiada in[illegible]ión sobre nosotros mismos a Internet, por lo que es fácil saber qué nos [illegible]a y qué no. A su vez, explotan la **sensación de soledad y aislamiento que generan las redes sociales** desde hace años.

e esta estafa son los casos de extorsión como **el grooming** (para un ven). En cualquier caso, si conocemos a alguien por Internet, no ar en esa persona hasta haberla conocido en persona y haber ue no supone una amenaza.

Módulo 3 – ojo con los recomendadores de siempre

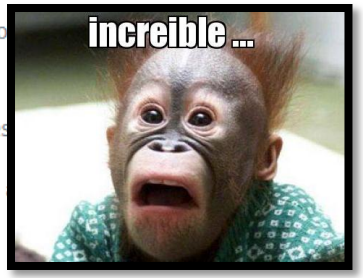
pero si es x mail?

paginas eurpeas??

otra vez que tienen que ver las contraseñas!!!!

- **Utilizar páginas web de confianza**: Con protocolo https y conexión directa. Fundamental fijarse si la página web cuenta con los datos de identificación de la empresa en el aviso legal. Se recomienda contratar preferentemente con páginas europeas.
- Revise las **condiciones de compra** de la web. El cliente debe informarse y comprobar las condiciones generales de contratación antes de realizar cualquier adquisición, los plazos de devolución y cuanto nos cobrarán por los gastos de envío.
- **Utilizar contraseñas seguras** en sus dispositivos desde los que se realiza la conexión.
- **No responder a correos que nos solicitan datos personales**, incluidos los datos bancarios, ni pinchar en enlaces o descargar ficheros adjuntos sin antes comprobar su procedencia.
- **Cuidado con las tarjetas bancarias.** Se aconseja utilizar una tarjeta para uso exclusivo de compras o recarga y a la vez autónoma de las cuentas bancarias.
- **Ojo con las ofertas o descuentos desorbitados**, detrás de ellos suelen encontrarse muchas de las es

Y, sobre todo, si considera que está siendo víctima de una ciberestafa, **actúe con inmediatez, denunciando con urgencia la situación.**



Módulo 3 – este si es un post recomendable

No todo lo que circula por Internet tiene por qué ser cierto

Artículo del blog

Sabías que las fake news preocupan al 86% de internautas españoles

Artículo del blog

Ponle freno a los fraudes y bulos con buenas prácticas

Artículo del blog

Deepfakes, ¿cómo se aprovechan de esta tecnología para engañarnos?

Christian Javier Vila

CTO Director de Tecnologías – ISEC Global Inc.

CIEH Certified Ethical Hacker, EC Council.

Sub Inspector (r) de la Policía de Seguridad Aeroportuaria

Especialista Investigación de Homicidios (MAT N° 510, ACRA)

Agente de Inteligencia (FAA)

notrootanymore@gmail.com

enlace a linkedin

enlace a investigaciones y exposiciones aquí

eof ()