NUEVAS HERRAMIENTAS INVESTIGATIVAS CONTRA LA CRIMINALIDAD ORGANIZADA ORIENTADA A LA PESQUISA DE DELITOS ECONÓMICOS

2023

ECO
Estudio sobre el Crimen Organizado

AMFM
MCML XXV

29-06-2023 - Morón, P.B.A.

ESTA PRESENTACIÓN FORMA PARTE DE

Proyecto
Libro Azul

PARA MÁS INFORMACIÓN, CONTACTÁNOS:

@ASOCIACIONECO

INFORMATE@ACECO.ORG.AR

AGUSTINA DEL ROSARIO ANZISI

ABOGADA PENALISTA - UBA

ESPECIALIZACIÓN EN CIBERCRIMEN Y EVIDENCIA DIGITAL - UBA

MINISTERIO PÚBLICO FISCAL DE LA NACION

MIEMBRO DE LA ASOCIACION CIVIL DE ESTUDIOS SOBRE EL CRIMEN ORGANIZADO

A G U S T I N A . A N Z I S I @ G M A I L . C O M

HERRAMIENTAS DIGITALES DE INVESTIGACIÓN

- INTELIGENCIA. CONCEPTO. TIPOS
- INGENIERÍA SOCIAL.
- OSINT
- EMPRESAS PRIVADAS
- COOPERACIÓN INTERNACIONAL
- REGULACIÓN

INTELIGENCIA

EL PRODUCTO RESULTANTE DE RECOLECTAR, EVALUAR E INTERPRETAR LA INFORMACIÓN DISPONIBLE QUE OFRECE VALOR INMEDIATO

INTELIGENCIA: LEGISLACION

LEY 25.520
"...ARTICULO 2° — A LOS FINES DE LA PRESENTE LEY Y DE LAS ACTIVIDADES REGULADAS POR LA MISMA, SE ENTENDERÁ POR:

1. INTELIGENCIA NACIONAL A LA ACTIVIDAD CONSISTENTE EN LA OBTENCIÓN, REUNIÓN, SISTEMATIZACIÓN Y ANÁLISIS DE LA INFORMACIÓN ESPECÍFICA REFERIDA A LOS HECHOS, AMENAZAS, RIESGOS Y CONFLICTOS QUE AFECTEN LA SEGURIDAD EXTERIOR E INTERIOR DE LA NACIÓN.

2. CONTRAINTELIGENCIA A LA ACTIVIDAD PROPIA DEL CAMPO DE LA INTELIGENCIA QUE SE REALIZA CON EL PROPÓSITO DE EVITAR ACTIVIDADES DE INTELIGENCIA DE ACTORES QUE REPRESENTEN AMENAZAS O RIESGOS PARA LA SEGURIDAD DEL ESTADO NACIONAL.

3. INTELIGENCIA CRIMINAL A LA PARTE DE LA INTELIGENCIA REFERIDA A LAS ACTIVIDADES CRIMINALES ESPECÍFICAS QUE, POR SU NATURALEZA, MAGNITUD, CONSECUENCIAS PREVISIBLES, PELIGROSIDAD O MODALIDADES, AFECTEN LA LIBERTAD, LA VIDA, EL PATRIMONIO DE LOS HABITANTES, SUS DERECHOS Y GARANTÍAS Y LAS INSTITUCIONES DEL SISTEMA REPRESENTATIVO, REPUBLICANO Y FEDERAL QUE ESTABLECE LA CONSTITUCIÓN NACIONAL..."

TIPOS DE INTELIGENCIA

OSINT:
FUENTES ABIERTAS DE INFORMACION

SIGINT:
INTERCEPCIÓN DE SEÑALES

IMINT:
BASADA EN IMÁGENES

ELINT:
SEÑALES ELÉCTRICAS

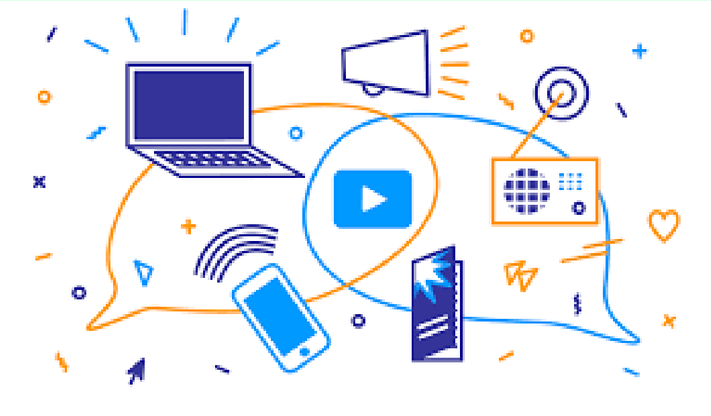
GEOINT:
IMÁGENES SATELITALES DE LA TIERRA

FININT:
INFORMACIÓN FINANCIERA

SOCINT:
REDES SOCIALES

OSINT (OPEN SOURCE INTELLIGENCE)

Aplicación de **inteligencia** a la información recopilada a través de la exploración de fuentes abiertas de información.
Comprende variadas técnicas para recopilar, analizar y darle un sentido a un conjunto de datos disponibles para todos.



FUENTES ABIERTAS DE INFORMACION

Aplicado al entorno digital, podría decirse que es todo aquello que se encuentra accesible en Internet sin restricciones de ningún tipo.
Pero también son fuentes los diarios, revistas, otros medios de comunicación, papers, foros, etc.

FUENTES ABIERTAS DE INFORMACION

Carlos Seisdedos y Vicente Aguilera (referentes en Europa) plantean que en nada obsta a una fuente de ser abierta su gratuidad.
Señalan que la condición de "abierta" radica en que cualquier persona podrá acceder a esa información de forma legal. No resulta relevante que tenga que pagar.

A nivel nacional no se describió lo mismo:
el Ministerio de Seguridad de la Nación planteó al respecto que entiende como fuentes digitales abiertas
"*...a los medios y plataformas de información y comunicación digital de carácter público, no sensible y sin clasificación de seguridad, cuyo acceso no implique una vulneración al derecho a la intimidad de las personas, conforme lo normado en la Ley de Protección de Datos Personales N° 25.326 y sus normas reglamentarias...*"

Resolución 144/2020 (RESOL-2020-144-APN-MSG). 2 de junio de 2020. Aprobación del "Protocolo General Para La Prevención Policial Del Delito Con Uso De Fuentes Digitales Abiertas". B.O. 34.395.

LISTADO DE FUENTES ABIERTAS DE LOS PAÍSES MIEMBRO DE LA RED DE RECUPERACION DE ACTIVOS DEL GAFILAT (RRAG)

HTTPS://WWW.GAFILAT.ORG/INDEX.PHP/EN/BIBLIOTECA-VIRTUAL/GAFILAT/DOCUMENTOS-DE-INTERES-17/PUBLICACIONES-WEB/4019-INVENTARIO-DE-FUENTES-ABIERTAS-RRAG-VERSION-PUBLICA/FILE

IDENTIFICACIÓN:
Se reconocen sitios de referencias y se contrastan las fuentes.

OBTENCIÓN:
Se implementan las herramientas que se utilizaran para la recolección de los datos. Existen aplicaciones útiles para ello, tales como plug-ins de Google (Nimbus capture, Nimbus clipper) y/o el programa OSIRT Browser.

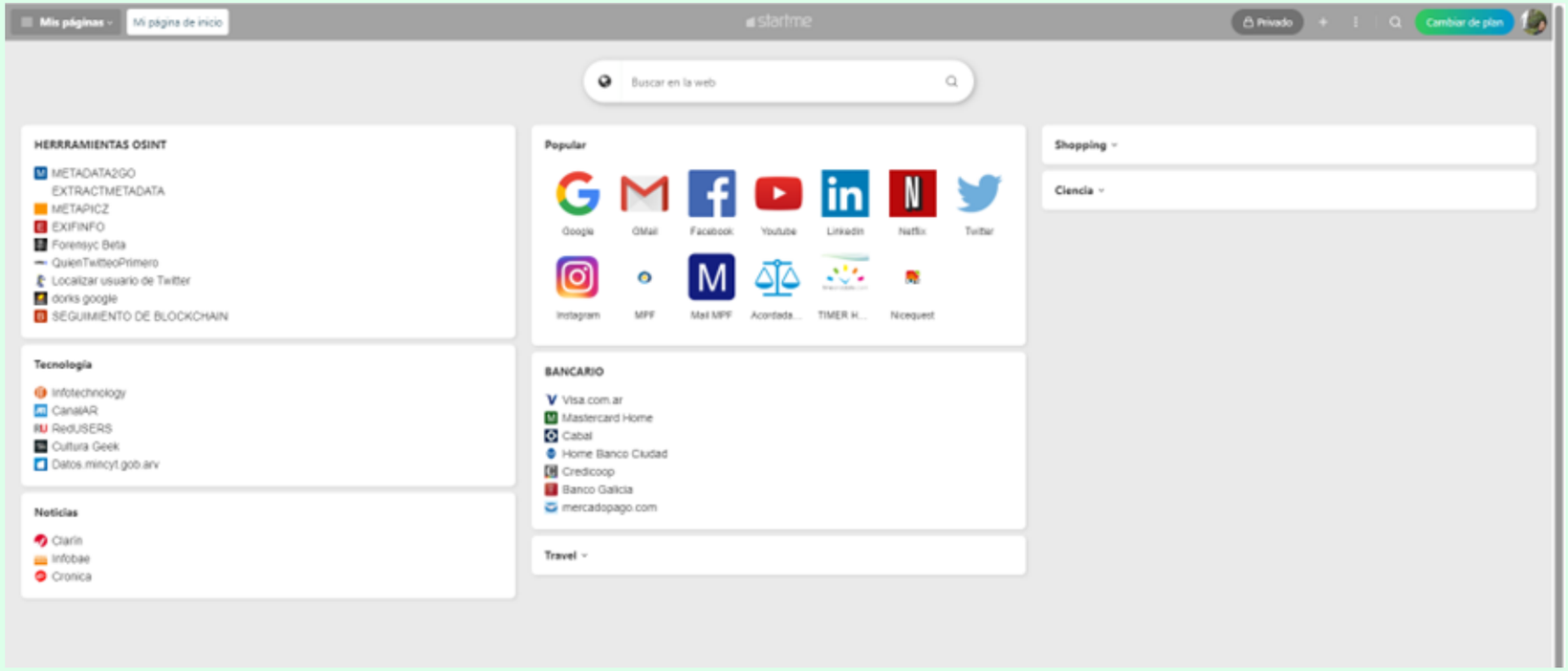
PROCESAMIENTO:
Consiste en dar formato y enriquecer los datos.

ANÁLISIS:
Comprende la contextualización, enriquecimiento, e incluso la aplicación de algoritmos para enriquecer la información.

REPORTE:
El informe debe ser legible y comprensible. Por ejemplo, Osirt Browser incluye dentro de sus funciones la emisión de un informe respecto de las tareas realizadas.

PASOS PARA EL INVESTIGADOR

PREPARACION:
Es el momento en que se definen los objetivos. Se equipa con herramientas, ya sea materiales para el espacio de trabajo o conocimiento por medio de capacitaciones. Algunas herramientas útiles son la agrupación de pestañas de Chrome, Start.me y Trello.



ALGUNOS MOTORES DE BÚSQUEDA

- DUCK DUCK GO
- GOOGLE
- BING
- YANDEX

OPERADORES DE BUSQUEDA Y GOOGLE DORKS

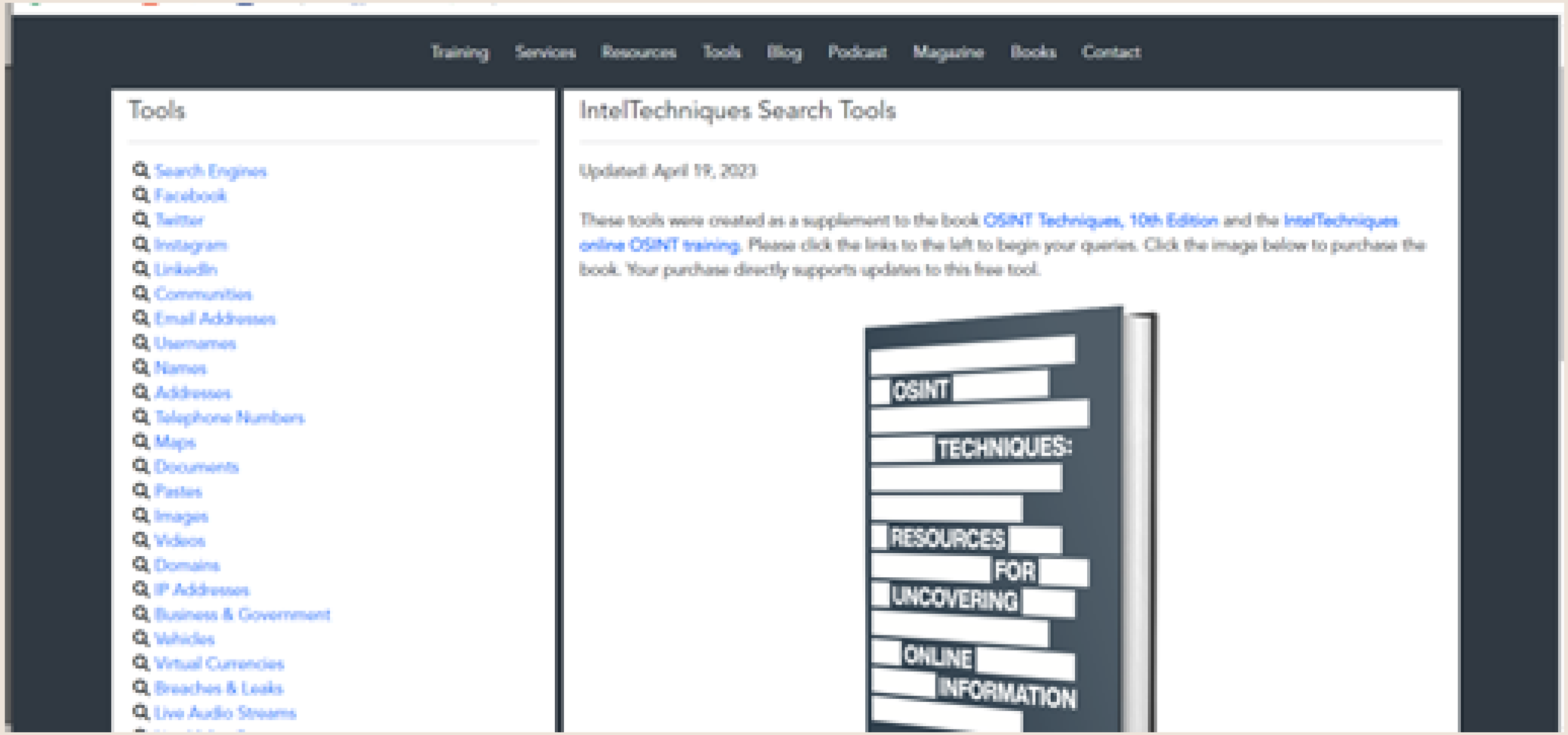
- "..." PARA PALABRAS EXACTAS
- + O - PARA EXCLUIR
- .. ENTRE DOS NÚMEROS PARA BUSCAR INTERVALO
- * COMODÍN
- OR ENTRE DOS PALABRAS ALTERNATIVAS
- SITE: PARA BUSCAR UN SITIO WEB
- RELATED: PARA BÚSQUEDA RELACIONADA
- CACHE: PARA VER EL RESULTADO ALOJADO EN GOOGLE

ES FUNDAMENTAL TENER IMAGINACIÓN

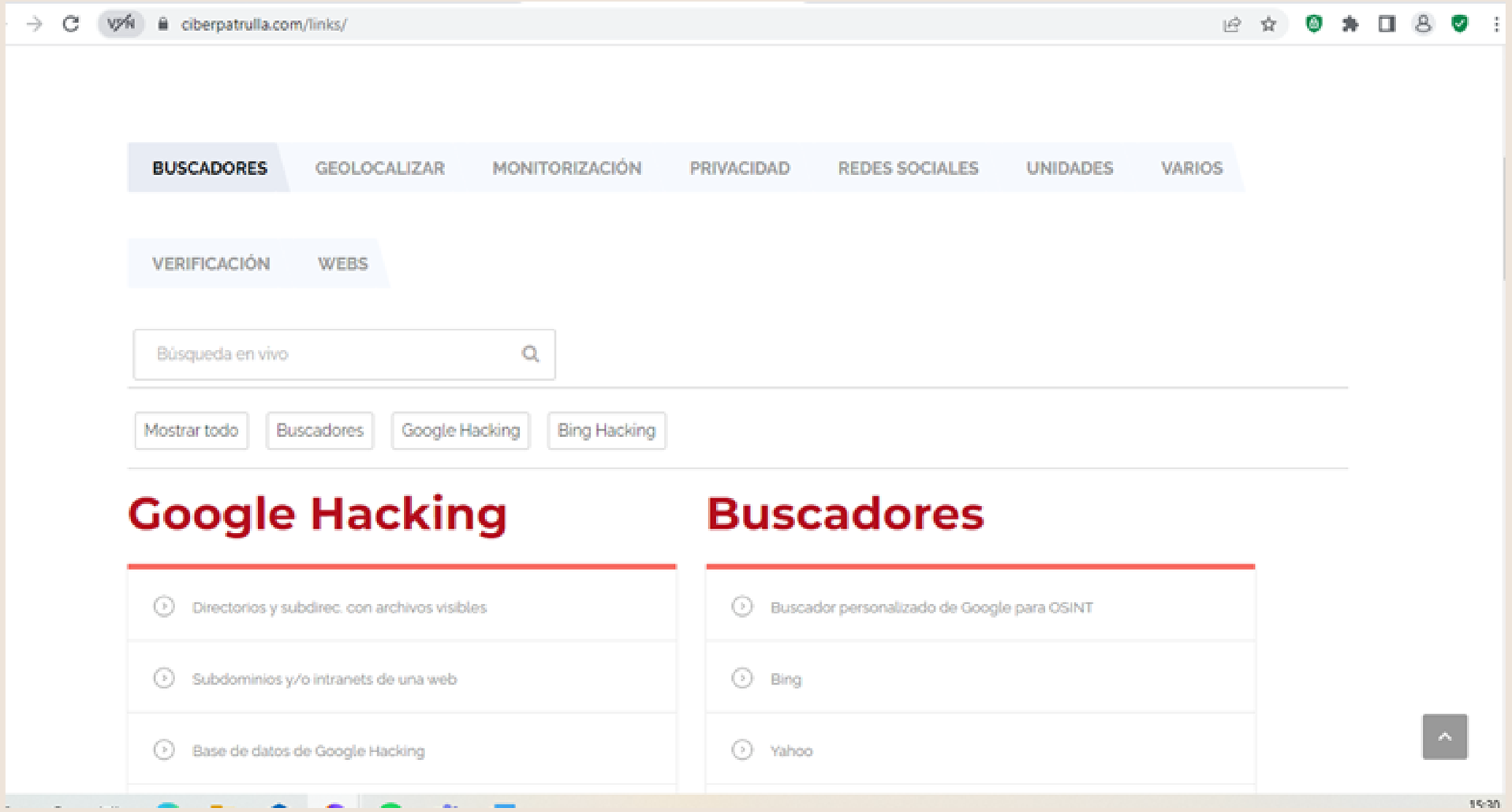
ALGUNOS RECURSOS UTILES:

- HTTPS://LOOKUP-ID.COM/

- HTTPS://INTELTECHNIQUES.COM/TOOLS/INDEX.HTML



- HTTPS://CIBERPATRULLA.COM/LINKS/



- https://namechk.com
- https://pipl.com
- https://numeracion.enacom.gob.ar/
- https://www.cuitonline.com/
- https://www.informemultiburo.com
- https://www.dateas.com/es
- https://seti.afip.gob.ar/padron-puc-constancia-internet/ConsultaConstanciaAction.do
- https://www.bcra.gob.ar/BCRAyVos/Situacion_Crediticia.asp
- https://www.bcra.gob.ar/SistemasFinancierosYdePagos/Entidades_financieras.asp
- https://www.telexplorer.com.ar
- https://tinfoleak.com/
- http://mentionmapp.com
- http://www.twimemachine.com/
- http://sleepingtime.org/
- https://www.instagram.com/explore/tags/nombre

INGENIERÍA SOCIAL

PUNTUALMENTE, RADICA EN LA EXPLOTACIÓN DE CARACTERÍSTICAS HUMANAS RECURRENTES PARA LOGRAR MANIPULAR O INFLUIR A UNA PERSONA, VARIAS O, INCLUSO, GRUPOS DE ELLAS, PARA QUE ACTÚEN DE UNA DETERMINADA MANERA, OPUESTA A LA REACCIÓN QUE INSTINTIVAMENTE SE DARÍA EN UN ENTORNO HABITUAL.

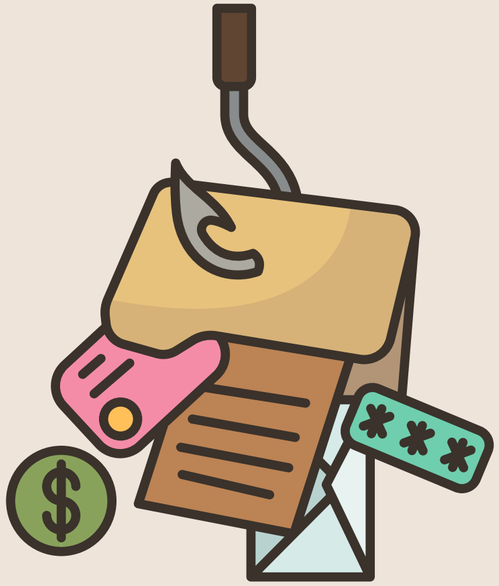
ESTAS CUALIDADES FRECUENTES QUE SE EXPLOTAN SON EL ALTRUISMO, LA VANIDAD, EL TEMOR O INCLUSO LA MERA CURIOSIDAD -ENTRE OTRAS-, LAS CUALES PUEDEN LLEVAR A LOS INDIVIDUOS A ACTUAR APRESURADAMENTE, CON DESESPERACIÓN O INCLUSO INSPIRADOS, SIN REFLEXIONAR PREVIAMENTE COMO LO HARÍAN ANTE UNA SITUACIÓN HABITUAL.

INGENIERÍA SOCIAL APLICADA:

EJEMPLO: HTTPS://YOUTU.BE/5OJVBXDTAXM

PHISHING

ENVÍO DE MENSAJES FALSOS COMO ANZUELO PARA ***“PESCAR”*** CONTRASEÑAS Y DATOS PERSONALES VALIOSOS
LAS MISIVAS PUEDEN SER CORREOS ELECTRÓNICOS, SMS, WHATSAPP, CARTA, ETC.



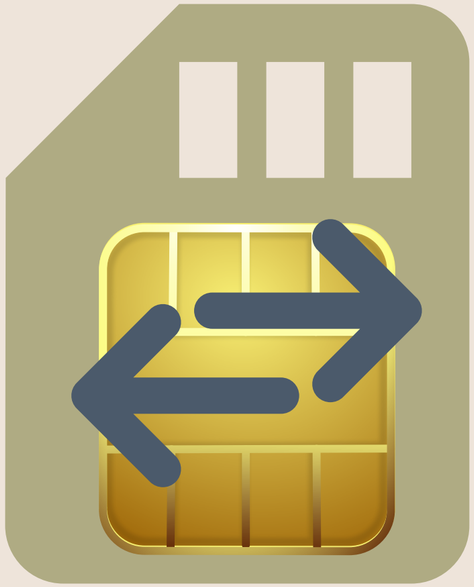
PHARMING

ES UNA PRÁCTICA DE EXPLOTACIÓN QUE SE REALIZA MEDIANTE LA INFILTRACIÓN DE ORDENADORES INDIVIDUALES O EL ENVENENAMIENTO DE UN SERVIDOR. AMBAS OPCIONES UTILIZAN UN CÓDIGO QUE REDIRIGE LOS SITIOS WEB, PERO CADA UNA SE EJECUTA DE FORMA DIFERENTE.

SMISHING Y VISHING

ES LA VARIANTE ESPECIFICA DE PHISHING DEFINIDA EN FUNCION DEL MEDIO DE COMUNICACION UTILIZADO PARA EL ENGAÑO.
PUEDE SMS O LLAMADA TELEFONICA

SIM SWAPPING



ES UN ATAQUE EN EL CUAL SECUESTRAN NUESTRA LÍNEA DE TELÉFONO MEDIANTE LA CLONACIÓN DE CHIP, EL ATACANTE RECIBIRÁ EN SU TELÉFONO EL CÓDIGO DE SEIS DÍGITOS PARA ACCEDER A NUESTRAS CUENTAS

Recomendaciones de la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI)

“SIMswapping”: alertan sobre el robo de cuentas de redes sociales, correo electrónico y bancarias mediante duplicación de la tarjeta SIM del celular

13.12.2021 en Ciberdelincuencia

La modalidad delictiva consiste en duplicar la tarjeta SIM de usuarios, que tienen asociados sus números de teléfono móvil como método de recuperación de contraseñas. Así, los atacantes acceden a las cuentas y sustraen la información. Consejos para evitar ser víctima de este ciberdelito.

RECURSOS DE ORGANIZACIONES PRIVADAS

SEGÚN LAS CONDICIONES DE SERVICIO, LAS DISTINTAS EMPRESAS RECOPILAN DIVERSA INFORMACION DE SUS USUARIOS.
EN LA MAYORIA DE LOS CASOS, LA INFORMACION DE SUSCRIPTO ES POSIBLE SOLICITARLA SIN EXHORTO INTERNACIONAL.

ALGUNAS EMPRESAS HAN DESARROLLADO SUS PROPIOS PORTALES PARA REQUERIR INFORMACION

META

TODO LO REFERENTE A INSTAGRAM Y FACEBOOK PUEDE SOLICITARSE MEDIANTE EL PORTAL

HTTPS://WWW.FACEBOOK.COM/RECORDS/LOGIN/

DE IGUAL MODO, WHATSAPP TIENE SU PROPIA PLATAFORMA

HTTPS://WWW.WHATSAPP.COM/RECORDS/LOGIN/

Service	Facebook
Target	10005[redacted]
Account Identifier	facebook.com/[redacted]
Account Type	User
Generated	2023-01-05 15:51:54 UTC
Date Range	2022-04-01 00:00:00 UTC to 2022-10-19 23:59:59 UTC
Ncmec Reports Definition	NCMEC Cybertips: NCMEC cybertip reports associated to the account of the sender. CyberTip ID: Unique identifier associated with the cybertip. Time: Date and time the NCMEC cybertip was sent. Responsible Id: Identification number of the sender's Facebook account associated with the NCMEC cybertip report.
NCMEC CyberTip Numbers	No responsive records located
Name Definition	Name: Name provided by the account holder. First: First name provided by the account holder. Middle: Middle name provided by the account holder. Last: Last name provided by the account holder.
Name	**First** [redacted] **Middle** **Last** [redacted]
Emails Definition	Registered Email Addresses: Displays a list of registered email addresses. To "register" an address, it requires confirmation by the account holder.
Registered Email Addresses	[redacted]
Vanity Definition	Vanity: Username associated with the account.
Vanity Name	[redacted]
Registration Date Definition	Registration Date: Date and time of account creation.
Registration Date	2020-04-27 19:49:59 UTC
Registration Ip Definition	IP address associated with account creation.
Registration Ip	186.143.202.22

Service WhatsApp
Account Identifier +5491[redacted]
Account Type WhatsAppUser
Generated 2023-03-28 17:30:16 UTC
Date Range 2023-03-01 00:00:00 UTC to 2023-03-13 23:59:59 UTC

Emails Definition Emails: Account holder's recovery email (if provided by the account holder)

Registered Email Addresses No responsive records located

Connection Info Definition
Connection Info: Account connection and device information (if available)
App Version: Latest version of WhatsApp running on the account holders mobile device
Connected From Address: Full IP address with port number when the account holder is currently online only
Connection State: Account holder's current connection status
Connection Time: Date and time stamp related to account holder's current connection status
Device OS Build Number: Mobile device's current operating system
Device Type: Account holder's type of device I.E. iPhone, Samsung, Web etc.
Inactive Since: Date and time since the account holder has been inactive - the account holder is not actively using the app but has it running in the background of their mobile device
Last Connected IP: Account holder is currently offline and reflects the last captured online IP without port number
Last Seen: Last date and time the account holder opened and viewed the app before going offline
Push Name: Name provided (if available) by the account holder
Service Start: Date and time the account holder registered the mobile device to start using WhatsApp on their phone

Connection

Device Id	0
Service start	2023-01-20 05:41:56 UTC
Device Type	iPhone
App Version	2.23.3.77
Device OS Build Number	os: 15.7.1, model: Apple iPhone 7
Connection State	OFFLINE
Last seen	2023-03-21 03:30:32 UTC
Last IP	181.46.57.107

Web Info Definition
Web Info: Information about the account holder's webclient/WhatsApp desktop app (if available)
Availability: Status of webclient (if available)
Online Since: Date/time of last session initiated on webclient (if available)
Platform: Type of device being used (Mac, PC, etc) (if available)
Version: Current WhatsApp webclient version (if available)

Web Info No responsive records located

Small Medium

ES FUNDAMENTAL ENTENDER QUE LAS EMPRESAS EXTRANJERAS **ELIGEN** COLABORAR, PERO NO ESTÁN OBLIGADAS A HACERLO. ADEMÁS LO HACEN SEGÚN SUS TÉRMINOS DE COOPERACIÓN. PARA SABER QUÉ INFORMACIÓN CONSERVAN, SE DEBEN LEER SUS TERMINOS Y CONDICIONES Y/O POLITICAS DE PRIVACIDAD DE LOS DATOS.

Convenio de Budapest

CONSEJO DE EUROPA - BUDAPEST, HUNGRÍA

SE FIRMÓ EL 23 DE NOVIEMBRE DE 2001 Y ENTRÓ EN VIGOR EL 1° DE JULIO DE 2004.
ES EL PRIMER TRATADO INTERNACIONAL CON EL OBJETO DE PROTEGER A LA SOCIEDAD FRENTE A LOS DELITOS INFORMÁTICOS Y LOS DELITOS EN INTERNET.
DELIMITA DIRECTRICES A SEGUIR LEGISLATIVAMENTE POR LOS ESTADOS.
DEFINE TERMINOLOGÍA

HTTPS://WWW.OAS.ORG/JURIDICO/ENGLISH/CYB_PRY_CONVENIO.PDF

SEGUNDO PROTOCOLO ADICIONAL DE LA CONVENCIÓN DE BUDAPEST

14/07/2021 - ESTRASBURGO, FRANCIA

EL OBJETO PRINCIPAL DE ESTE INSTRUMENTO FUE DEFINIR LAS REGLAS INTERNACIONALES COMUNES PARA REFORZAR LA COOPERACIÓN INTERNACIONAL EN MATERIA DE CIBERDELINCUENCIA Y DE OBTENCIÓN DE PRUEBAS DIGITALES EN LAS INVESTIGACIONES Y PROCESOS PENALES CUANDO SE ENCUENTRA ALOJADA EN EXTRAÑA JURISDICCIÓN

HTTPS://DATA.CONSILIUM.EUROPA.EU/DOC/DOCUMENT/ST-14898-2021-INIT/ES/PDF

¿DUDAS?

@ASOCIACIONECO

INFORMATE@ACECO.ORG.AR

AGUSTINA.ANZISI@GMAIL.COM

Proyecto
Libro Azul

¡MUCHAS GRACIAS!