Prevención y Sensibilización sobre los Nuevos Riesgos Digitales

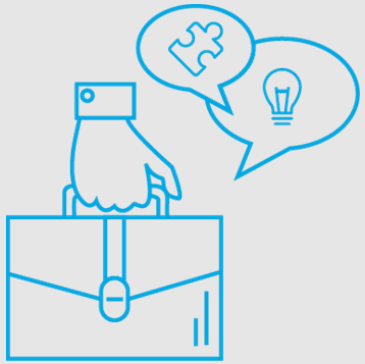
Ciberseguridad, El efecto pandémico en niños y familias

Agosto 2020

BTR Consulting
BUSINESS DIGITAL SOLUTIONS

RSM

CONSULTORÍA - PRINCIPALES SERVICIOS



DISEÑO ORGANIZACIONAL

- Diseño de Procesos Adm
- Normas Internacionales
- Selección de ERP
- Implementación de Sistemas
- Selección de RR.HH.

ASESORAMIENTO EN RIESGO

- Protección de Datos
- SOX Compliance
- Auditoria Interna de Procesos
- Forensic Investigations
- Control de Lavado de Dinero
- Anti-Corrupción
- Cibersecurity

FINANZAS CORPORATIVAS

- Fusiones y Adquisiciones
- Transaction Support
- Due Diligence
- Asistencia en Procesos de Insolvencia
- Valuaciones

RSM

BTR en el mundo

+500
Proyectos

+35
Países en los que prestamos servicios

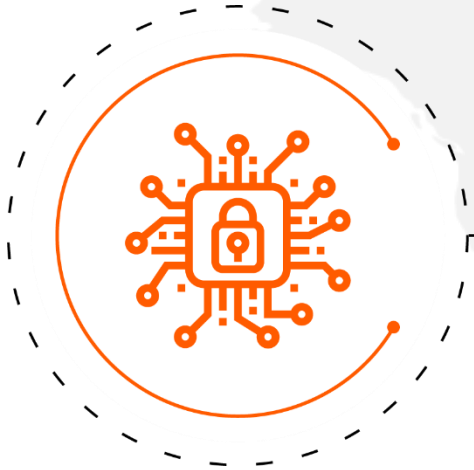
+200
Companías

Proyectos realizados en:

Arabia Saudita • Argentina • Bolivia • Brasil • Canadá • Chile • China Colombia • Ecuador • Emiratos Arabes • España • Filipinas • Paraguay Rumania • Sudáfrica • Uruguay • USA • y otros...

Servicios BTR Consulting

Cybersecurity



- EVALUACIOŃ Y OPERACIÓN DE CIBERSEGURIDAD
- SERVICIO DE MONITOREO / SOC
- HACKEO ETÍCO

Risk & Audit

- AUDITORÍA INTERNA
- COMPLIANCE
- CONTINUIDAD DE NEGOCIOS
- GESTIÓN DE RIESGOS

Consulting

- NEGOCIOS
- INFRAESTRUCTURA Y NUBE
- SOFTWARE

Knowlegde

- CIBERSEGURIDAD
- TALENTO DIGITAL

Alucinación invertida

Nueva normalidad

Contexto actual

Si ya era poco el tiempo que pasábamos en el "**mundo real**", ahora, la gran mayoría de nosotros está viviendo en la "**realidad virtual**".

Tormenta perfecta de oportunidades

RSM BTR Consulting
BUSINESS DIGITAL SOLUTIONS

8.5 Billones

de usuarios y dispositivos
en línea al mismo tiempo

#COMERCIO #EDUCACION #RELACIONAMIENTO #ENTRETENIMIENTO

Previo a COVID-19
se pronosticaba que los **daños por ciberdelitos** a nivel mundial costarían hasta

$ 6 BILLONES ANUALES PARA 2021

Durante la pandemia la cantidad de delitos digitales creció por lo menos un 70%

Tormenta perfecta de oportunidades

A medida que las personas de todo el mundo enfrentan temores y preocupaciones sobre la pandemia de COVID-19, los **delincuentes también están tomando nota**. Y desafortunadamente, están usando esto como una oportunidad.

Muchas de estas estafas intentan hacerse pasar por **organizaciones legítimas** ofreciendo actualizaciones **informativas falsas** e incluso promesas de **acceso a vacunas**.

Contexto mundial

Marzo tuvo un promedio diario de

600

campañas de phishing

América Latina y el caribe

3

Millones

Intentos de ataques solamente de virus / malware en los primeros **3 meses del año**

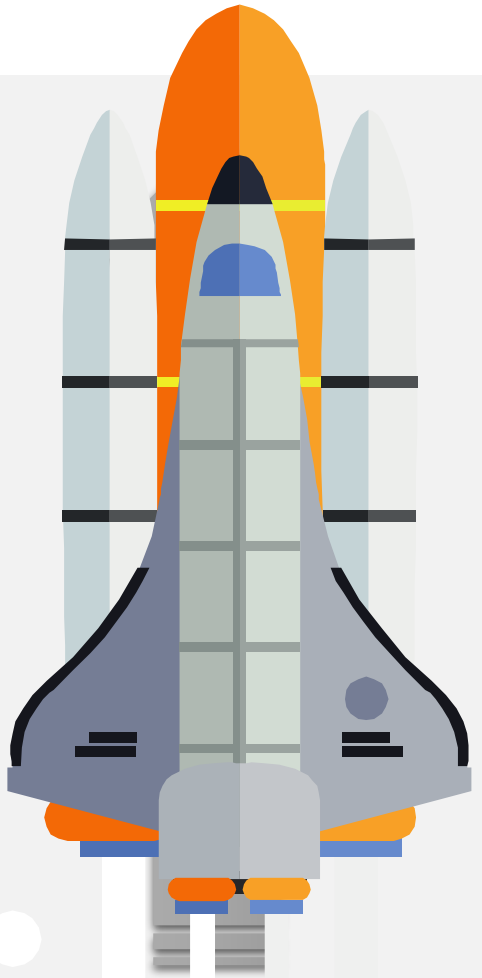
América Latina y el caribe

Durante el primer trimestre de 2020 se identificó un aumento en los virus en comparación con los mismos meses en 2019.

17% Enero

52% Febrero

131% Marzo



Argentina

Sufrió más de **187 millones** de intentos de ciberataques en el primer trimestre del año

Targets y Riesgo en la Pandemia

1. Los **niños asistiendo a la escuela on-line** pasan mucho más tiempo conectados y pueden encontrarse en mayor riesgo.
2. El **teletrabajo** es una puerta nueva, que expone a millones de empresas y personas al riesgo de cibercrimen.
3. Las **compras on-line** de todo tipo crecieron significativamente.
4. El **Fraude bancario/homebanking** y con tarjeta de crédito se multiplica.

TUS DATOS

Uno de los principales instrumentos utilizados para la comisión de delitos económicos, reputación, extorsivos, contra las personas e instituciones y de espionaje comercial y gubernamental

Targets y Riesgo en la Pandemia

Vectores de ataque

- Phishing
- Malware
- Apropiación de identidad
- Ingeniería social
- Data breach - fuga de datos
- Ciberinteligencia

Estafas en cuarentena

- Credenciales bancarias
- Anses - Bono 10.000 $
- Sextortion
- Bonificacion Netflix o servicio de streaming
- Ofrecimiento de trabajo remoto
- Venta fraudulenta en sitios de e-commerce

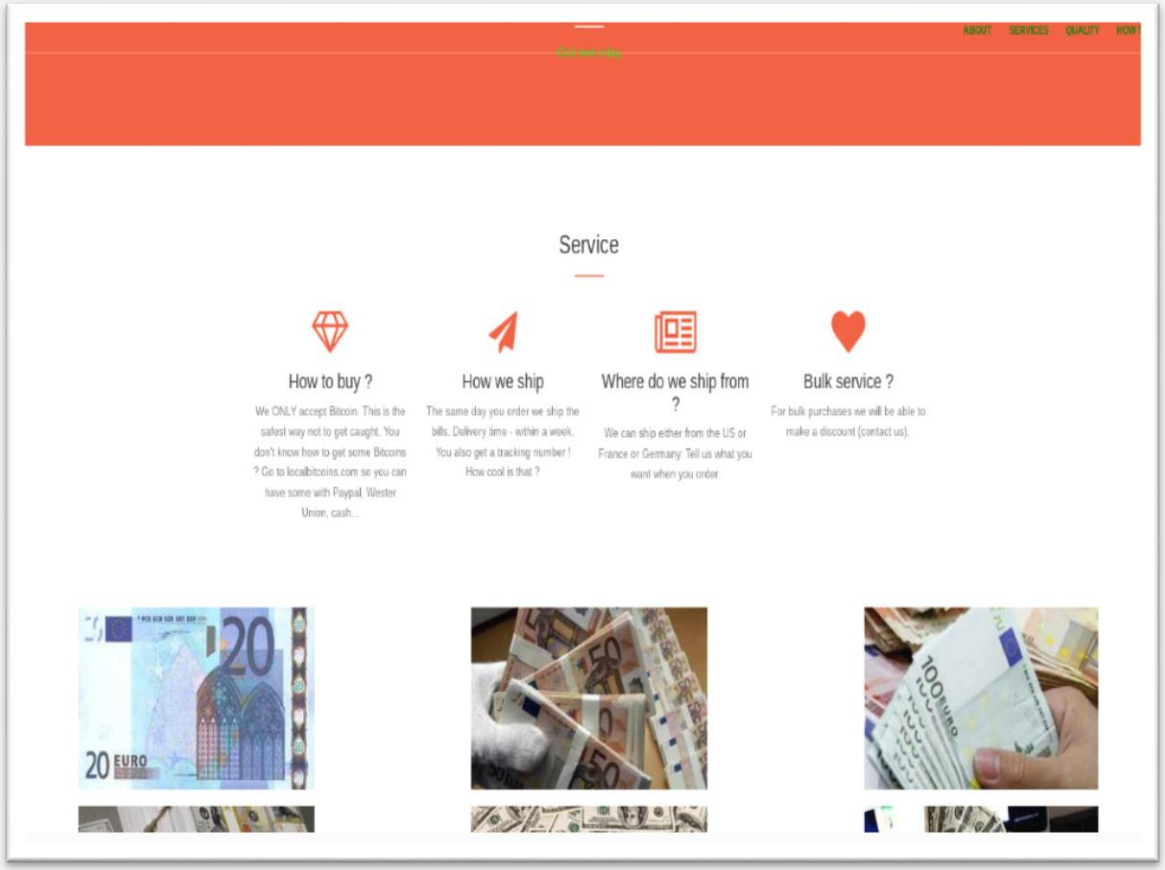
Deep & Dark Web

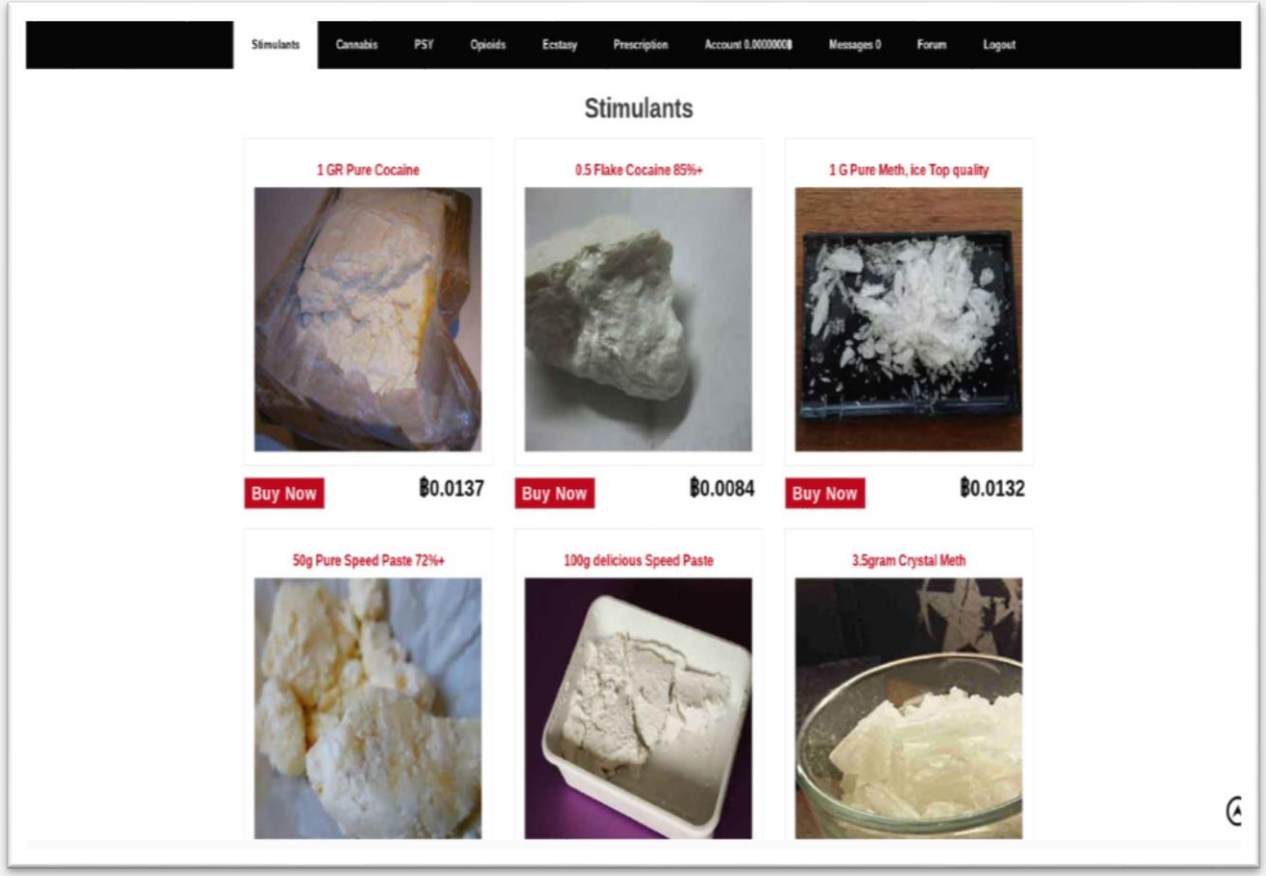
VENDEN VACUNAS PARA COVID-19 E HIDROXICLOROQUINA

Analizamos + de **400 productos** en 15 mercados/sites en la DarkWeb, encontramos productos de protección personal que se promocionan como posibles curas para el virus.

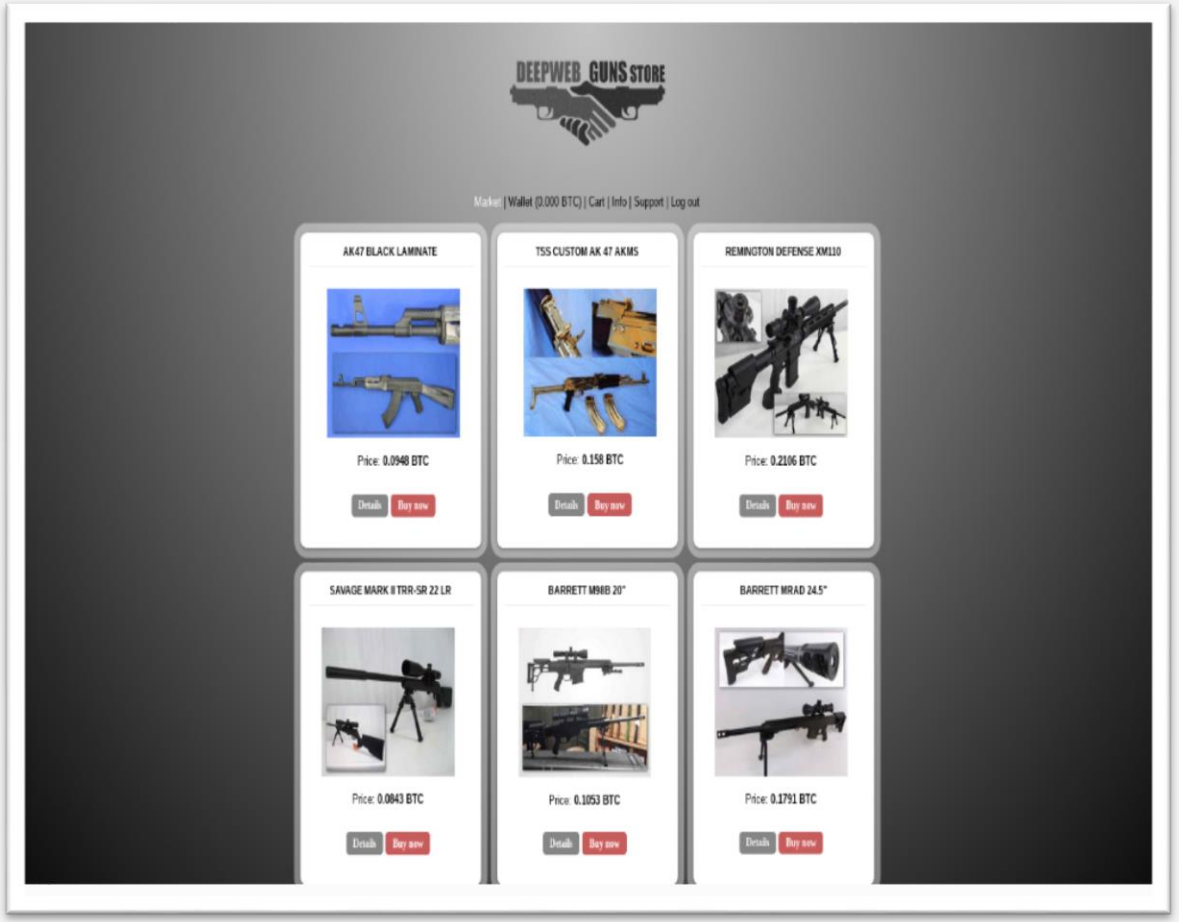
Muchos de los listados ofrecían vacunas falsas con un precio promedio de unos **u$s 750**, la cloroquina por 100 píldoras a **u$s 90**, todo pagadero con criptomonedas.

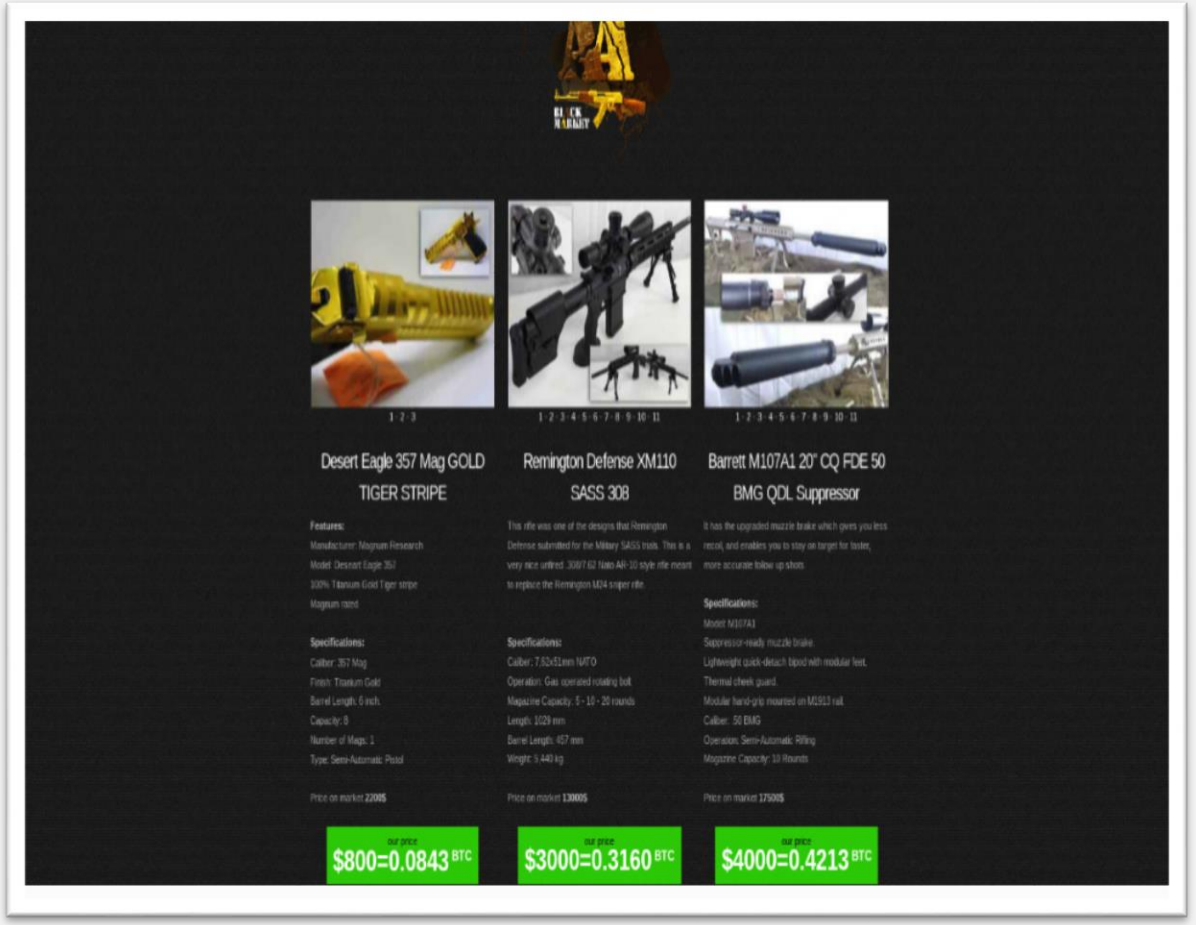
Deep & Dark Web





Deep & Dark Web

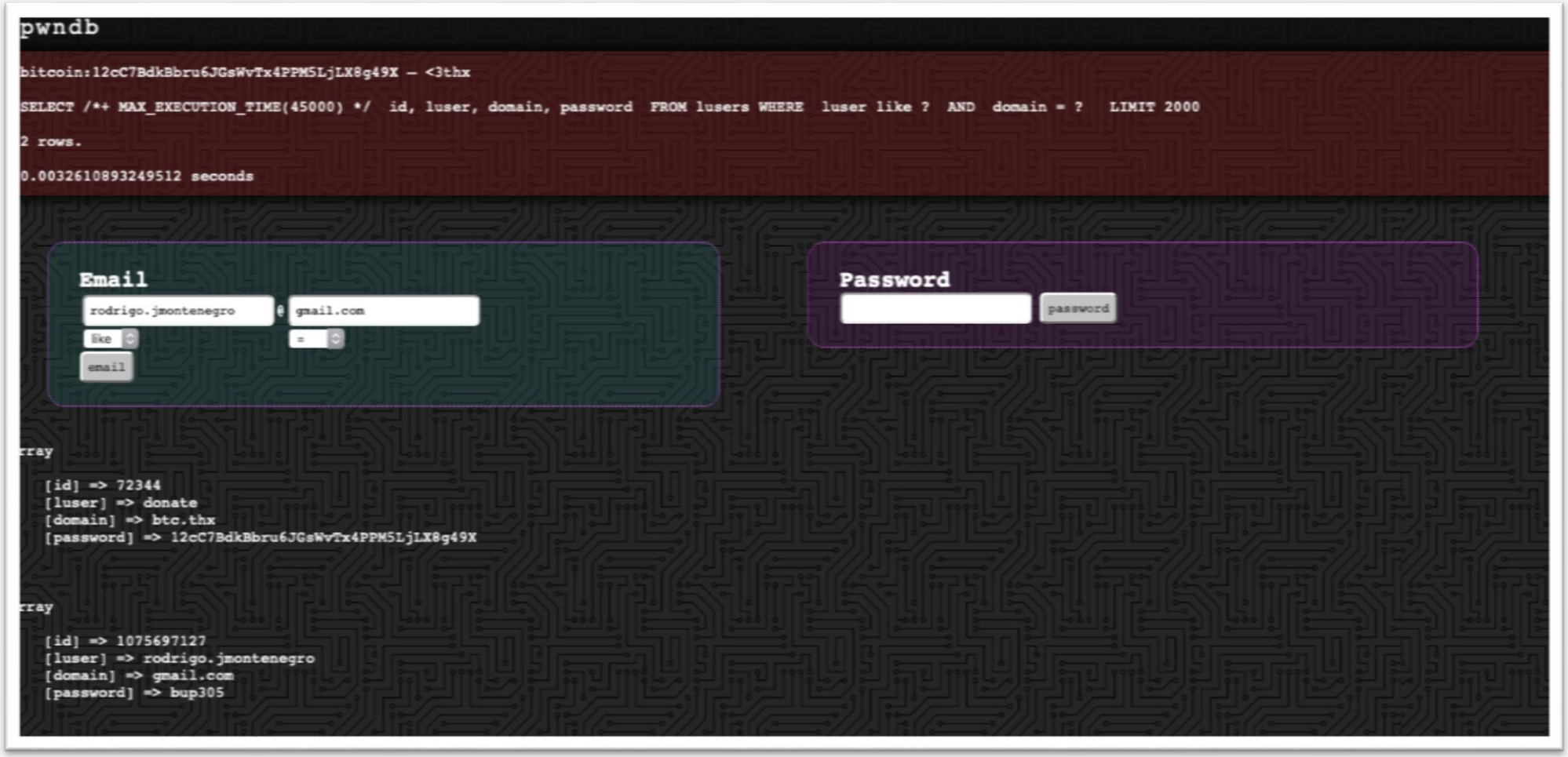




No es necesario hackear!

PWNDB

Base de datos con más de 10.000 millones de usuarios y sus passwords



https://pwndb2am4tzkvold.onion.ws

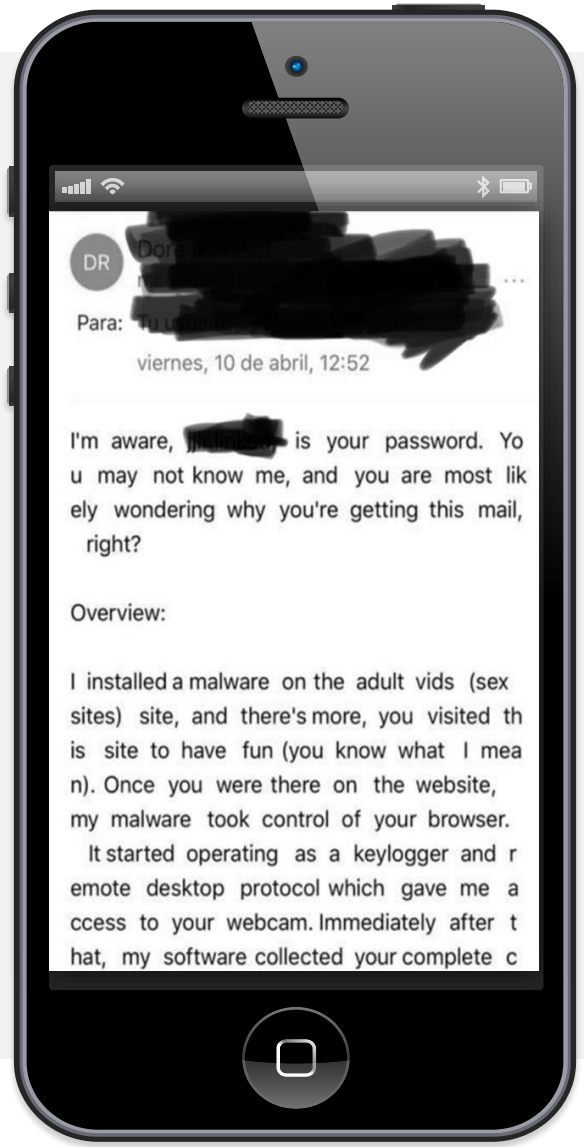
Corona-Virus-Map.com

Un sitio web malintencionado que infecta a los usuarios con el troyano **AZORult**, un programa de robo de información que puede filtrar una variedad de datos confidenciales.

Sitio web malicioso "Corona-Virus-Map.com" que pretende ser un rastreador legítimo de COVID-19.

Sextortion

Correos electrónicos **solicitando un pago / rescate** para recuperar fotos y videos propias con alto **contenido sexual**

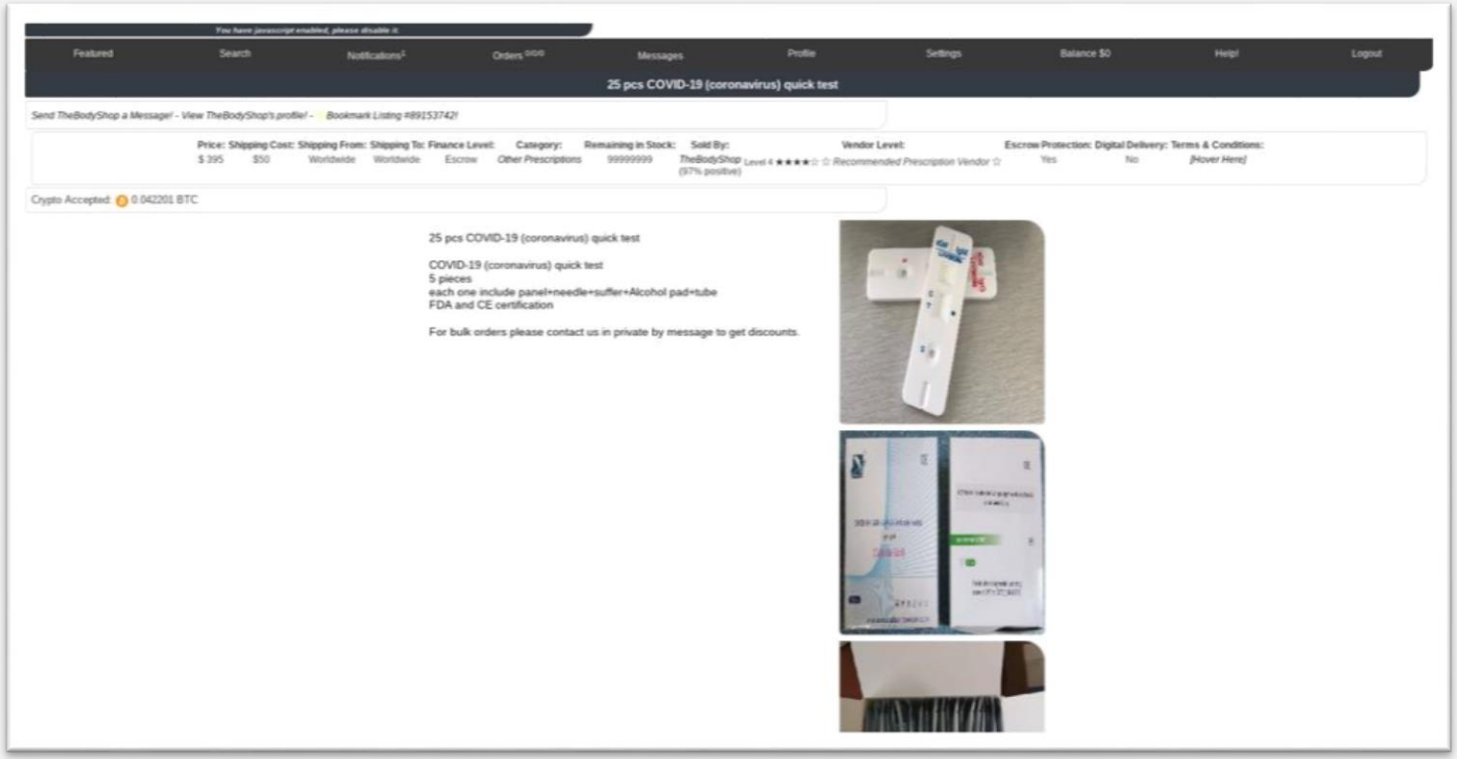


Phishing

Correos electrónicos de phishing relacionados con el coronavirus que incluyen **malware** camuflado en archivos adjuntos.

E-Comerce

Falsas tiendas y servicios online de **venta de productos** “**esenciales**” contra el coronavirus.



Casos testigo

"No huelo nada, tengo fiebre" Google sabe tanto de nosotros que hasta predice contagios de Covid-19

Google conoce las búsquedas que has hecho desde cualquier dispositivo conectado (celular, PC, tablet...) a tu historial de navegación, lo que influye en el perfil que la compañía tiene de vos para mostrarte los anuncios que ves cuando utilizas sus servicios. Ubicación, género, edad, hobbies, intereses profesionales... todo está incluido, además de cómo, cuándo y dónde has usado cada una de las aplicaciones que tienes instaladas, desde WhatsApp a la linterna. Por supuesto, tambíen los vídeos de YouTube.

COVID-19 / HEMOS IDENTIFICADO MÁS DE 130 ATAQUES E INTENTOS DE ESTAFAS EN LOS ÚLTIMOS MESES QUE IMPLICAN LA POSIBILIDAD DE ROBO DE TUS CREDENCIALES Y TARJETAS DE CREDITO Y DEBITO

Los delitos y estafas on-line han aumentado al menos en un 70%, durante el confinamiento, la gente está más conectada y más sensible que nunca. Durante la cuarentena el "phishing" es el tipo de Cyberattack más frecuente, representa el 45% de los ataques de seguridad ocurridos.

En que consiste el 'carding' o fraude de tarjetas de crédito

Hasta los cibercriminales más novatos pueden robar dinero de las tarjetas; este tipo de robos es cada vez más común, ocurre todos los días y supone pérdidas financieras significativas.

La huella (o "footprint") es una de las técnicas que instrumentan las entidades financieras para evitar el 'carding'. Esta huella representa el comportamiento online del usuario basado en diferentes parámetros, como su historial web, el sistema operativo y la información del navegador, como los complementos instalados y demás.

MANDRAKE EXISTE, HACE 4 AÑOS QUE VIVE EN GOOGLE PLAY STORE Y ESPÍA TU TELÉFONO

Una variante de spyware para Android estuvo encubierta en Google Play Store durante cuatro años, oculto en aplicaciones asociadas a Coinbase, funcionando como supuesta billetera de criptomonedas y en otros casos como apps vinculadas a Amazon, Gmail, Google Chrome, y aplicaciones de varios bancos australianos y alemanes, el servicio de conversión de moneda XE y PayPal.

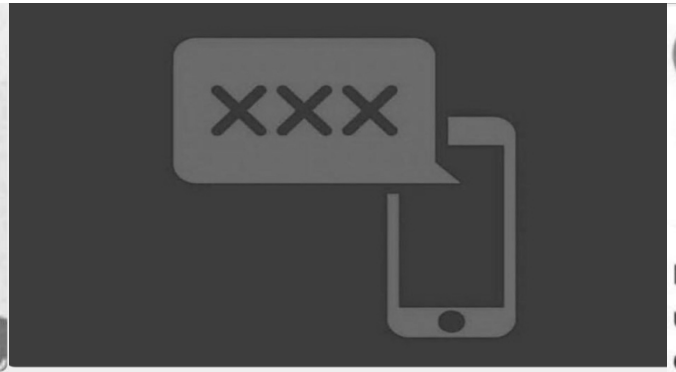
Casos testigo

TE HACKEARON?? DONDE VA A PARAR TU CUENTA DE USUARIO Y TU PASSWORD ??
ENTERATE

Cuando sufrís un hackeo u ocurre una brecha de seguridad en algún sitio web o portal transaccional, la mayoría de las veces los datos se ven expuestos, generalmente de forma inadvertida por sus propietarios. ¿Qué significa?: Que nuestros datos son a diario robados por ciberdelincuentes y no nos damos cuenta ó los portales y apps que son víctimas de estas fugas no lo informan.

SECUESTRAN CUENTAS DE WHATSAPP DURANTE LA CUARENTENA

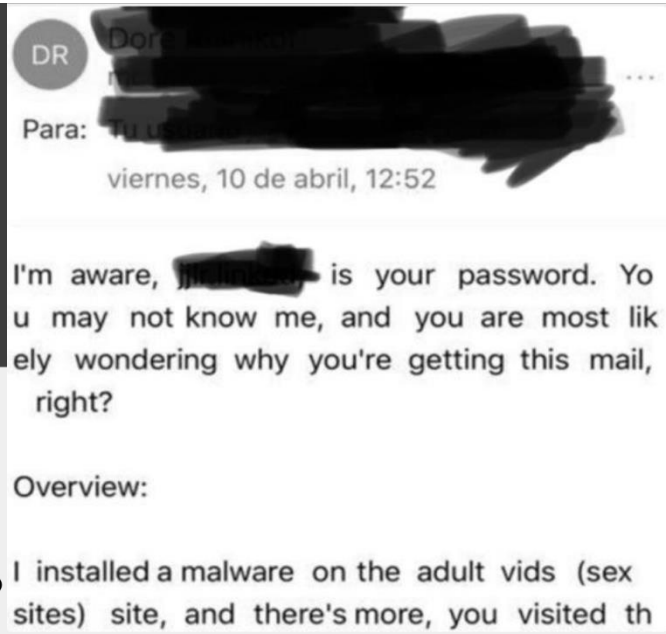
El engaño consiste en el muy utilizado modo delictivo de "Suplantación de Identidad" combinado con "Ingeniería Social" que llega a través de WhatsApp y que busca el secuestro de cuentas, te contactan con un mensaje a través de algún servicio de mensajería o de un SMS con distintos argumentos de ingeniería social, invitación a conectarte a zoom y su clave de acceso, por error, etc. Recibís un código de verificación de seis dígitos que se envió a su teléfono y te solicitan que reenvíes el mensaje con el código.



*SEXTING,PORNOVENGANZA Y SEXTORTION
TRES FENÓMENOS QUE CRECEN*

Diariamente se envían 65.000 millones de mensajes de whatsapp, su contenido es encriptado y es el vehículo ideal para la práctica de sexting, pornovenganza y sextortion.

El sexting es un fenómeno que crece rápidamente entre jovenes 12 y 20 años de edad, quienes utilizan whatsapp intensamente. Igualmente la pornovenganza que es la publicación de videos, imágenes y grabaciones de tipo sexual sin el consentimiento de la persona que protagoniza el contenido, finalmente, Sextortion, chantaje que solicita dinero, bitcoins, etc.



CYBEREXTORTION, SCAM, ENGAÑO: Los ciberdelincuentes no descansan durante la Pandemia de COVID19

¿Qué harías si durante la cuarentena, recibieras un correo electrónico de alguien que dice tener tu contraseña, y que a partir de ello ha violado tu intimidad y te ha grabado a través de tu cámara web mientras estás viendo pornografía?.

Los chicos en cuarentena

Los distribuidores de imágenes de abuso sexual infantil intercambian enlaces en YouTube, Facebook, Twitter e Instagram utilizando un lenguaje "**codificado**" para evadir las herramientas de detección.

USAN CODIGOS SECRETOS PARA NO SER DETECTADOS

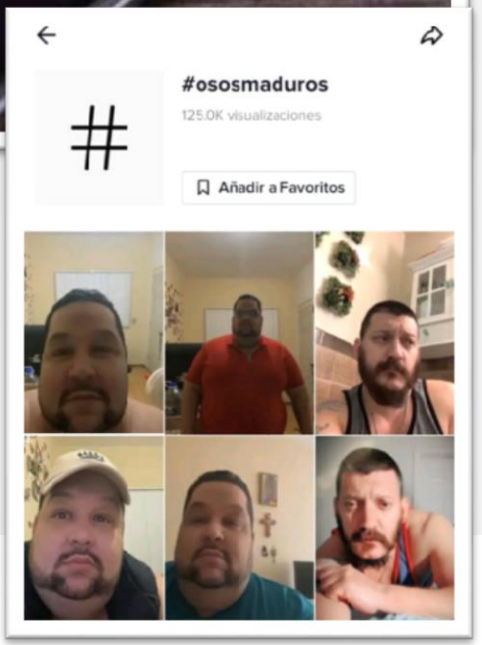
Los chicos en cuarentena

Las víctimas no están en la escuela, permanecen hiperconectadas, **los agresores** esconden fácilmente su verdadera identidad y se cuentan por millones, las plataformas **relajaron los controles** y además en muchos casos el abusador es un miembro de la familia.

Internet conecta a tus hijos con el mundo, sabes quien está en el mundo conectándose con ellos ?

TIKTOK #OSOSMADUROS, #OSOS, etc.

El papá de un **nene** de **10 años** muy preocupado y alarmado nos consultó ya que su hijo recibió "sobre impreso" en varios videos de **TikTok** un link en donde se exponían imágenes de desnudez de personas mayores y/o adultos manteniendo relaciones sexuales. Seguidamente nos preguntaron sobre etiquetas y recomendaciones, siempre dentro de **TikTok**, que indicaban a menores efectuar búsquedas de imágenes en **Google**, escribiendo: "**OSOSMADUROS**".



OMEGLE #CHAT CON DESCONOCIDOS

Es posible hablar con desconocidos de forma instantánea, selecciona países específicos, conexión rápida de webcam
a webcam, sin necesidad de registrarse
o darse de alta para conversar online
con chicas y chicos online.
Omegle es una de las plataformas más notorias en la categoría de aplicaciones
de amistad online, convirtiéndose en un caldo de cultivo para agresiones
y ciberdelitos.

La mayor virtud de OMEGLE radica en la libertad absoluta para mantener el anonimato, construir identidad o suplantarla.

Redes Sociales – Child Abuse

La escala completa de la explotación sexual infantil on-line es difícil de conocer.

Observamos que diferentes sitios se disfrazan para parecer legítimos, o se ocultan en la Deep y Dark Web, lo que permite a las personas actuar de forma anónima.

- **1 de cada 3** usuarios de internet son niños.
- **1 de cada 5** chicos **entre 8 y 11 años** tiene un perfil en las redes sociales.
- **7 de cada 10** chicos **entre 12 y 15 años** tiene un perfil en las redes sociales.
- **1 de cada 4** chicos ha experimentado una situación molesta en alguna red social.
- **1 de cada 5** chicos será contactado con fines sexuales.

Ciberdelito / Child Abuse

La escala completa de la explotación comercial de contenidos e imágenes domésticas inapropiadas con participación de menores es difícil de conocer.
Los sitios a menudo se disfrazan para que parezcan legales, o se ocultan en la deep y dark web, lo que permite a las personas actuar de forma anónima.

Los delincuentes pueden estar viendo material en el Reino Unido, alojado en un servidor en Holanda, mostrando imágenes del sudeste asiático, producido en Latinoamérica.

Ciberbullying

Una de las prácticas que existe en los espacios digitales es lo que se conoce como ciberbullying, es decir, el hostigamiento online. Una práctica que no es propia o generada por lo digital, pero que encuentra en estos ámbitos un lugar de reproducción.

La discriminación existe tanto en los espacios online como en los offline. Las tecnologías ofrecen una amplia variedad de canales para realizar el acoso, como pueden ser mensajes personales, grupos en redes sociales, memes (fotos con texto incitando a la burla), imágenes o videos difamatorios. Esto reproduce el daño ya que se combinan los dispositivos y se multiplican los canales de difusión y recepción.

Entonces, el **anonimato**, **la no percepción o registro del daño causado a otro**, y la posibilidad de **viralización** hacen que el ciberbullying sea un tema a tratar tanto en el ámbito familiar como en las escuelas e instituciones.

Sexting

Una de las prácticas entre los jóvenes con el uso de tecnología es la producción de contenidos de índole sexual, principalmente fotos y/o videos íntimos.

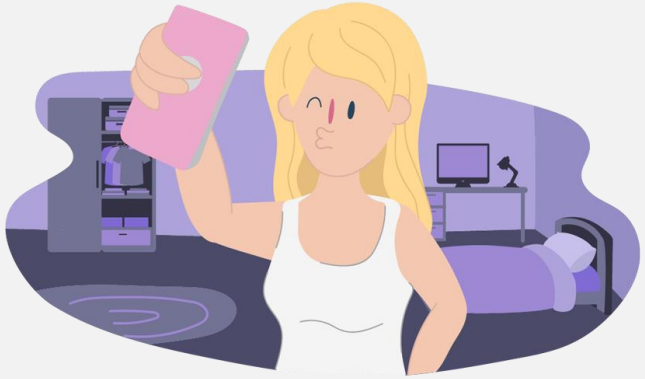
La palabra sexting viene de la combinación en inglés de las palabras sex (sexo) y texting (texteo, envío de mensajes de texto mediante teléfonos móviles). La práctica surge del uso de tecnologías digitales y consiste en la circulación de un contenido sexual a través de dispositivos móviles (celulares, tabletas) y que se da mediante diversas aplicaciones (Whatsapp, Facebook, Instagram, Twitter, Snapchat, etc.). Es decir, el envío de imágenes y vídeos sexuales no solo vía mensaje de texto sino, también, mediante mensajería instantánea, foros, posteos en redes sociales o por correo electrónico.

De este modo, **la imagen es enviada a uno o varios contactos que, a su vez, pueden reenviarla y comenzar la viralización.**

Sexting

Las imágenes que componen el fenómeno de sexting son obtenidas, en algunos casos, de manera voluntaria.

Es decir, el chico o la chica que aparece revelando su identidad es consciente de ello. O bien es el/la que se filma o fotografía, o bien da su consentimiento para que otro lo haga.



Esto no significa que exista un consentimiento para la divulgación de los contenidos.

Existe una diferencia entre el aceptar ser tomado por una cámara y el que estas imágenes sean publicadas en espacios públicos como internet o las redes sociales. Este es uno de los grandes conflictos que existen respecto de este tema, por lo que es necesaria la intervención del adulto para dialogar junto con los jóvenes sobre la problemática.

Grooming

Es la acción de un adulto de acosar a un menor mediante el uso de recursos digitales, comunicaciones electrónicas, redes sociales, whatsapp, etc.

Los perpetradores de este delito adoptan una identidad FALSA en una red social, sala de chat, etc., enmascarándose en un perfil similar al de un chico, intentan construir relación de amistad y confianza.

La tecnología brinda herramientas que plantean nuevos escenarios a problemáticas previamente existentes. Es decir, el abuso o acoso sexual a chicos y la pedofilia no surgen con **internet y las redes sociales**, lo que sucede es que se son capaces de **potenciar los distintos tipos de abuso**.

En Argentina, el grooming es un delito incluido en el Código Penal.

Fases del Grooming

Contacto para conocer gustos, costumbres y rutinas de los chicos. El acosador suele mentir sobre su edad al entrar en contacto. El objetivo es mostrarse como un par.

AMISTAD, CONTACTO Y ACERCAMIENTO

Se busca ganar confianza, por medio de extensas y Continuas conversaciones. De esta manera el acosador consigue el envío del material Con componentes sexuales o eróticos.

RELACIÓN, GENERACIÓN DE CONFIANZA Y OBTENCIÓN DEL MATERIAL

El material entregado por el chico o chica se vuelve luego objeto de chantaje, ya sea para la gestación de mayor cantidad de material o bien para lograr un encuentro presencial.

COMPONENTE SEXUAL. CHANTAJE Y ACOSO

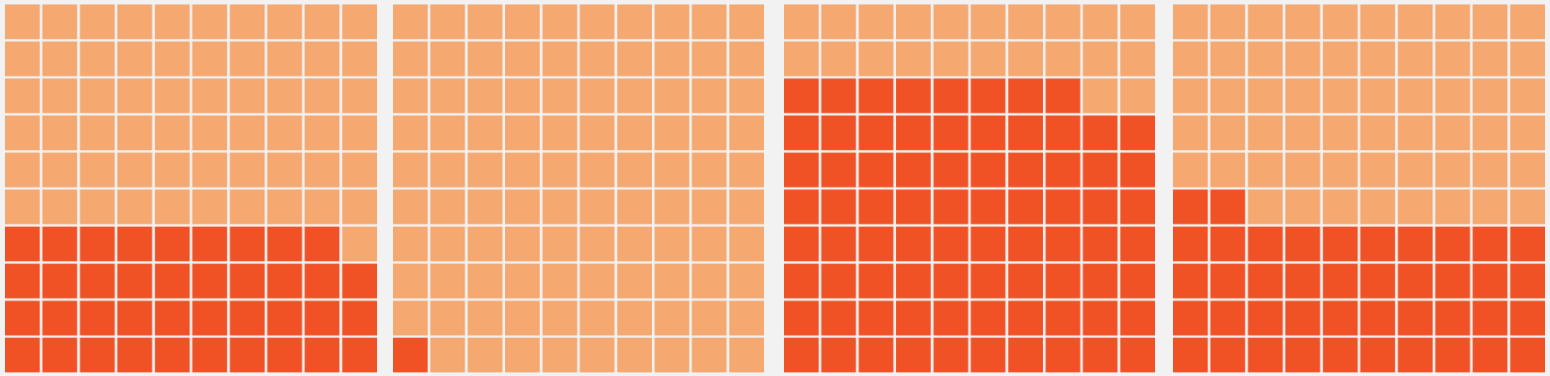
Una nueva tendencia preocupante en el abuso de los niños son las capturas de transmisiones en vivo que muestran a los niños siendo preparados o alentados a realizar actos privados, el llamado contenido de 'autoproducción' representa más de uno de cada tres denuncias.

Transmisión en VIVO

Los niños son acosados, coaccionados y chantajeados para que transmitan en vivo imágenes privadas a través de cámaras web, tablets y teléfonos móviles.

Una muestra de la IWF identificó 2.082 en 3 meses imágenes y videos de abuso infantil transmitido en vivo. Reveló que el 98% de las imágenes encontradas eran de niños menores de 13 años, el 28% tenían 10 años o menos, mientras que la víctima más joven tenía solo tres años.

- El 96% de las víctimas eran niñas.
- El 96% mostró un niño en un ambiente hogareño.
- El 18% del abuso fue categorizado como Categoría A, que incluye violencia física.
- El 40% del abuso fue categorizado como Categoría A o B, lo que indica abuso grave.



39%
de las víctimas tienen 10 años o menos.

1%
de las víctimas tienen 2 años o menos.

78%
de imágenes donde las víctimas eran niñas.

43%
de imágenes evaluadas como categoría A o B.

La "moda" de selfies inapropiadas. **ALERTA PADRES** menores cuelgan selfies y videos íntimos a cambio de "likes". Las publicaciones corresponden a menores de entre 2 y 13 años de edad y los motivos de esta preocupante práctica, entre los más mayores, eran la búsqueda de seguidores para sus canales de Youtube, Instagram, etc y más likes en sus publicaciones.

Los menores aprovechaban los momentos de intimidad en sus domicilios para grabar las imágenes con un alto contenido de intimidad, donde aparecían en muchos casos junto a amigos o familiares de su misma edad.

VISIÓN 2020

BTR Consulting
BUSINESS DIGITAL SOLUTIONS

RSM

PREVENCION PARA LAS ORGANIZACIONES

- La nueva normalidad, la hiperconectividad y la dependencia de la TI indican que habrá 5 **millones de empleos de Cybersecurity** sin cubrir para 2021. 5G y Starlink agravarán el diagnóstico hacia 2025.
- Para 2020, **el 25% de los Cyberattacks** contra empresas **involucrarán dispositivos IoT**.
- El **ransomware dominará el Cybercrime** y los ataques dirigidos seguirán afectando a las organizacions.
- El creciente impacto de **AI (Inteligencia Artificial) y ML (Machine Learning) están reinventando las necesidades** de las organizaciones en su conjunto y son áreas que definitivamente deberán abordarse en 2020.
- Los **Cyberattacks a los servicios públicos y la infraestructura pública continuarán aumentando**.

> “El **90% de las organizaciones** afirma tener una estrategia de Cybersecurity, pero solo el **49% ha implementado** esta estrategia completamente”

PREVENCION PARA FAMILIAS

- Explicarles que **NO todo lo que ocurre** y se expone en el entorno **digital es REAL**. No aceptar en redes sociales a personas desconocidas.
- Hacer uso de la opción **perfil privado en redes sociales.**
- Rechazar los mensajes de **tipo sexual o pornográfico**.
- Si se ha producido una situación de acoso, **guardar pruebas: conversaciones, mensajes, capturas de pantalla, entre otras**.

> “El **‘Grooming’** sigue creciendo: **adultos adoptan identidad FALSA,** intentan construir una **relación de amistad y confianza.**”

Recomendaciones

Es importante entender que **el mundo digital atraviesa la vida de los niños y jóvenes** y que a pesar que existen riesgos devenidos de su uso, **ser consientes de esto es lo más importante.** Por eso para comenzar a hablar de prevención, siempre lo primordial es la construcción del diálogo respecto a estos temas.

Debemos incorporar cuestiones de la cultura digital para poder acompañar el riesgo al que nos enfrentamos.

En internet y las redes sociales suceden eventos fundamentales en la vida social de los más jóvenes y es importante que las familias, adultos y niños tengan herramientas para poder intervenir.

Consejos básicos

- **NO** todo lo que ocurre en el entorno digital es **REAL.**
- **No aceptar** en redes sociales a **personas desconocidas.**
- Hacer uso de la opción **perfil privado** en redes sociales.
- Antes de subir una foto en redes sociales. Pensar, esa imagen pueda verla **cualquier persona y para siempre.**
- Utilizar programas para **protegerse** contra software malintencionado.

Consejos básicos

- Verificar URLs y HTTPS
- Utilizar **contraseñas** complejas y renovarlas periódicamente.
- **Rechazar** los mensajes de tipo **sexual o pornográfico.**
- Si se ha producido una situación sospechosa **guardar pruebas:** conversaciones, mensajes, capturas de pantalla, entre otras.
- Si se ha producido una situación no deseada, **NO ceder** ante pedidos **y hacer la denuncia.**

¡Gracias !

+54 11 4343 1218

info@btrconsulting.com

www.btrconsulting.com

/btr-consulting

BTR Consulting

BUSINESS DIGITAL SOLUTIONS

RSM