HACKEADOS

Delitos en el mundo 2.0 y medidas para protegernos.

JORGE LUIS **LITVIN**

“No se permite la reproducción parcial o total, el almacenamiento, la venta o alquiler, la transmisión o la transformación de este libro, en cualquier forma o por cualquier medio, sea electrónico o mecánico, mediante fotocopias, digitalización u otros métodos, sin el permiso previo y escrito del autor. Su infracción está penada por las leyes 11.723 y 25.446 de la República Argentina. Depósito previsto en Ley 11.723 en trámite”

Primera edición.
Fecha de publicación digital 13 de abril de 2020.
Diseño por Andrés Mariuzzo.

Existen dos tipos de individuos:
Los que fueron hackeados.
Los que aún no se enteraron.

Estimado lector, póngase cómodo y sea usted bienvenido. Pensé y escribí este libro de forma tal que pueda leerse de corrido (vaaamos, es cortito). De todos modos, para el caso de que - una vez finalizado - quiera acceder rápidamente a uno de los temas desarrollados, queda a su disposición el índice de contenidos.

Índice

Agradecimientos

Desde que era estudiante de primer año de la carrera de Derecho que sueño con esto.

Imaginé mi primer libro como los del resto: de cientos de páginas, lenguaje complicado, citas dogmáticas y olor a cuero.

Lo que hoy presento es muy distinto a eso, no lo siento mejor ni peor, lo siento exactamente lo que quiero.

Este pequeño trabajo es una suma de grandes esfuerzos prolongados en el tiempo, algunos míos y muchos otros ajenos. Amigos, profesores, familiares, y colaboradores incondicionales me dieron las herramientas para poder poner en palabras algunos pensamientos.

Gracias a todos los que colaboraron con hacer realidad lo que alguna vez fue sólo un sueño, y gracias a vos (si, a vos) que me estás leyendo.

1 Presentación del trabajo y del autor.

Ya van varios años desde que vivimos en una doble realidad, en donde una es la virtual. La ciencia y la tecnología, con su avance hicieron maravillas, la "internet" es su hija prodigia.

¿Qué es internet? Una red que permite tejer infinitas redes. Piénsela como un universo: con galaxias, sistemas solares y planetas y lo minúsculos que somos cada uno de nosotros habitando en ella.

Los más jóvenes lectores nacieron con los beneficios de este mundo paralelo, ni se imaginan cómo sería vivir sin ellos. A los que tenemos un poco más de kilometraje nos colmó de facilidades que en alguna época estaban fueran de nuestro alcance.

Hacer una lista completa de los "updates" que la red hizo a nuestra vida cotidiana haría este texto eterno, pero recordemos al menos algunos de ellos: La red nos acerca a personas que tenemos lejos e inclusive nos permite hacer contactos nuevos. Ya no hace falta escribir cartas ni usar un telégrafo, podemos "tipear" un mensaje, hablar y escuchar nuestras voces y hasta vernos en video, de inmediato y en cualquier momento.

Vivimos en una especie de "all inclusive" de la información, no podemos decir que no tenemos herramientas para enterarnos y aprender lo que sea al día de hoy. Portales de noticias, escuelas de idiomas, redes sociales y hasta universidades que dictan carreras de grado y posgrado completamente virtuales.

Se abrieron las puertas del home office y cientos de nuevas oportunidades de trabajo. La inteligencia artificial avanza a pasos agigantados, automatiza y simplifica procesos que antes demandaban mucho tiempo y esfuerzo humano, disminuyendo considerablemente los gastos.

Para comprar ya no necesitamos transportarnos hasta ningún local o mercado, hoy casi todas las operaciones se hacen desde aplicaciones al alcance de nuestra mano y lo que adquirimos nos llega a nuestro hogar cuando lo deseamos.

Pero no todo es arcoíris en este mundo nuevo, hay un lado B oscuro y tétrico, al que en las siguientes páginas me estaré refiriendo, y es que **el crimen también encontró su lugar en el universo 2.0.**

Le doy la bienvenida estimado lector al emocionante mundo de los hackers. No de todos ellos, por el momento, sólo de aquellos que utilizan sus conocimientos informáticos para hacer de su hobby o profesión "delincuentes virtuales"-, de los virus y los códigos extraños que se despliegan a gran velocidad en su pantalla como Hollywood y Netflix supieron mostrarle. Todas las imágenes y escenas que se le vinieron a la mente en este instante no son de ficción ni algo que para un futuro lejano es esperable, sucede en este mismo instante.

Es más, me arriesgaría a apostar que usted ya fue víctima de alguna de las conductas que se describirán sin que se entere o imaginara que detrás de ese suceso había un criminal.

Antes de asustarlo, que no es el objeto de este trabajo, si no me presentara sería muy maleducado. Mi nombre es Jorge Litvin, el derecho penal es mi área de trabajo y en cibercrimen estoy especializado. Pero que no cunda el pánico, no voy a escribir en "código abogado". Nada de ZzZzZz, ¿está claro?.

Esto está sucediendo, está chequeado, no va a leer el típico artículo escrito por un letrado. Intentaré no usar términos técnicos ni complicados, tampoco lenguaje rebuscado, a esta altura ya se habrá percatado de que puede leerme rimando (algún verso lo invito a rapearlo). No es azaroso, es para mantenerlo enganchado. Si en algún momento de estas páginas pierdo su atención esto lo consideraré un fracaso, así que pongámosle entusiasmo.

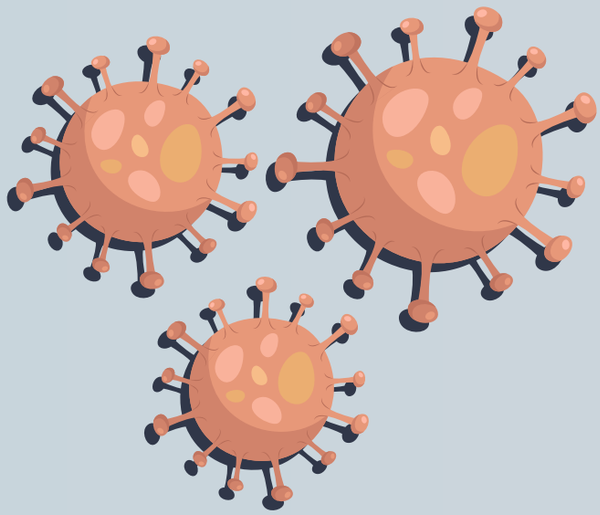
¿Qué pretendo? Que comprendamos que internet no es un electrodoméstico que enchufamos y encendemos, es un mundo paralelo, y aunque ya tiene sus años renueva constantemente sus rincones, peligros y misterios. Tiene sus propias leyes y códigos de conducta internos, y creo que todos los que habitamos en este territorio virtual en paralelo merecemos poder entenderlo, sin necesidad de haber estudiado una carrera de informática y/o derecho.

Eso es lo que aquí intento, mostrar el lado oscuro de la red, y no para llenarlos de miedos, sino para que estén atentos.

Con su permiso –y sin él también sigo- voy a valerme del actual contexto médico-global que estamos viviendo, facilitará explicar la importancia de ser cuidadosos e ilustrar los casos con lo más actuales ejemplos.

2 El aislamiento como escenario ideal para el crimen digital.

"Virus": concepto biológico que hace referencia a un agente infeccioso. Son imperceptibles al ojo humano, no podemos ver a estas estructuras orgánicas, pero están dispersas por todos lados. Se trasladan a gran velocidad y con insólita facilidad, se adhieren, penetran y se replican en los organismos que tienen por víctimas, es difícil detectar que los portamos hasta que ya está producido el daño. La conceptualización es idéntica cuando se trata de un "virus informático".



Transitamos los primeros meses del 2020 y al momento en que redacto estas líneas el COVID-19 (conocido como Coronavirus), ya fue reconocido como pandemia por la Organización Mundial de la Salud. Originado en China, viajó y se esparció por todo el globo hasta llegar a la Argentina, donde hasta le hicimos memes dándole la bienvenida. Su arribo nos obligó a cambiar por tiempo indefinido nuestro estilo de vida.

Se implementaron restricciones y prohibiciones de movilidad que nos conminan a resguardarnos en nuestro hogar. Si ya era poco el tiempo que pasábamos en lo que llamo "mundo real", ahora la gran mayoría de nosotros está viviendo en una verdadera "realidad virtual". Trabajamos remotamente desde el hogar, las pocas operaciones de compra y contacto que todavía hacíamos de forma presencial ahora las hacemos a través de alguna plataforma digital, el nuevo "tiempo extra" también invita a navegar mucho más, en la web y en toda red social.

Podríamos decir que físicamente estamos en nuestras casas, pero en el aislamiento que impone el contexto gran parte de lo que decimos y hacemos ahora es en el mundo 2.0. Las calles están cada vez más vacías y el ciberespacio se convierte en la zona más concurrida. **¿Sabe estimado lector cuáles son las "zonas calientes" en actividad delictiva? Adivinó: donde están las víctimas.**

El virus del que nos protegemos nos pone a la merced de los oportunistas delincuentes 2.0, que siempre son los primeros en intentar sembrar pánico, desinformar y obtener algún beneficio –generalmente- financiero. Pasa todo el tiempo, pero toma aún más relevancia en este contexto. Vamos con algunos ejemplos:

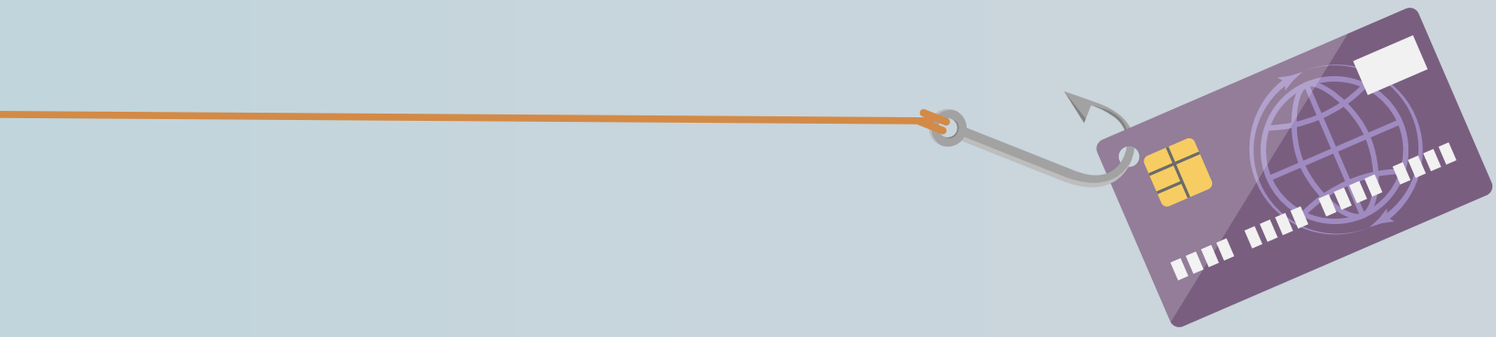
3 El “phishing” y la distribución de software malicioso.

Para definir al “phishing” juguemos a hacer un paralelismo con “fishing”, que en inglés significa “pescar”. El pescador es el cibercriminal, su línea un correo electrónico o un mensaje de texto, su anzuelo son hipervínculos o archivos adjuntos que vienen incluidos en ellos y algo que llame la atención a su presa su señuelo. Usted es la presa mi estimado lector 2.0.

Para que se comprenda esta expedición de pesca en el actual contexto. **Ya circula un sinnúmero de mails y mensajes que utilizan COVID-19 como carnada para ocultar el virus verdadero.**

El contenido de los milagrosos correos nos llega como caído del cielo, “la cura”, “la información para no contraerlo”, “mapas de contagio” y hasta la “receta para una vacuna”. Por un momento nos lamentamos no tener el contacto de los científicos israelíes que están desarrollando un remedio para reenviárselo, y a continuación nos disponemos a iluminarnos.

El texto del mensaje puede lucir procedente de un organismo oficial (como la OMS o un Ministerio de Salud Estatal) o de un laboratorio espectacular, y nos invita a acceder a la información haciendo clic en un enlace que se nos copia o a un archivo adjunto descargar.



¡Que sencillo, que tremendo acto de generosidad, ojalá hubiera más gente así, que manda la cura de una pandemia a mi correo y yo no siquiera se los tuve que pasar! Ah no, pará... ese anzuelo mejor evitar.

Bienvenidos al concepto de "ingeniería social", que en pocas palabras consiste en utilizar técnicas de manipulación psicológica para obtener información o para que el sujeto pasivo (vos) actúe de una forma que le termina ocasionando un perjuicio. Puede pasar seguido, con tu esposa o tu marido, pero los delincuentes son más sutiles y sólo te hacen entrar a una página o descargar archivos.

Esto no es novedoso y no surgió a raíz del fenómeno del coronavirus. "Se ha detectado actividad sospechosa o intentos de inicio de sesión, confirme en el siguiente enlace su información"; "Su pago de Netflix no pudo ser procesado con éxito, complete el siguiente formulario para evitar la suspensión de la cuenta" (crisis, instantánea, vas por la 3 de 8 temporadas y tenes 9 series más guardadas!). "Le acompañamos la factura de su compra realizada en Apple", "Usted ha sido elegido para recibir un reembolso/subsidio por parte del Estado" (como se nota que no lo redactó un argentino).

La cantidad de ejemplos es infinita, pero la modalidad es siempre la misma: Una alerta preocupante o la promesa de un beneficio gigante, a un click de distancia en un archivo o un enlace.

¿Y qué pasa si descargo el archivo o sigo el hipervínculo? Bueno, los escenarios son bien distintos, en ninguno quisieras tomar protagonismo.

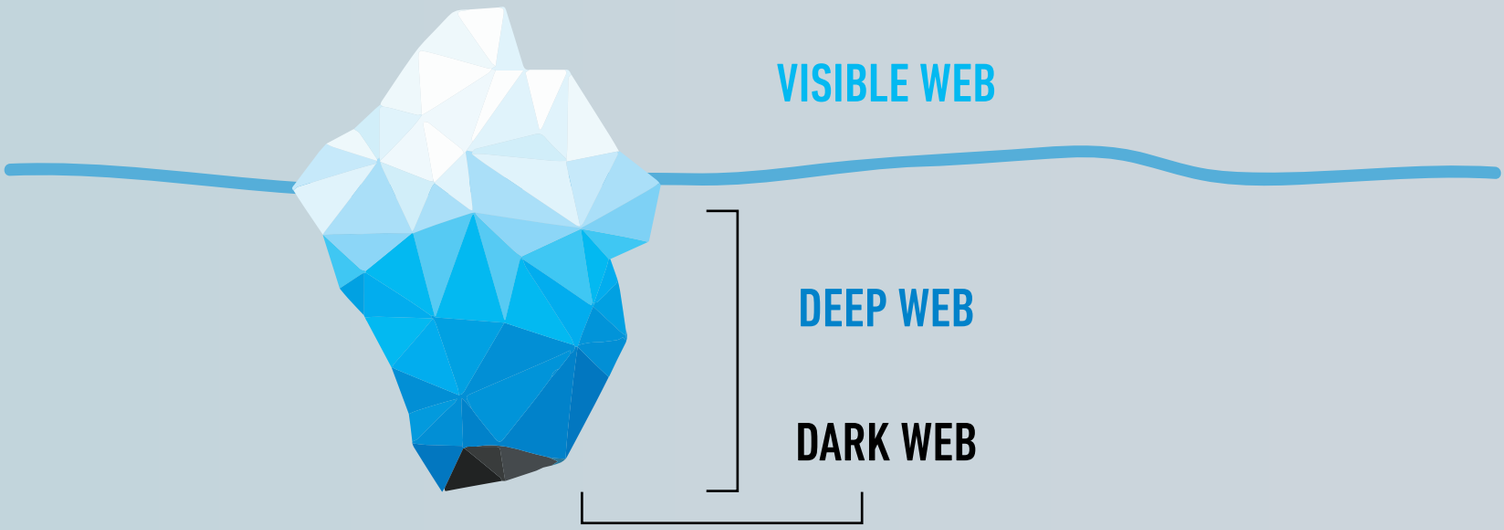
Un enlace (la dirección URL –el www..., ¿se entiende?–) puede llevarnos a una página en donde completamos un formulario en el que envolvemos nuestros datos para regalo, y no hablo de poner nuestro nombre y apellido, sino de que para recibir la vacuna milagrosa entregamos nuestro número de DNI y domicilio; o inclusive los datos de otras personas que viven o trabajan con nosotros y para quienes queremos hacer extensivo el "beneficio".

Es muy probable que alguna de estas páginas nos requiera los datos de nuestra tarjeta de crédito (quien quiera la cura, que ponga el dinero). En la desesperación caótica sembrada por los propios criminales mediante la difusión de noticias falsas a través whatsapp y redes sociales (a quienes les tendiste amablemente una mano cuando sin chequear fuente y veracidad reenviaste), introducís el número de tu tarjeta, fecha de vencimiento y código de seguridad, quedando a la espera de que el milagro llegue por mail, Fedex, UPS o Correo Argentino a tu hogar. A veces van por menos, y en el formulario sólo te piden usuario y contraseña de alguna red que uses para el "loggeo". No es cuento ni invento, en varios países más adelantados en el avance del virus (y de todo el resto) ya se denuncian hechos como estos.

¿Y para que quieren nuestros datos? La respuesta es porque son lucrativos en el mercado. “Pará, pará pará...” ¿Me estas diciendo que alguien pagaría por...datos”? Exacto.

En la “Dark Web” (una especie de Mordor o Bosque Prohibido 2.0) funciona un mercado negro en el que se ofrece cualquier cosa: nuestros datos personales, credenciales, información bancaria y de tarjetas de crédito, drogas, pornografía infantil, los sicarios ofrecen “sus servicios”, hasta se califican entre vendedores y compradores. Es como Mercado Libre, pero todo es un poco más... digamos... ilícito.

Nuestra información es un producto valioso en ese mercado, aunque “onerosamente” es de la lista mencionada lo más “barato” (por la facilidad que tienen los criminales para juntarlos). Los clasifican, arman “combos” y ganan miles de dólares en el intercambio.



Ya sé lo que te estas preguntando... "**¿para qué quiere el comprador mis datos?**". Fines bien variados, pueden usarlos para suplantar tu identidad (hacerse pasar por vos dentro de la comunidad online), realizar operaciones financieras –si consiguieron los datos de tus cuentas o tarjetas- o valerse de esa información para hacerte víctima de un nuevo phishing o de una extorsión virtual.

La cuestión puede tomar otra dimensión y peligrosidad si en lugar de una web con un formulario se nos adjunta un archivo que descargamos. No lo vemos, no nos percatamos, pero esa "inhalación digital" hace que el indetectable virus entre por el sistema respiratorio de nuestro organismo virtual. ¿Te acordas de la historia del caballo de Troya? Bueno, ilustra perfecto porque a esos archivos los llaman "troyanos", tocan la puerta como un regalo, pero cuando los dejas entrar siembran destrucción y caos.

Pasa todos los días y cada vez más, y en épocas del COVID-19 la estadística va a aumentar. Ya se detectaron varios correos que incluyen troyanos conocidos como "Emotet", "Trickbot" y "AZORult" que roban la información alojada en el dispositivo donde los instalas. Vienen camuflados dentro de un PDF, un archivo de Excel o también descargarse automáticamente al seguir un enlace, cuyo destino es una página en la que, en lugar de un formulario, terminamos viendo... nada, está en blanco, pero aunque parezca vacía de contenido ahí estaba escondido el archivo. Le abrimos la puerta sin darnos cuenta al enemigo.

4 La “infodemia”. Fake news en épocas de pandemia.

Desinformar y confundir son actos preparatorios de los que se vale habitualmente un cibercriminal. Les permite crear un contexto que haga que sus técnicas de ingeniería social aumenten sus probabilidades de funcionar.

Esto es algo que la pandemia actual me permite explicar, desde enero de 2020 la cantidad de dominios registrados en la red vinculados con el COVID-19 ha aumentado significativamente, contabilizándose más de 1500 sólo en los últimos tres meses (un dominio en internet es la denominación que identifica a un sitio web en internet, vamos de nuevo, el “www” ...).

Seguramente muchas de esas webs sean legítimas y hayan sido creadas para prevenir, alertar y dar información cierta sobre el coronavirus, pero **un porcentaje considerable de dominios fueron registrados con el fin de difundir información errónea, de alojar páginas de phishing o cometer fraudes.**

La información falsa respecto del COVID-19 se viene difundiendo principalmente a través de las redes sociales (Twitter, Facebook e Instagram) y las plataformas de mensajería como Whatsapp. Pero cuando la información proviene de una web que se maquilla como oficial tiene una cuota extra de credibilidad. Los criminales se valen de esos dominios para publicar noticias falsas, o imágenes y videos que previamente fueron retocados/adulterados para cambiar su contenido o descontextualizarlos.

¿Cuál es el beneficio? El asedio de información puede provocar en muchos sentimientos de angustia, estrés, miedo y confusión, un cóctel ideal para volvernos más permeables a las técnicas de ingeniería social que nos disparan mediante spam. Esos estados emocionales influyen no sólo en nuestra salud sino también en nuestra conducta.

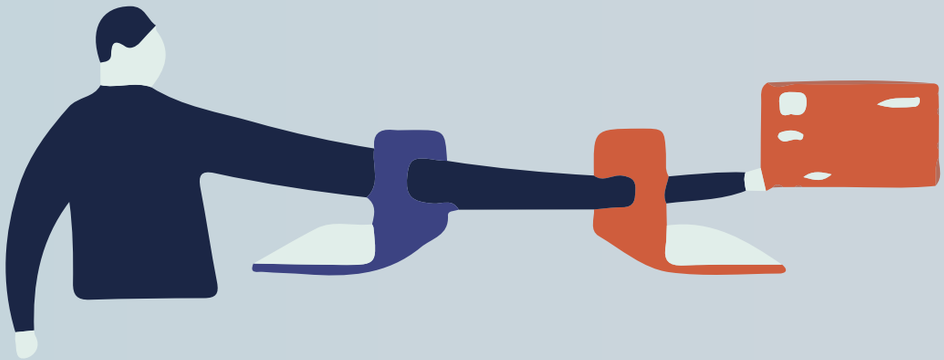
A modo ilustrativo, si leemos una recomendación sobre el uso de determinadas máscaras para prevenir el virus o una noticia que celebre el descubrimiento de una cura, es muy probable que nos dispongamos a buscarlas para comprarlas, si es que "casualmente" en la misma web no hay un enlace al sitio web en donde encontrarlas.

Cierto es que la diseminación de noticias falsas o adulteradas trae aparejadas alteraciones sociales como el pánico, el racismo y la xenofobia, pero sólo representan consecuencias colaterales a los fines de los criminales, quienes en realidad buscan generar un ambiente idóneo para que caigamos en trampas y fraudes.

5 Estafas y fraudes por medios digitales.

El contexto señalado es ideal para inducirnos a error mediante un engaño y lograr con ello que hagamos alguna disposición patrimonial que termine por perjudicarnos (lo que técnicamente se define como estafa en idioma abogado).

La paranoia sembrada por las noticias falsas dio lugar a cientos de fraudes –o al menos intentos- a lo largo de todo el mundo, que podrían ser miles si contemplamos por estimación los que no fueron advertidos o denunciados.



El ejemplo más claro es mediante la oferta en sitios web de máscaras faciales que nunca llegan al comprador o que son una burda falsificación. De hecho, aun cuando existan y sean legítimas, no cumplen con la función para la que se las publicita. Y es que en realidad son esenciales para la seguridad del personal médico, pero tienen poco efecto en la prevención de infecciones en personas sanas (la OMS recomienda que no se usen máscaras faciales a menos que se trate de un individuo con una sospecha de infección por COVID-19).

Otros casos de estafas actuales incluyen la venta de supuestos mapas de infecciones, medicamentos, vacunas y equipamiento médico que promete prevenir y erradicar el COVID-19 y cuyo único efecto es que nuestro patrimonio sufra un detrimento.

Acudí a esos ejemplos porque son los más habituales en estos días. Pero no saca de vigencia a las clásicas estafas cometidas a través de tiendas online (en las que tanto el comprador como el vendedor pueden ser víctimas).

También existen antecedentes de negociaciones empresariales que se llevaron a cabo puramente a través de mails o mensajes de texto y que resultaron ser fraudes.

No puedo dejar de mencionar que la mayoría de nosotros ha recibido –o recibirá- la triste noticia de que una tía rumana (cuya existencia desconocíamos) falleció y nos legó su fortuna. Festejamos con lágrimas –de tristeza y dicha- mientras leemos como el considerado abogado del extranjero (un rumano que escribe en perfecto español) nos da su pésame y nos hace saber que sólo necesitamos transferirle una "pequeña suma de dinero" para gestionar nuestra herencia.

Si bien estas trampas se ven muy poco sofisticadas y creíbles (mis colegas estarán pensando en la inidoneidad de los ardides), lo cierto es que hay un motivo por el que siguen circulando hace años: alguien cae, sí, de vez en cuando. Un despistado o un desesperado cada tanto es suficiente para seguir intentando.

6 Extorsiones 2.0.

Si nuestros datos sensibles llegaron a la persona equivocada por haber mordido el anzuelo o, porque ese pescador habilidoso luego vendió su pesca en el mercado negro 2.0, lo más probable es que un criminal intente chantajearnos con ellos.

Mails que advierten que cuentan con tu usuario y contraseña, documentos confidenciales, videos o fotos íntimas o el historial de tus visitas a páginas de pornografía o cualquier dato que pueda comprometerte –o a tu negocio- frente a tu pareja, clientes, círculo o familia. ¿El precio para dejarte en paz? Una módica suma de dinero digital (criptomonedas, ya las escuchaste mencionar).

Dentro de esta categoría también están los llamados **ataques de "ransomware"**, que se cometen a través de un software malicioso que instalaste al ser víctima de phishing, por visitar algún sitio o descargar un archivo comprometido.

En este caso, se nos restringe el acceso a nuestros archivos y carpetas, se inutiliza nuestro dispositivo y emerge una notificación que demanda dinero a cambio de poder recuperar control del mismo.

El "malware" (programa maligno) encripta nuestros archivos y restringe el uso de las funciones más básicas haciéndolo prácticamente decorativo hasta que no paguemos la suma exigida por el autor del delito (que oscila entre los 20 dólares y... no tiene techo, dependiendo el valor del sistema comprometido y los datos en juego).

Otro supuesto, muy de moda en este momento, es la **"sextorsión"**, en donde se amenaza a la víctima con divulgar o hacer públicas sus imágenes intimas. La exigencia puede ser en dinero o inclusive en más fotos y videos de connotación sexual.

¿Cómo obtuvieron mis imágenes? Puede ser que no las tengan y sólo usen esa amenaza para extorsionarte (y si de casualidad te fotografiaste y grabaste actúas en el convencimiento de que tu imagen esta en juego), también puede ser que te hayan robado o hayas perdido un dispositivo de donde las pudieron sacar, que hayas compartido esas imágenes en algún chat e inclusive que te hayan espiado remotamente a través de tu webcam o la cámara del celular.

7 Los menores de edad como víctimas predilectas del predador digital.

Hace algunos años la naturalización del uso de internet y sus facilidades devinieron en que los adultos otorguen acceso sus hijos a temprana edad como herramienta para comunicarse.

Hoy los niños son nativos digitales, la tecnología se les presentó a la par que los pañales y en muchos casos cuentan con más horas y expertise en la red que sus padres.

Pero la falta de control sobre el uso, tiempo y exposición de un menor, en conjunto con su inmadurez natural para hacer frente a determinada situación, lo hacen víctima del ciberpredador.

Como leones disfrazados de corderos, estos perversos utilizan el anonimato de maleza y señuelo, están constantemente al acecho. Generalmente crean perfiles con identidades falsas en redes sociales, las que más usan los menores y más olvidadas tienen los padres. Fue Facebook en su momento, pero Instagram, Snapchat y Tik Tok tienen el protagonismo en estos tiempos.

El "grooming" es la conducta más frecuente de la que tenemos alertarlos y protegerlos. ¿Qué es? En pocas palabras, un adulto que mantiene diálogo con un menor del que busca ganarse su confianza, establecer un vínculo o "amistad", y una vez que consigue esa retorcida conexión emocional, la usa para acercarse al niño que pretende abusar o cometer otro delito contra su integridad sexual.

El "sexting", un acrónimo que se forma de unir "sex" y "texting" es una tendencia que no es exclusiva de quienes transitan la adolescencia, pero los menores de edad son los más vulnerables a sus consecuencias. ¿Qué implica? Enviar mensajes con fotos y videos íntimas a través de alguna aplicación de correo o mensajería.

Los adultos lo usan como práctica sexual en sí misma, para subir la temperatura entre parejas o cuando están conociendo a alguien a través de redes sociales o aplicaciones de citas -si, como Tinder y Happn, no pongas mirada distraída ;)-.

Todo suena candente y sensacional hasta que esa imagen o video aparece en un lugar adonde no debería llegar. Una difusión no consentida de ese archivo, "pornovenganza" (creo que el término es autosuficiente y no cabe agregar nada más) o una filtración de seguridad son suficientes para que esa imagen íntima se distribuya como virus a un ritmo descomunal.

Ahora bien, estamos lo suficientemente creciditos como para hacernos cargo de lo que decidimos, no sucede lo mismo cuando la misma conducta la lleva a cabo un niño.

Los menores, inclusive los pre-adolescentes de 10 y 12 años también lo hacen, "pero mi hijo no..." ¿estas 100% seguro y consciente de lo que tu hijo hace en redes...? Ojalá no sea el caso, pero lo cierto es que por diversión o imitación, o quizás producto del grooming de un perverso agresor, los más chicos también sextean al día de hoy.

¿Consecuencias? Graves e inmensas. La más liviana es que su imagen se comprometa con todos sus compañeros de la escuela, el bullying que le espera y los efectos que eso conlleva de por vida en su psiquis como carga eterna.

¿Eso era lo más liviano? Imaginemos el siguiente escenario: Un groomer crea un perfil falso en el que simula ser un menor de la misma edad que su víctima potencial. Consigue de aquél su confianza y su amistad, lo seduce y logra que el menor le envíe una imagen de contenido sexual. A partir de ese momento empieza un círculo extorsivo que no tiene final. Lo amenaza con que si no le envía más contenido divulgará el que tiene a sus compañeros, a su papá y su mamá. El niño aterrorizado y acorralado por las posibles consecuencias envía otra imagen más, en la falsa esperanza de que con eso todo terminará. Que equivocado está, el depredador sexual no se conforma jamás, de hambre voraz extorsionará al niño hasta el final... Prefiero no contar el final.

El grooming y el sexting son algunas de las fuentes de explotación sexual documentada de menores de edad. ¿De la qué?! En la Ley como **"Pornografía infantil"** la encontras.

¿Te acordás del mercado negro de la Dark Web? Las imágenes producto del grooming, sexting y los abusos consumados se difunden, se intercambian y ahí se pueden vender. Ni siquiera hay que escarbar muy profundo y navegar en la "Deep Web" (un sector no indexado de la red, cuyo contendido en una simple búsqueda no va a aparecer), en la superficie el producto de la explotación sexual infantil se encuentra también.

El Estado dedica mucho esfuerzo y recursos a perseguir esas perversidades, pero desde la educación y la toma de conciencia pueden prevenirse y evitarse.

Finalmente, los menores han sido históricamente víctimas y victimarios del acoso y hostigamiento (bullying) en las escuelas y colegios. Internet y el uso de las redes sociales es una herramienta muy funcional a tal efecto y, como veremos, los adultos ya no son ajenos a eso.

8 Hostigamientos y acosos virtuales.

Maltrato, molestias y acoso son acciones que ya se ven con más asiduidad en la interfaz digital por sobre la física.

Sabemos que las redes sociales son el entorno predilecto para las campañas de violencia, humillación y escraches, los vemos en Twitter, Instagram y Facebook con una naturalidad que es preocupante.

El actual contexto de la cuarentena impuesta por el COVID-19 puede ser leña que avive el fuego de los hostigamientos y acosos digitales. El "tiempo extra" y el mayor contenido que circulará en este tiempo funcionarán como detonantes, en este punto espero equivocarme.

Quienes los despliegan, "trolls" y "haters" en lengua moderna, suelen tener un gran número de lectores (contactos, seguidores) tienen el poder de poner a cualquier persona frente a una multitud de jurados virtuales que en su mayoría emiten veredictos lapidantes contra quien se juzga simple y llanamente por su afinidad con el usuario hostigante.

Estos criminales –que jamás se reconocerían como tales- no necesariamente tienen amplios conocimientos informáticos, de hecho, cualquiera puede ser autor de ese tipo de ataque. Las víctimas preferidas suelen ser personalidades de la política, del espectáculo o influencers de las redes sociales, aunque todos somos targets potenciales.

Un paso en falso, un error, una fotografía, un video o simplemente la expresión de una idea son suficientes para desatar una guerra de humillación, en la que estos personajes reclutan a sus lectores/seguidores a sumarse al ataque, multiplicando así su capacidad vulnerante.

Disparan publicaciones y comentarios sin compasión como si contaran con una ametralladora cuyas balas son la incitación al odio y humillación, lo hacen de modo sistemático y reiterado, sin contexto ni compasión. Acribillan con palabras, generalmente ocultando su identidad, y eso produce consecuencias fuera de la realidad virtual, produce dolor, dolor real, angustia, ansiedad y una sensación de censura que termina limitando el derecho a expresarse libremente ante los demás.

Si los casos de bullying en redes sociales no te parecen lo suficientemente graves, déjame decirte que **hay decenas de antecedentes documentados que en el suicidio de la víctima derivaron.**

En este sentido, el aislamiento por cuarentena no sólo aumenta las posibilidades de casos de cyber-bullying, sino que además es una circunstancia que agrava sus consecuencias.

9 Métodos de prevención para cuidarse en entornos digitales.

Tarde o temprano aparece una cura o un remedio para todos los males, pero soy un convencido de que prevenirlos es la mejor forma de tener que evitar curarse (ocuparse para no preocuparse). Va un listado de tips y recomendaciones para –en cierta medida- inmunizarse. Tomalo como "check-list" para cuidarte.

- **No tengas la red Wifi de tu casa u oficina abiertas** (sin contraseña). Configura la red con cifrado "WPA2". Eso lo haces desde las opciones del router. ¿Cómo? Depende del modelo y del proveedor (arnet, fibertel, telecentro, etc...), en el manual que te proveyeron con el modem está la información. Si lo tiraste o no lo encontrás ingresa a la web de tu proveedor de internet o llamá al número de atención al cliente para que te guíen.

- Como extensión del consejo anterior, **generá contraseñas robustas y modificalas con asiduidad.** No uses fechas de cumpleaños, ni siquiera de familiares cercanos, fragmentos de tu nombre o de allegados, olvidate de la patente del auto o de cualquier combinación con menos de 7 caracteres de longitud, todas se descifran a través de software malicioso relativamente fácil y rápido.

LAS CONTRASEÑAS SON COMO LA ROPA INTERIOR

cambialas seguido, mantenelas privadas y no las compartas

- **No uses una contraseña para todo**. Si la cerradura de tu casa, tu auto y tu oficina se abren con llaves distintas para acceder a todos tus dispositivos y cuentas no pretendas usar la misma ;).

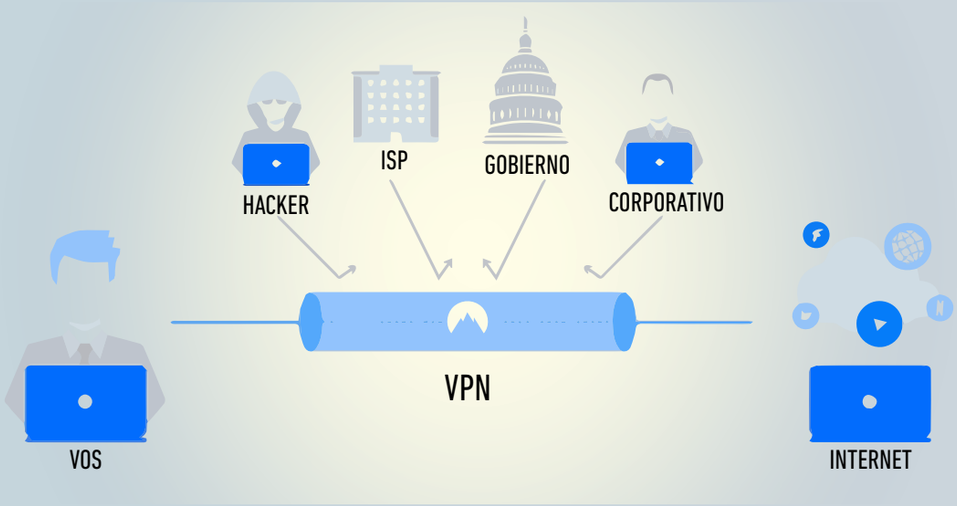
- **Revisá si el sistema operativo de tus dispositivos está actualizado** a la última versión, inclusive los pequeños "updates" cotidianos suelen tener relación con su protección. Activar las actualizaciones automáticas puede ser una buena decisión.

- **¿Tenés un programa de antivirus?** ¿En todos tus dispositivos? Que adquieras uno es la recomendación. Si, no sólo para la PC, para teléfonos y tablets también. Las marcas principales ofrecen combos para proteger todos tus dispositivos al mismo tiempo e inclusive algunos extensivos a toda la familia para que todos le saquen provecho. No es un costo, es una inversión. Te aseguro que la prevención es más barata que la solución (ESET, McAffee, Norton, AVG, Kaspersky, BitDefender, Panda, son algunas de las más confiables como marcas).

- **Ojo con ingresar datos,** contraseñas y hacer operaciones financieras desde redes abiertas (vamos de nuevo: gratuitas, sin contraseña). Generalmente están en aeropuertos, cafés, restaurantes, museos, etc. Por las dudas, cuando digo "ojo" estoy diciendo "QUE NI SE TE OCURRA HACERLAS".

- Que no cunda el pánico por el punto anterior, configurar una red **VPN** puede ser una solución. Las siglas son por **"Virtual Private Network" (Red Privada Virtual).**

Para explicarlo quiero que imagines que los datos de red son cartas que envías por el correo tradicional. Las remitís para que la lea el destinatario final, nadie más. Sin embargo desde el punto de inicio al punto de destino esa carta pasa por muchas personas y lugares distintos (el cartero, el personal del correo, quien la lleva a destino final, etc.) Una red privada virtual garantiza que la carta llegue cifrada (cerrada) al otro extremo, y que a pesar de que muchos tuvieron contacto con el sobre ninguno pudo ver que había dentro.



Puede configurarse en cualquier computadora (independientemente de que utilice Windows o Mac) y también en dispositivos móviles (independientemente de si utilizan Android o iOS).

Enseñar a hacerlo correctamente excede el objeto y longitud de este libro (una buena frase para camuflar que "no tengo tan claro cómo se hace, se lo pedí a un informático amigo :p).

- **No ingreses datos personales en sitios no seguros** (verifica que la dirección inicie con "HTTPS" y veas el ícono de un candado acompañándola al lado). Va una captura de pantalla de como luce la barra de direcciones para ilustrarlo.

- Cada vez que recibas un correo electrónico o un mensaje de texto sentite pez que no quiere ser pescado, inhala profundo y repetite esto como mantra antes de "morder" algo: **"no voy a hacer clics en links ni descargar archivos que no estaba esperando y provienen de un desconocido"**. Escribo divertido, pero hablo bien en serio: REPETILO.

- Específicamente, no entres a las webs de entidades bancarias siguiendo un enlace de un correo electrónico, tipea la dirección en la barra correspondiente o crea un acceso directo en favoritos para facilitarte el acceso.

- Dejemos en claro esto: "**Las empresas serias** NO piden información personal o financiera por correo electrónico o mensajes de texto". Léelo de nuevo, ahora en voz alta, otra... hasta que no se te grabe que no se corte el loopeo (dale, aprovecha que rima, hacelo).

- Cuando recibas un mail **verificá la autenticidad del remitente**. El nombre que figura como "descripción" no es indicio suficiente. Yo puedo crear una cuenta y poner que vos leas que te escribió el Presidente, pero el dominio nunca miente (lo que viene después del "@" en la dirección del remitente). Si ofrezco la cura del COVID-19 presentándome como funcionario de la OMS, pero mi dirección de correo es jorgelitvin@teestahackeando.com espero que cuanto menos sospeches de la verosimilitud de lo que se te ofrece.

- **Habilitá la doble-verificación en todas las plataformas en las que esté disponible (Google, Instagram, Facebook, Twitter y LinkedIn de movida lo permiten)**. ¿Qué es? Un paso extra de seguridad para acceder a tus cuentas, cada inicio de sesión en un nuevo dispositivo exige un código que se manda al número de celular (o a un mail alternativo) que pusiste al crear la cuenta. Esto significa que aún cuando descifren o roben tu contraseña, sólo quien tenga acceso a tu móvil o a tu correo alternativo podrá acceder a tu cuenta.

Como quiero que esto lo hagas ya, te invito a que vayas a los anexos del final. Ahí vas a encontrar un tutorial con el paso a paso en imágenes de cómo configurar la doble verificación en cada red social. Hasta que no lo hagas en todas las que uses, al siguiente tip no te dejo avanzar (espero tener algo de autoridad).

- La mayoría de las aplicaciones y plataformas exigen la creación de un usuario para iniciar sesión (por ejemplo, hoy está muy de moda "Zoom" para trabajar y estudiar de forma remota).

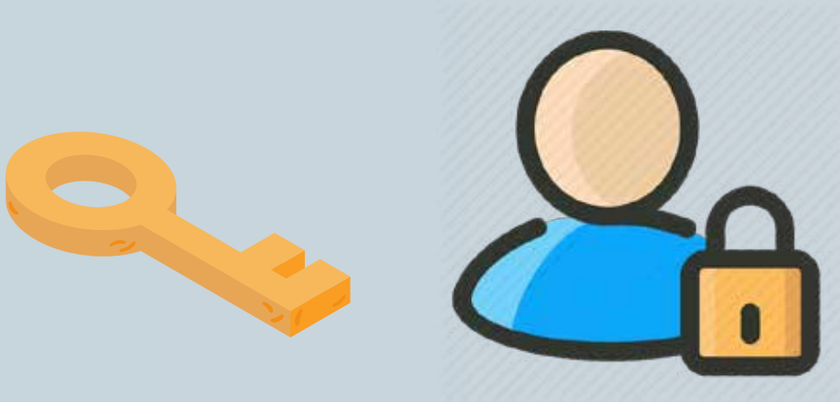
El alta de tu nuevo usuario exige rellenar un formulario con tus datos, "¿otra vez?". Hay una alternativa: un camino corto y tentador "iniciar sesión con...".

Se te ofrece que con una cuenta de Facebook, Twitter, Google o alguna otra red social hagas el log. Es mucho más cómodo que rellenar otro formulario, ¿no?. Por supuesto, pero el precio del atajo pueden ser tus datos (todos a los que les des acceso y que en la red social que estas usando tengas alojados).

Ante la duda mejor completar el formulario entregando solo los datos que son indispensables (suelen estar identificados con un *). Si te parece que para lo que te ofrecen te están pidiendo información de más, replanteate si realmente la necesitas.

- Webs y aplicaciones que te permiten revisar quién te bloqueó, quién ve tu perfil y te piden usuario y contraseña de la red, suelen ser el moño con el que el acceso y control a tu cuenta envolvés. Ni siquiera es un dato que vale la pena saber, ni lo intentés.

- Salvo que seas un usuario que genera contenido en redes sociales a la expectativa de obtener alcance (como un influencer, empresa, emprendimiento o por motivos laborales), **mejor mantené privados tus perfiles.** Evitá abrirle la puerta a desconocidos a que husmeen quiénes son tus amigos, tus familiares, horarios y lugares en los que pueden encontrarte, y mucho mejor si no se enteran de que te fuiste de viaje. Después la gente se sorprende cuando regresa y encuentra su casa vacía post-viaje, pero "¿CÓMO SE ENTERARON?", estem... vos lo publicaste.



- Por supuesto que el sentido del punto anterior es resguardar tu privacidad y seguridad, lo cual quedaría invalidado si toda solicitud de seguimiento o "amistad" aceptás. Prestá atención a las cuentas que no tienen contactos, que nadie las sigue, que no usan nombre y apellido y no tienen una imagen de perfil que como personas las identifique. ¿Si alguien con pasamontañas toca timbre para entrar a tu casa le abrirías la puerta? Me gustaría pensar que no. En redes el anonimato es el pasamontaña digital, a los que lo usan mejor no los dejes entrar.

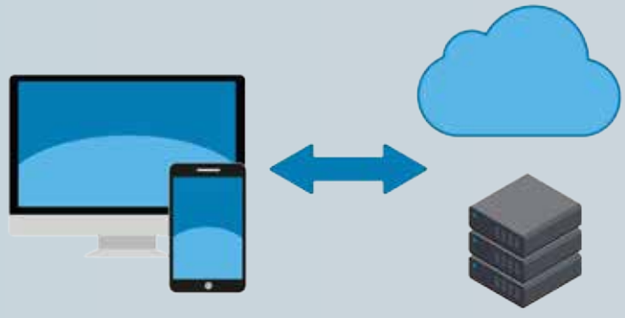
- Vamos con los fraudes: Ofertas increíbles, veamos... IN-CREÍBLES, ¿me entendiste? **Si algo se ve demasiado bueno para ser verdad lo más probable es que haya algo oculto detrás**. Que las ganas no te quiten el criterio y te hagan víctima de una estafa. Si los científicos de Israel siguen trabajando en una vacuna contra el coronavirus, ¿qué te hace pensar que la que te ofrecen por correo electrónico tiene algo de legítimo?

- A todos nos resulta más sencillo –y hoy indispensable- comprar online. Para prevenir un fraude a) constatá que la página empiece con "https://"; b) Si el vendedor es una empresa, nunca está de más hacer una pequeña búsqueda en internet para verificar la razón social, domicilio físico, opiniones de otros compradores, básicamente corroborar si existe en realidad; c) En lugar de un giro de dinero o transferencia, paga con tarjeta (las operaciones realizadas con ellas están protegidas por las entidades y sus divisiones antifraude).

- Los vendedores también son víctimas de fraudes por operaciones realizadas en la web. La modalidad es bien conocida: el comprador paga con tarjeta de crédito y luego de recibir el producto desconoce el pago ante el ente emisor, que en muchas casos reintegra al verdadero estafador el dinero. Una posible recomendación es ofrecer productos mediante plataformas que tengan habilitada la verificación 3DSecure (generalmente aparece el logotipo de "Verified by Visa" o "SecureCode by MasterCard").

Muy brevemente. Cuando hacemos una compra online se nos requiere el número de la tarjeta, su fecha de caducidad y el criptograma visual (¿el qué!?: el Código de Seguridad). Con lo cual, con cualquier tarjeta ajena o conociendo los datos de aquella (por obtención ilegitima física o digital) se podría comprar. La verificación 3DS agrega un paso más. Una vez ingresados esos datos y al confirmar la compra se nos redirecciona a una web del banco emisor que autentifica que quien esta haciendo la compra es el tarjeta habiente en cuestión. ¿Cómo? Puede requerir un password, tarjeta de coordenadas o token, u otro dato pre-configurado que valida la identidad de quien está comprando.

- **Hacé copias de seguridad de tus datos más importantes.** Puede ser en un disco rígido externo o en la nube (Dropbox, Google Drive, Microsoft One Drive, etc.). De este modo si quieren bloquear tu acceso a ellos mediante ransomware pero vos tenés acceso a recuperarlos, los despojas de una motivación para cumplir con el pago. Y lo importante: Mantenés íntegros tus datos.



- **Antes de instalar una aplicación o descargar un software preguntate si es realmente necesario.** De ser así, buscá en la descripción (la "letra chica" diríamos los juristas) a qué le das acceso cuando la instalas, si te parece excesivamente intrusiva la evitas.

Por poner un ejemplo, una determinada app de "linterna" es lógico que pida acceso a la cámara para poder usar el flash, pero qué pasa si además le das acceso al ubicación, fotos, videos y el ID de llamada de tu teléfono; o si un juego infantil pide permiso para ver tus contactos y la información de tu red wifi. Suena a exceso, ¿no? **De eso es lo que quiero que estés atento.**

- En línea con el punto anterior, **si tenés dudas sobre los permisos que otorgaste o si sentís que la seguridad de tu dispositivo puede estar comprometida cubrí la cámara cuando no la usás.** Es un buen momento para revisar a cuáles aplicaciones le diste permiso de acceder a ellas (si ahora, ya). No es por exagerar, no es de ciencia ficción lo que imagins.

- **No grabar videos ni capturar fotos íntimas es la mejor medida preventiva contra la sextorsión que te puedo dar.** Si lo vas a hacer igual, encriptá los archivos y no se los mandes absolutamente a nadie. Después de este artículo espero que mejore mucho tu manejo de la seguridad virtual, pero no podemos asegurar que a quienes les envíes ese contenido serán igual de prolijos en su ciberseguridad.

- **Si notás que se está llevando a cabo algún procedimiento extraño o si sentís que fuiste hackeado (porque alguna vez caíste en algo de lo que venimos mencionado) desconectá tu dispositivo de internet de inmediato.** Activá modo avión para los que para navegar utilizan datos. Corré un análisis de anti-virus/anti-malware hasta que te saques la duda de si hay "algo" infiltrado. Cambiá tus contraseñas desde un dispositivo distinto al que sospechas infectado y no sería mala idea dar aviso a tu banco.

- **Si tenés hijos menores de edad utilizá las herramientas de "controles parentales".** Permiten tener registro y evitar que accedan a material inapropiado, también habilitan establecer un tiempo de uso de los dispositivos. Concientízalos del funcionamiento y los riesgos de la tecnología e internet.

Es un tema que incluso sirve como punto de vinculación. Por si te sirve el consejo (tómalo o déjalo): a mis hermanos menores les pregunto por las aplicaciones que están usando y les pido que me cuenten para qué sirven y por qué la descargaron.

- **Alertá a los mayores de edad**. A tus padres, a tus abuelos, o a cualquier familiar que no maneje debidamente el mundo 2.0. Los mayores suelen ser víctimas preferidas, advertiles de la existencia de mensajes y llamados telefónicos fraudulentos, son el medio de ataque predilecto.

Los criminales suelen hacerse pasar por un familiar solicitando dinero, una entidad bancaria pidiendo datos o manifestando que le harán un cambio de billetes por otros nuevos, o un empleado público que ofreciendo gestiones de la ANSES.

Establezcan una "pregunta y respuesta de seguridad" que sólo conozcan ustedes, de modo que se revele si alguien intenta hacerse pasar por vos para engañar. Insistí en que no brinden información personal ni financiera a desconocidos, que no hagan depósitos si les ofrecen premios o planes de ahorro. Ante la mínima sospecha, que corten el teléfono.

- **Cuando recibas noticias, audios o imágenes siempre verificá la autenticidad del contenido y su autoría antes de reenviarlas y desparramarlas por todas partes.** Además de estar colaborando con el caos estarías desinformando, y con los mismos cibercriminales que te buscan como presa estarías colaborando.

10 ¿Se puede contraatacar?

Para todos los escenarios descriptos hay una respuesta contemplada en el Código Penal de la Nación o bien en el Contravencional de la Ciudad de Buenos Aires (hay determinadas acciones que aún no son consideradas reprochables por las demás legislaciones locales –por ejemplo la suplantación de identidad y los hostigamientos digitales-).

Aunque soy penalista este artículo no pretende hacer un análisis dogmático de la estructura típica de todas las conductas que fueron descriptas, eso será objeto de una publicación distinta, para mis colegas juristas.

El fin es otro, y es que todos los individuos de la sociedad que están leyéndome resguardados y conminados a permanecer en su hogar sepan que en estos tiempos de vida digital hay otros "virus" circulando, de los cuales también tenemos que cuidarnos ya que son de muy fácil contagio. No podemos verlos y no es seguro que una vacuna nos libre de ellos, la cepa muta y mejora todo el tiempo.

Por ahora me conformo con generar conciencia, poner alerta. Que sepan que hay un fenómeno que existe para que tomen todos los recaudos posibles para protegerse del cibercrimen.

ANEXOS

I

¿Qué, dónde y cómo denunciar?

Espero que este sea el anexo menos consultado. También espero que llegado el caso, si sos víctima de hechos como los que se explicaron, no dudes en denunciarlos.

Lo que busca este libro es prevenir, y una forma de hacerlo es que los delincuentes dejen de sentirse impunes por los ilícitos que cometen.

Para ello es fundamental que frenemos el aumento de la "cifra negra del delito": el número de aquellos cometidos, pero que no llegan a conocimiento de las autoridades por distintos motivos.

¿Cuáles?

1 - Las personas no se dan cuenta que fueron víctimas de "algo".
2 - Las personas no saben que ese "algo" configura un ilícito.
3 - Las personas que si saben que fueron víctimas de un "algo" que por la Ley puede ser investigado y reprimido, no saben cuál es la contravención o el delito.
4 - Los que si saben todo lo anterior, desconocen dónde denunciarlos, o no lo hacen pensando que es un trámite tedioso o, que para ello necesitan contratar un abogado.

¿Qué se puede denunciar?

En primer lugar, aclaremos que no es necesario que sepas ni cites ninguna normativa para denunciar. Alcanza con que relates lo que te sucedió, si es posible que lleves toda la prueba que lo acredite con vos, el Servicio de Justicia se va a encargar de calificar el hecho por vos.

Quienes residimos en la Ciudad de Buenos Aires, somos privilegiados por el compromiso, los recursos y la vocación que tiene el Ministerio Público Fiscal para investigar este tipo de hechos, a pesar de las dificultades y obstáculos propios que presenta el entorno 2.0.

Soy consciente de que la situación no es idéntica en todos los sectores del país, pero confío en que pronto lo podremos revertir.

Dicho esto, a mero título informativo, dejo enumeradas algunas de las conductas vinculadas con nuestra vida digital tal como están contempladas por el –aún vigente- Sistema Penal:

- Injurias y calumnias: Los clásicos ataques contra el honor, pero usando como medio la internet (Arts. 109 y 110 del Código Penal).
- Explotación sexual de menores documentada: distintos supuestos de producción, ofrecimiento, comercialización y distribución de "pornografía infantil" (Art. 128 del Código Penal).

- Exhibiciones obscenas (Art. 129 del Código Penal)
- Grooming (Art. 131 del Código Penal)
- Amenazas y Coacciones a través de medios digitales (Art. 149bis del Código Penal)
- Acceso, interceptación, desvío o supresión ilegítima de comunicaciones electrónicas: Los habituales "hackeos" de cuentas de correo electrónico y aplicaciones de mensajería (Art. 153 del Código Penal).
- Acceso ilícito a sistemas informáticos: Suelen tratar de ingresos no autorizado -o excediendo la autorización poseída- a datos restringidos en cualquier sistema (Art. 153bis del Código Penal).
- Publicación abusiva de comunicaciones electrónicas (Art. 155 del Código Penal)
- Violación de secretos por medios informáticos (Art. 156 y 157 del Código Penal).
- Acceso, revelación o inserción ilegítima de información contenida en un banco de datos personales (art. 157bis del Código Penal).

Extorsión –ransomware- y chantaje –sextorsión- (Arts. 168 y 169 del Código Penal)

- Estafas cometidas por medios informáticos y fraudes informáticos (Arts. 172 y 173, inc. 16º del Código Penal)
- Daño informático: La alteración, destrucción o inutilización de datos, documentos, programas o sistemas informáticos (Arts. 183, segundo párrafo y 184, inciso 6º del Código Penal).
- Interrupción de comunicaciones: Casos de ataques de denegación de servicios o DDOS –por sus siglas en inglés "Destributed Denial of Service"- (Artículo 197 del Código Penal).

- Sustracción, alteración, destrucción o inutilización de evidencia digital (Art. 255 del Código Penal).
- Algunas modalidades de delitos contra la propiedad intelectual: Delitos de piratería y distintos supuestos de fraudes relacionados con el copyright (Arts. 71 y siguientes de la Ley 11.723).

Otras conductas, de las cuales somos víctimas habituales pero que -lamentablemente- por ahora sólo califican como contravenciones en el ámbito de la Ciudad Autónoma de Buenos Aires:

- Difusión no autorizada de imágenes o grabaciones íntimas (Art. 71bis del Código Contravencional de la CABA)
- Hostigamiento digital (Art. 71ter del Código Contravencional de la CABA)
- Suplantación de identidad (Art. 71quinquies del Código Contravencional de la CABA).

¿A dónde denunciar?

En todo el país.

- Presencialmente en una fiscalía. Haciendo clic en el siguiente enlance accedes al mapa completo https://www.mpf.gob.ar/mapa-fiscalias/.
- Llamando al 134 para denunciar casos de grooming.
- Ante la duda, la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) cuenta con un canal de orientación a las víctimas vía correo electrónico (denunciasufeci@mpf.gov.ar) . Pueden escribir un correo contando su caso y se las orientará para concretar la denuncia del modo más conveniente.

El Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires cuenta además con los siguientes canales de denuncia:

- Podes comunicarte al 0800-333-47225.
- Descargate la aplicación "Denuncias MPF" disponible en iOS y Android Store.
- Desde la web www.mpfciudad.gob.ar.
- Presencialmente, podes buscar la unidad fiscal más cercana a tu domicilio en www.fiscalias.gob.ar/presencial.
- En la División de Delitos Tecnológicos de la Policía Federal Argentina (Cavia 3350 – CABA).

Recomendaciones para colaborar con la investigación.

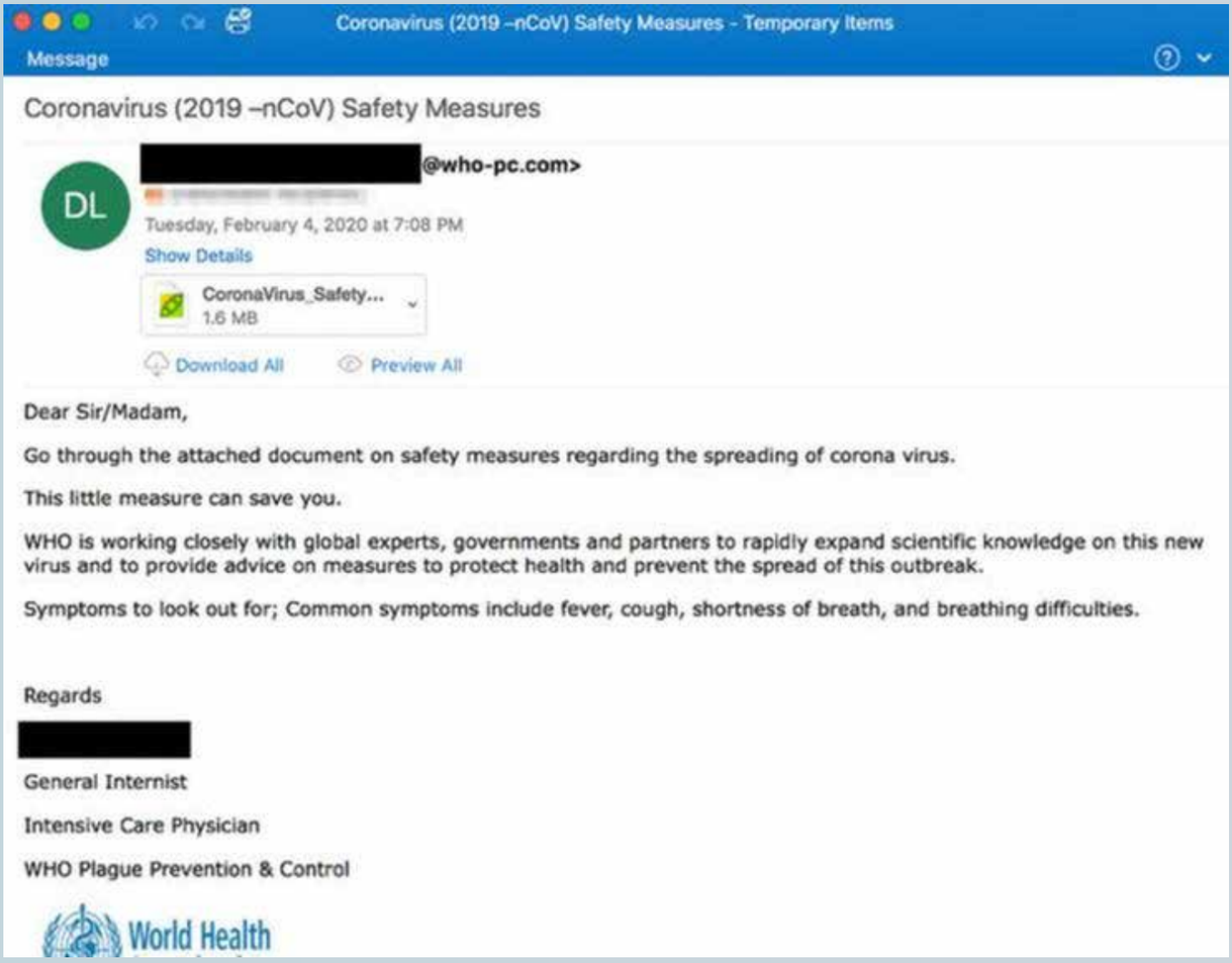
Uno de los mayores obstáculos de las investigaciones digitales es que la evidencia es muy volátil. Es muy fácil eliminarla o hacerla inutilizable. Algunos consejos para que no te pase:

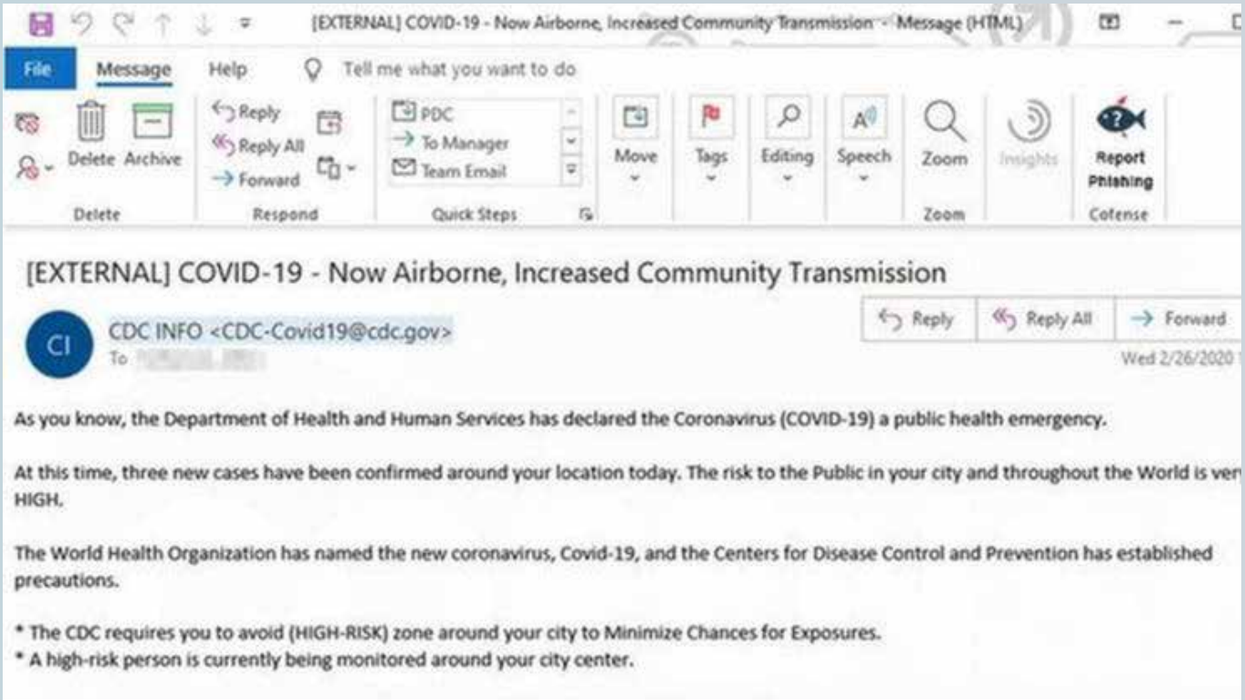
- Evitá alterar las pruebas de lo que te sucedió.
- No apagues ni modifiques la configuración del dispositivo involucrado.
- No modifiques ni elimines ninguna información vinculada con el hecho.
- No reenvíes el material a nadie hasta que no hayas radicado la denuncia.
- Documentá toda la evidencia posible tomando capturas de pantalla. De ser posible y contar con los medios, hacelo con un escribano. Ante cualquier duda, busca asesoramiento, legal e informático. Un abogado y/o un perito calificado pueden guiarte para resguardar la prueba e indicarte cómo proceder de la mejor manera.

II

Ejemplos reales de phishing y fraudes

Phishing





[EXTERNAL] COVID-19 - Now Airborne, Increased Community Transmission - Message (HTML)

File Message Help Tell me what you want to do

Delete Archive | Reply Reply All Forward | PDC To Manager Team Email | Move | Tags | Editing | Speech | Zoom | Insights | Report Phishing

Delete Respond Quick Steps Zoom Cofense

[EXTERNAL] COVID-19 - Now Airborne, Increased Community Transmission

CI CDC INFO <CDC-Covid19@cdc.gov>

To [redacted]

Reply Reply All Forward

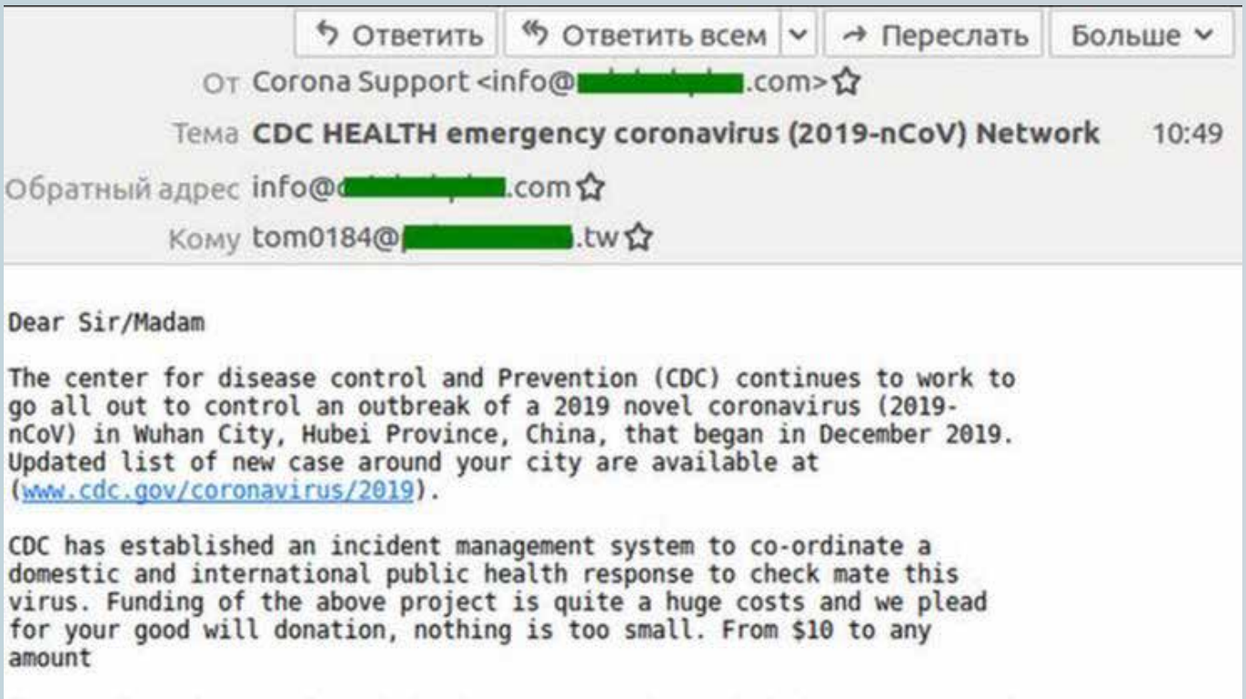
Wed 2/26/2020

As you know, the Department of Health and Human Services has declared the Coronavirus (COVID-19) a public health emergency.

At this time, three new cases have been confirmed around your location today. The risk to the Public in your city and throughout the World is ver HIGH.

The World Health Organization has named the new coronavirus, Covid-19, and the Centers for Disease Control and Prevention has established precautions.

* The CDC requires you to avoid (HIGH-RISK) zone around your city to Minimize Chances for Exposures.
* A high-risk person is currently being monitored around your city center.



Ответить | Ответить всем | Переслать | Больше

От Corona Support <info@[redacted].com>

Тема **CDC HEALTH emergency coronavirus (2019-nCoV) Network** 10:49

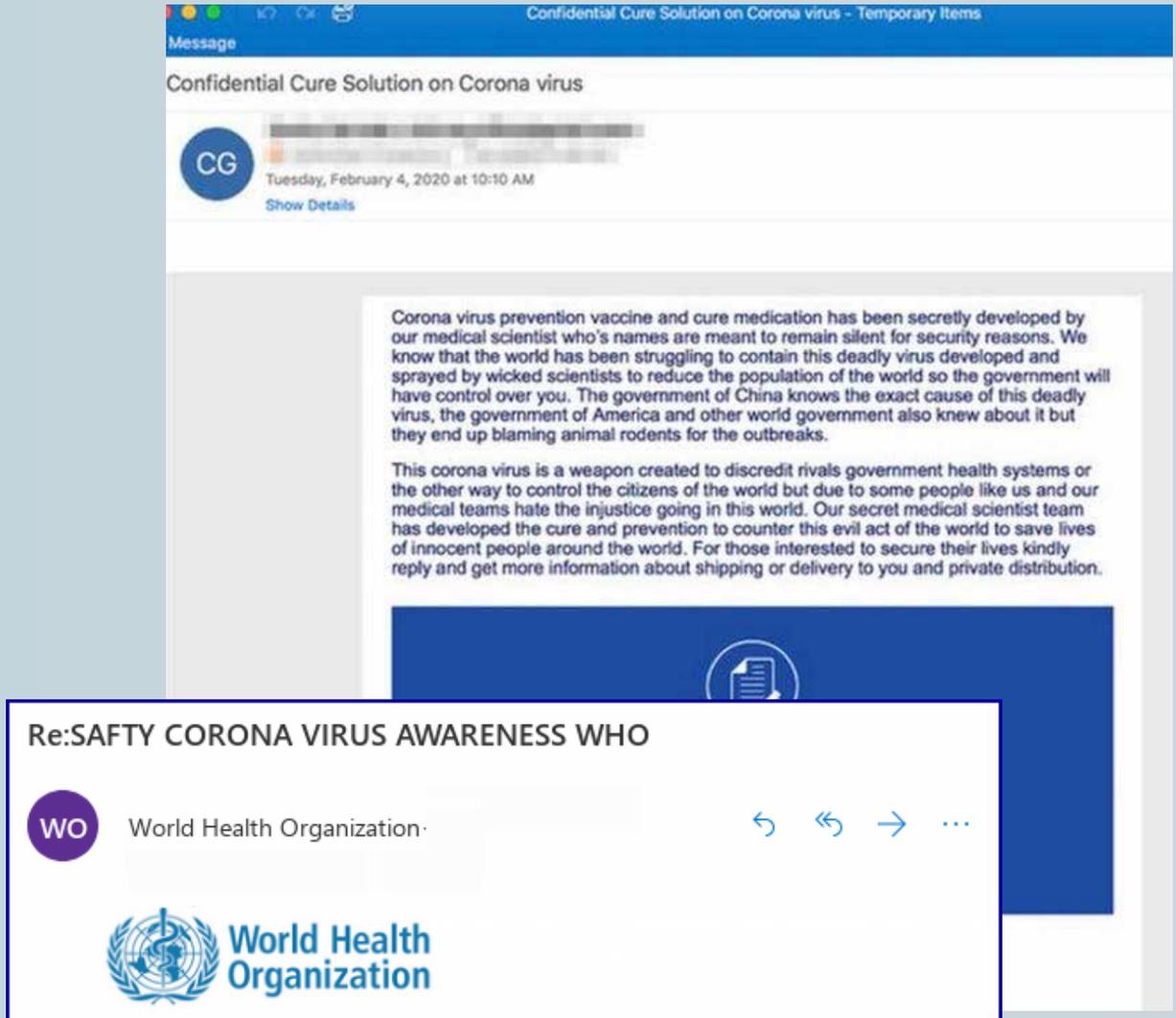
Обратный адрес info@[redacted].com

Кому tom0184@[redacted].tw

Dear Sir/Madam

The center for disease control and Prevention (CDC) continues to work to go all out to control an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China, that began in December 2019. Updated list of new case around your city are available at (www.cdc.gov/coronavirus/2019).

CDC has established an incident management system to co-ordinate a domestic and international public health response to check mate this virus. Funding of the above project is quite a huge costs and we plead for your good will donation, nothing is too small. From $10 to any amount


Confidential Cure Solution on Corona virus - Temporary Items
Message
Confidential Cure Solution on Corona virus
CG
Tuesday, February 4, 2020 at 10:10 AM
Show Details
Corona virus prevention vaccine and cure medication has been secretly developed by our medical scientist who's names are meant to remain silent for security reasons. We know that the world has been struggling to contain this deadly virus developed and sprayed by wicked scientists to reduce the population of the world so the government will have control over you. The government of China knows the exact cause of this deadly virus, the government of America and other world government also knew about it but they end up blaming animal rodents for the outbreaks.
This corona virus is a weapon created to discredit rivals government health systems or the other way to control the citizens of the world but due to some people like us and our medical teams hate the injustice going in this world. Our secret medical scientist team has developed the cure and prevention to counter this evil act of the world to save lives of innocent people around the world. For those interested to secure their lives kindly reply and get more information about shipping or delivery to you and private distribution.


Re:SAFTY CORONA VIRUS AWARENESS WHO
WO
World Health Organization
World Health Organization
Dear Sir,
Go through the attached document on safety measures regarding the spreading of corona virus.
Click on the button below to download
Safety measures
Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulties.
Regards,
Dr. Stella Chungong
Specialist wuhan-virus-advisory
FAKE

Apple ID

Para: informed-receipt@apple.com Cco: Jorge Litvin

Re : [Payment Receipt] [Receipt from App Store] 600 Diamonds Mobile Legends™, Order No. 258100982. Your purchases from App Store on Saturday, March 14, 2020 *Thailand Time [GMT+7]

Thank you,
You've made a purchase from Montoon on App Store.

Order number: 258100982
Ordered on: March 14, 2020 * Thailand Time (GMT+7)

You can see invoice and cancel this order on attachment. Thank you

Receipt-258100982.docx

s Master 18:07

Ver como página Web

Argentina

mastercard

SERVICIOS INHABILITADOS POR SEGURIDAD.

Estimado usuario:

Le informamos que se han registrado movimientos extraños dentro de su cuenta y por eso hemos decidido suspender sus servicios hasta realizar la verificación correspondiente.

Para mantener su seguridad online le recomendamos seguir el proceso de validación de identidad, así podremos asegurar la integridad de sus datos y mantenerlos seguros dentro de nuestra base de datos

VALIDAR INFORMACIÓN

Esta verificación no le tomará más de 5 minutos y la reactivación de sus servicios será inmediata.

MC 1967-2019

Enviado por **Netflix pagos argentina**

Apple ID. Entrada - Jorge Luis Litvin 13 de marzo de 2020, 17:14

[Informe de hoy] EN 13/03/2020: Alguien ingresó recientemente al sistema de inicio de sesión para iniciar sesión e... Detalles

Cc: 5f7qznkgafhxofyedbcnrtahr@jtxgm3vo.1u4j8q64ygr1bzz.id

APPLE ID

Estimado/a Cliente,

Lamentamos informarle que su cuenta ha sido bloqueada temporalmente en la cartera de **Apple-Particulares** en línea. Para su seguridad, complete de inmediato la siguiente verificación de cuenta.

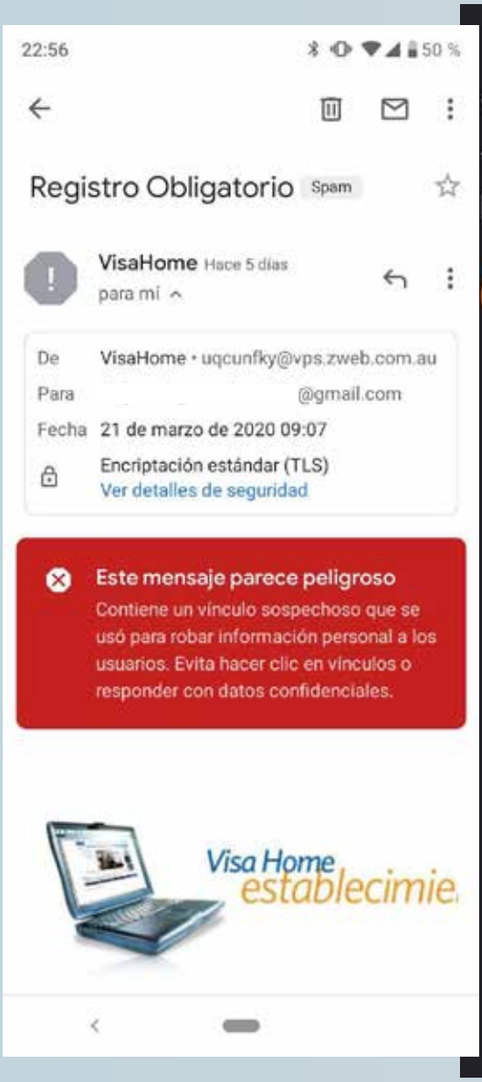
Para evitar el acceso bloqueado para siempre. Haga clic a continuación para verificar su cuenta de identidad.

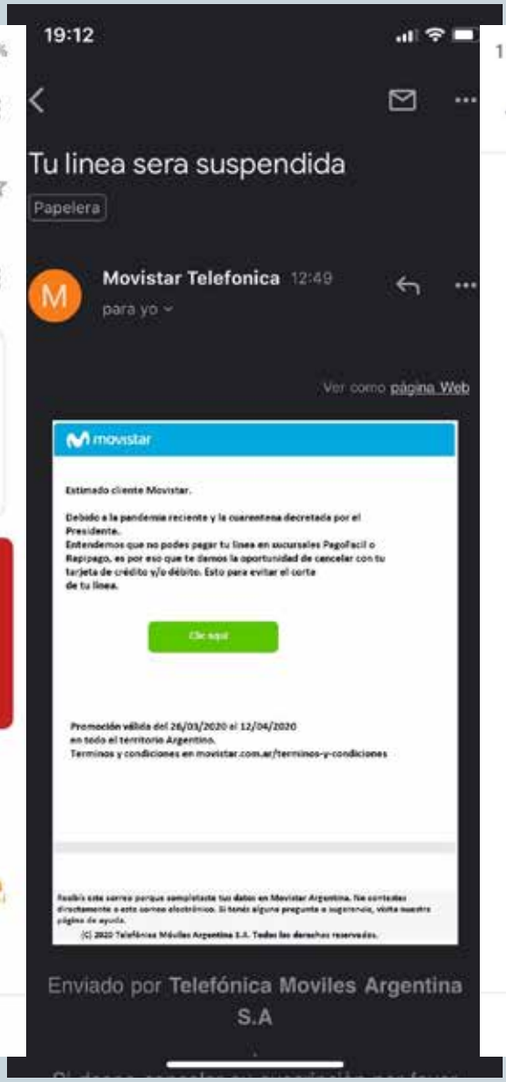
Verificar tu ID de Apple

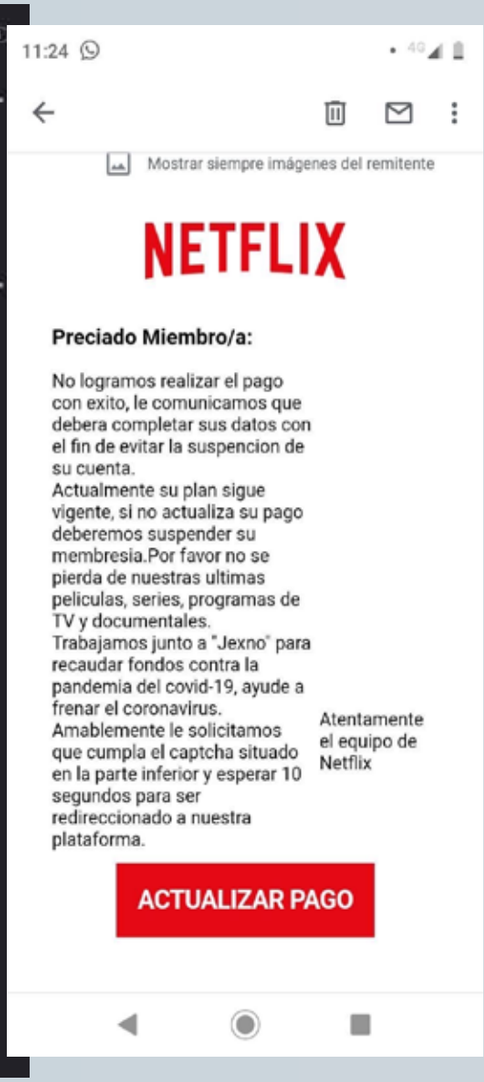
Por lo tanto, por su seguridad, le pedimos que cierre sesión de inmediato. Para evitar el acceso es manejado por alguien que no sea usted.

Atentamente,

Atención al Cliente ID de Apple.


22:56
50 %
Registro Obligatorio
Spam
VisaHome Hace 5 días
para mí
De VisaHome • uqcunfky@vps.zweb.com.au
Para @gmail.com
Fecha 21 de marzo de 2020 09:07
Encriptación estándar (TLS)
Ver detalles de seguridad
Este mensaje parece peligroso
Contiene un vínculo sospechoso que se usó para robar información personal a los usuarios. Evita hacer clic en vínculos o responder con datos confidenciales.
Visa Home
establecimie


19:12
Tu linea sera suspendida
Papelera
Movistar Telefonica 12:49
para yo
Ver como página Web
movistar
Estimado cliente Movistar.
Debido a la pandemia reciente y la cuarentena decretada por el Presidente.
Entendemos que no podes pagar tu linea en sucursales PagoFacil o Rapipago, es por eso que te damos la oportunidad de cancelar con tu tarjeta de crédito y/o débito. Esto para evitar el corte de tu linea.
Clic aqui
Promoción válida del 26/03/2020 al 12/04/2020 en todo el territorio Argentino.
Terminos y condiciones en movistar.com.ar/terminos-y-condiciones
(C) 2020 Telefónica Móviles Argentina S.A. Todos los derechos reservados.
Enviado por Telefónica Moviles Argentina S.A


11:24
Mostrar siempre imágenes del remitente
NETFLIX
Preciado Miembro/a:
No logramos realizar el pago con exito, le comunicamos que debera completar sus datos con el fin de evitar la suspencion de su cuenta.
Actualmente su plan sigue vigente, si no actualiza su pago deberemos suspender su membresia.Por favor no se pierda de nuestras ultimas peliculas, series, programas de TV y documentales.
Trabajamos junto a "Jexno" para recaudar fondos contra la pandemia del covid-19, ayude a frenar el coronavirus.
Amablemente le solicitamos que cumpla el captcha situado en la parte inferior y esperar 10 segundos para ser redireccionado a nuestra plataforma.
Atentamente el equipo de Netflix
ACTUALIZAR PAGO


Apple.com Notificación - "Información importante sobre las cuentas de Apple.com a las que se ha accedido ilegalmente" Nueva información: El bloqueo se ha aplicado siempre que COVID-19 siga activo 25/03/2020
Tenha cuidado. Esta mensagem parece ser uma tentativa de phishing. Saiba mais sobre phishing | Mostrar conteúdo bloqueado
AI
Apple ID.
Qua, 25/03/2020 17:46 Exibir mais
pdf
importante.#32a1a738974fb8ad...
PDF - 446 bytes


Text Message
Saturday 13:42
Due to the COVID-19 outbreak we will give out free iPhone 11 smartphones to keep you entertained. adrienne, visit appie6.info/NZluodentb

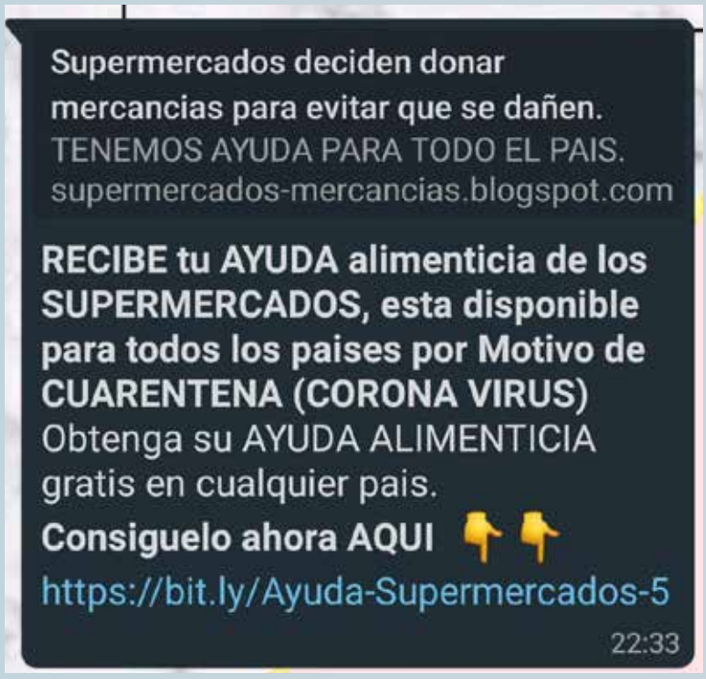
Eyes here! You can Stop CORONA VIRUS now!

anteayer, 00:10

Hey!

Military Source Exposes Shocking TRUTH
About This Deadly Pandemic And The "1
Thing"
You Must Do Before It's TOO LATE

http://pandemicsurvival.website

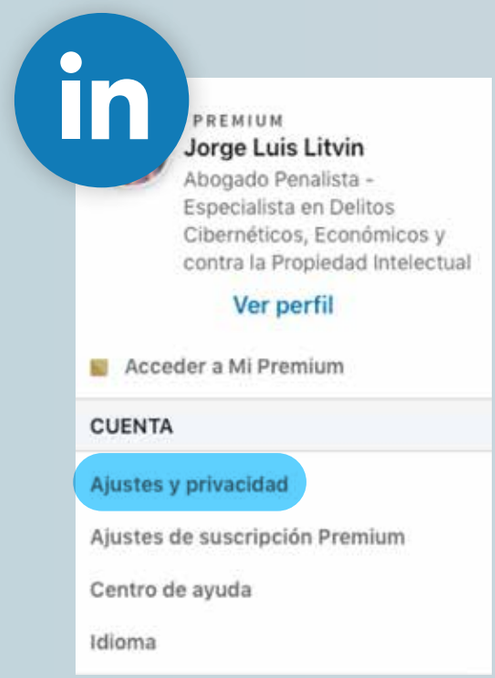


III

Tutorial para configurar la verificación en dos pasos

Autenticación en dos pasos

Autenticación en dos pasos



Verificación en dos pasos

Cuenta → Seguridad → Autenticación en dos fases

Acceso y Seguridad

Si estás leyendo estas palabras es porque la lectura de esta obra está finalizada.

Quizás llegaste hasta acá porque ya eras mi lector, o, quizás este libro sea nuestra presentación.

Ta vez llegaste hasta acá porque sos abogado o informático, o justamente por no ser ninguno de ambos.

Que hayas leído por completo el texto de este humilde autor puede deberse a que el cibercrimen tu curiosidad despertó, ¿o fue acaso tu preocupación? Hasta me animo a pensar que leer sobre cibercrimen en rimas te divirtió.

Puede que ya sepas todo lo que se escribió, o puede que de este texto te lleves algún concepto, consejo o recomendación.

Sea como sea, yo te agradezco de corazón, por llegar hasta acá, mi querido lector.

Decidí que este libro -al menos por este medio y en su primera edición- sea gratuito para vos, y también quiero que sepas que en la portada y en la contratapa tenés mis canales de contacto a tu disposición.

A cambio sólo te voy a pedir un favor: distribuyámoslo.
Reenvíalo a tus amistades, pareja o familiares, porque ellos también pueden ser víctimas de todos estos males.

La concientización empieza en algún lado, pero pretende llegar a todas partes.

Que el único virus que distribuyamos sea el de cuidarnos entre pares. Sumate.

Abrazo grande.

Tras años de trabajo, estudio e investigación en derecho penal y tecnología “Hackeados” se publica.

Un texto que a diferencia del resto de los escritos por abogados, no está dirigido a otros abogados, sino al resto de los ciudadanos.

En un lenguaje accesible, desprovisto de tecnicismos y con tintes humorísticos, el autor expone cuáles son algunos de los peligros a los que nos enfrentamos día a día en el universo 2.0. Incluye un capítulo específico con decenas de consejos y recomendaciones esenciales de ciberseguridad para prevenir ser víctimas de un delito en nuestro hogar.

Luego de advertir y concientizar, el último fragmento del libro incorpora una guía que responde a las preguntas “¿qué, cómo y dónde denunciar?”, cuáles son los tipos penales previstos por la legislación argentina actual, un anexo con ejemplos de casos reales y habituales de intentos de estafas virtuales y un tutorial paso a paso para protegernos de hackeos en nuestras redes sociales.

Más que un libro, Hackeados es una guía de concientización y prevención del ciberdelito.

Contacto (clickeá):

- ✉
-
-
- in

HACKEADOS

JORGE LUIS **LITVIN**