Nuevos tipos de ataque:

- Fraude al CEO
- Sextorsión
- Warranty Exploitation

¿Realmente estás protegido?

0. Introducción 3

1. Fraude del CEO 3

2. Sextorsión 13

3. Warranty Exploitation 29

4. Ejemplos reales 42

0 Introducción

0. Introducción

Sobre Mario Díaz:

- Más de 15 años de experiencia en seguridad
- He trabajado para:

isec auditors S21 SEC indra SECURITY

- Ahora trabajo en:

0. Introducción

By Victim Count

Crime Type	Victims	Crime Type	Victims
Non-Payment/Non-Delivery	65,116	Other	10,826
Extortion	51,146	Lottery/Sweepstakes	7,146
Personal Data Breach	50,642	Misrepresentation	5,959
No Lead Value	36,935	Investment	3,693
Phishing/Vishing/Smishing/Pharming	26,379	Malware/Scareware/Virus	2,811
BEC/EAC	20,373	Corporate Data Breach	2,488
Confidence Fraud/Romance	18,493	IPR/Copyright and Counterfeit	2,249
Harassment/Threats of Violence	18,415	Denial of Service/TDoS	1,799
Advanced Fee	16,362	Ransomware	1,493
Identity Theft	16,128	Crimes Against Children	1,394
Spoofing	15,569	Re-shipping	907
Overpayment	15,512	Civil Matter	768
Credit Card Fraud	15,210	Charity	493
Employment	14,979	Health Care Related	337
Tech Support	14,408	Gambling	181
Real Estate/Rental	11,300	Terrorism	120
Government Impersonation	10,978	Hacktivist	77

0. Introducción

By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,297,993,709	Tech Support	$30,697,026
Confidence Fraud/Romance	$362,500,761	Harassment/Threats of Violence	$21,903,029
Investment	$252,955,320	Misrepresentation	$20,000,713
Non Payment/Non Delivery	$183,826,809	IPR/Copyright and Counterfeit	$15,802,011
Real Estate/Rental	$149,630,114	Civil Matter	$15,177,982
Personal Data Breach	$148,892,405	Malware/Scareware/Virus	$2,411,601
Corporate Data Breach	$117,711,989	Health Care Related	$1,474,792
Identity Theft	$100,129,091	Ransomware	*$3,621,037
Advanced Fee	$92,271,682	Denial of Service/TDos	$2,052,340
Credit Card Fraud	$88,991,436	Re Shipping	$1,684,179
Extortion	$83,357,901	Charity	$1,006,379
Spoofing	$70,000,240	Gambling	$920,930
Government Impersonation	$61,211,765	Crimes Against Children	$265,956
Other	$63,125,929	Hacktivist	$77,612
Lottery/Sweepstakes	$60,214,826	Terrorism	$10,193
Overpayment	$53,225,507	No Lead Value	$0.00
Phishing/Vishing/Smishing/Pharming	$40,241,740		
Employment	$45,202,120		

1

Fraude del CEO

Ha arruinado las carreras de muchos ejecutivos y empleados leales.

CEOs ejemplares han sido despedidos
Los precios de las acciones de las compañías han caído en picado.

Empresas de fusiones y adquisiciones han sido eliminadas de la mesa de negociación.
El FBI ha reportado que este tipo de fraude ha afectado a más de 22000 organizaciones con unas pérdidas de más de 3 billones..

1. Fraude del CEO

En primer lugar hablaremos de como funciona este tipo de fraude, de como las empresas y los empleados son engañados y las empresas comprometidas.

Ampliamente se ha hablado en las noticias del fraude/phising del CEO, en el cual unos atacantes se hacen pasar por el CEO de la organización y contactan con el personal responsable de ventas/cobros para realizar importantes transferencias de dinero en efectivos a bancos en países remotos en el extranjero.

A continuación se muestran los tipos de organizaciones que podrían verse afectadas:

1. **Grandes empresas que trabajan con proveedores externos**
2. **Empresas que realizan y/o reciben un elevado número de transferencias bancarias**
3. **Suplantación de un letrado/ejecutivo de la compañía trabajando con datos confidenciales (nóminas, etc).**

1. Fraude del CEO

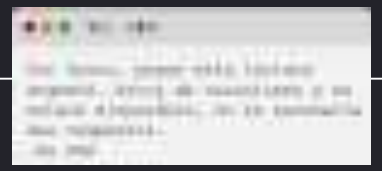
INICIO

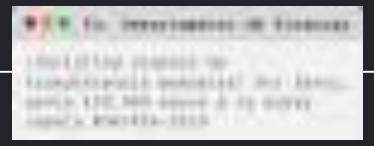
El atacante consulta si se puede suplantar el dominio y hacerse pasar por el CEO u otros miembros relevantes.

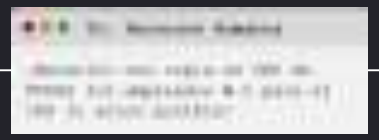
Los atacantes suelen extraer información durante meses hasta poder realizar un ataque de forma satisfactoria.

ANZUELO

Se mandan emails phishing a empleados de alto riesgo.

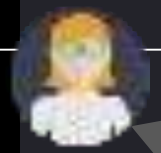




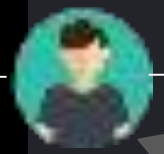


RESPUESTA

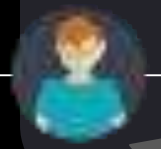
El empleado objetivo recibe dichos emails y actúa sin reflexionar o sin cuestionarse el origen de la petición.



¡Es el CEO, yo me encargaré de esto por él!



¡Será mejor que realice este pago a la nueva cuenta!



Suena importante. ¡Enviaré esto ahora mismo!

IMPACTO

La ingeniería social ha sido todo un éxito y el atacante ha conseguido su objetivo.

Esto causa transacciones bancarias y pérdidas masivas de datos.

RESULTADO

Las consecuencias de un ataque satisfactorio pueden ser altamente dañinas tanto para los empleados como para la compañía.

Posible impacto:

- El dinero tan sólo se recupera en un 4% de los casos.
- CEO despedido.
- CFO despedido.
- Se realizan denuncias.
- Intangibles – pérdida de reputación, de confianza, etc.

1. Fraude del CEO

1. Fraude del CEO

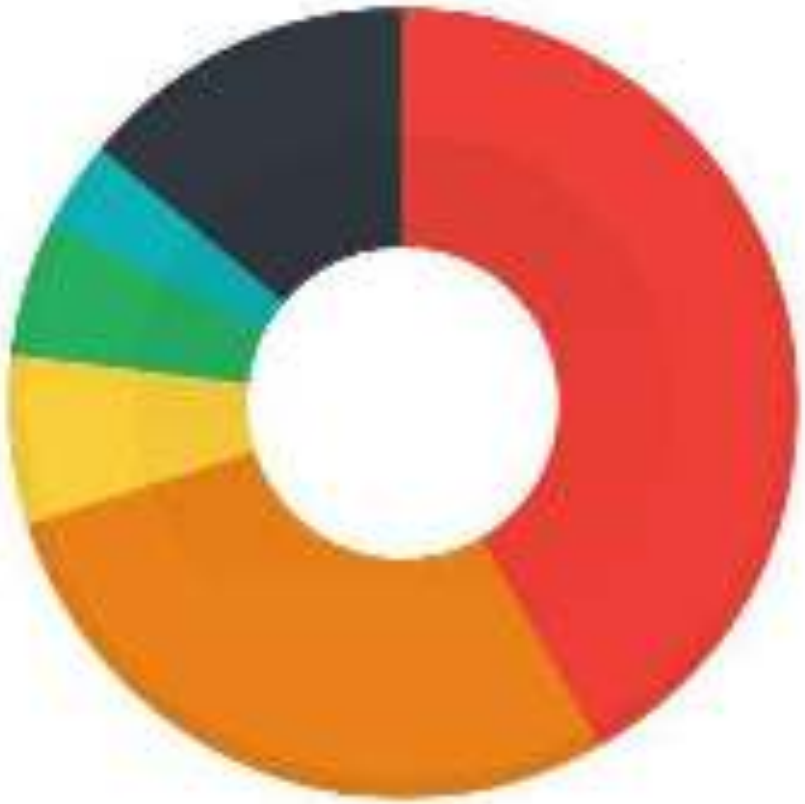
VÍCTIMAS

- Chief Executive Officer (CEO)
- Managing Director/Director
- President
- General Manager/Manager
- Chairman
- Others

TARGETS

- Chief Financial Officer (CFO)
- Director of Finance
- Finance Manager
- Finance Controller
- Accountant
- Others

1. Fraude del CEO



Chief Executive Officer (CEO)	41.83%
Managing Director/Director	28.29%
President	6.88%
General Manager/Manager	5.68%
Chairman	3.52%
Others	13.80%

VÍCTIMAS

Figure 2: Distribution of spoofed positions by BEC

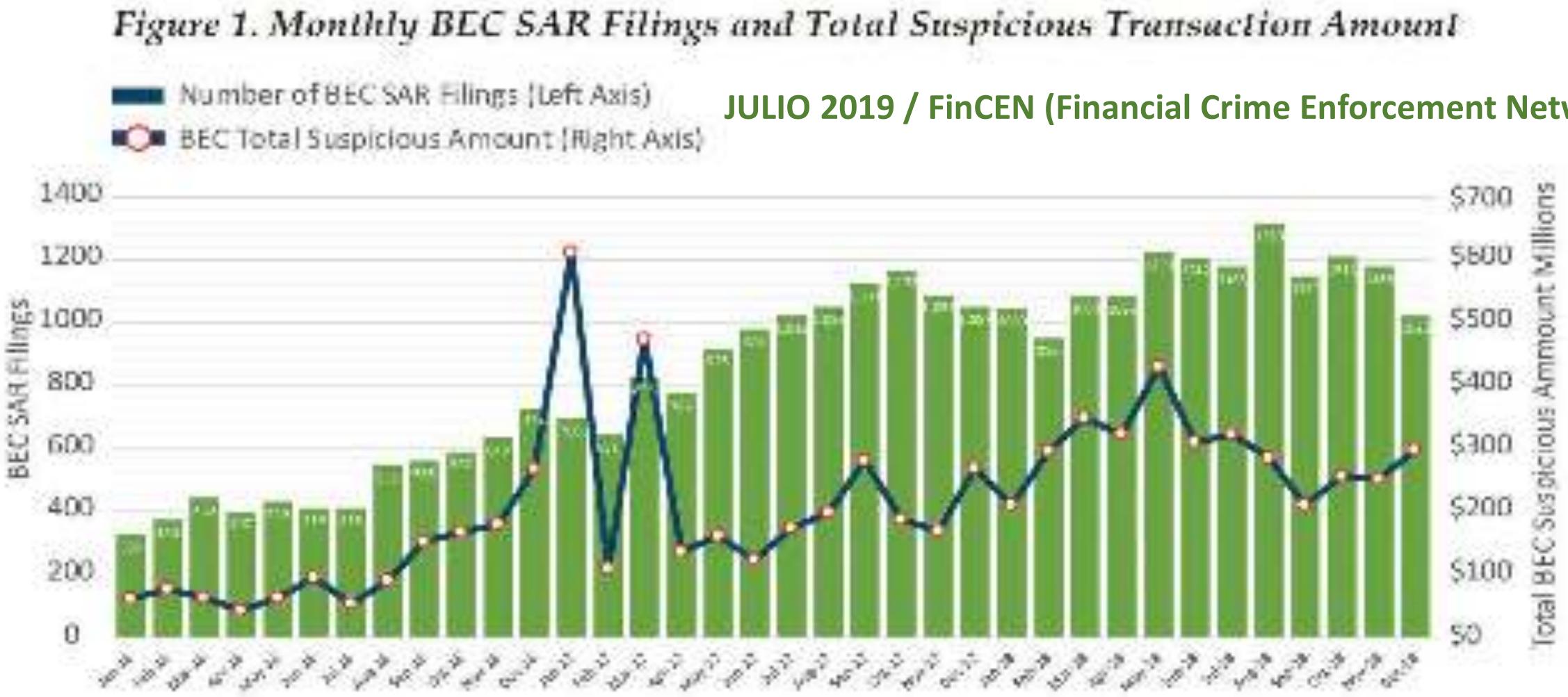
1. Fraude del CEO

Chief Financial Officer (CFO)	18.89%
Director of Finance	7.45%
Finance Manager	6.37%
Finance Controller	6.26%
Accountant	4.01%
Others	57.02%

TARGETS

Figure 1: Distribution of target positions by BEC

1. Fraude del CEO

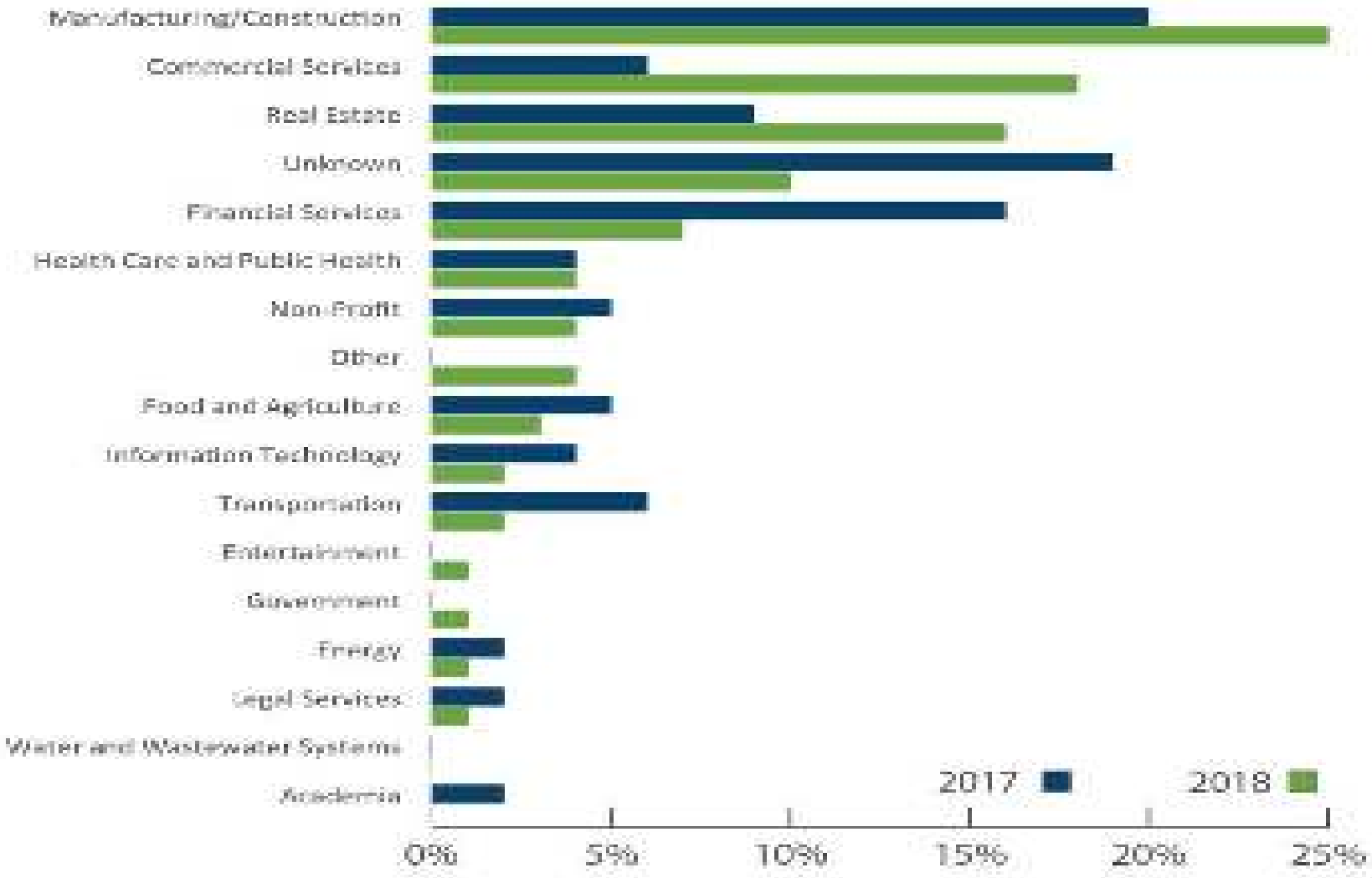


JULIO 2019 / FinCEN (Financial Crime Enforcement Network)

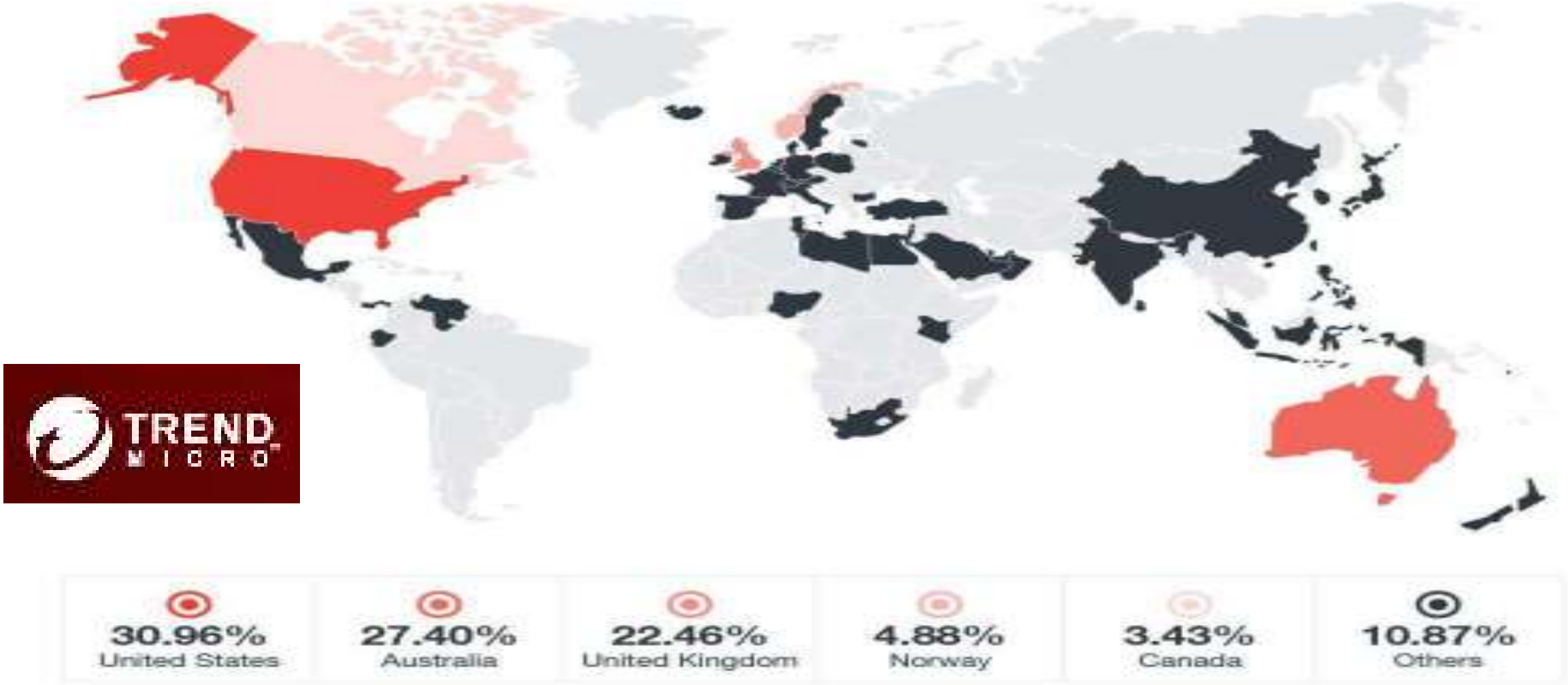
1. Fraude del CEO

JULIO 2019 / FinCEN (Financial Crime Enforcement Network)

Figure 2. 2017 and 2018 BEC Targets by Industry



1. Fraude del CEO



1. Fraude del CEO

NCN | ISACA

Eres target?

"No puedes hacer 500 millones de amigos sin hacer unos cuantos enemigos"

"The Social Network"

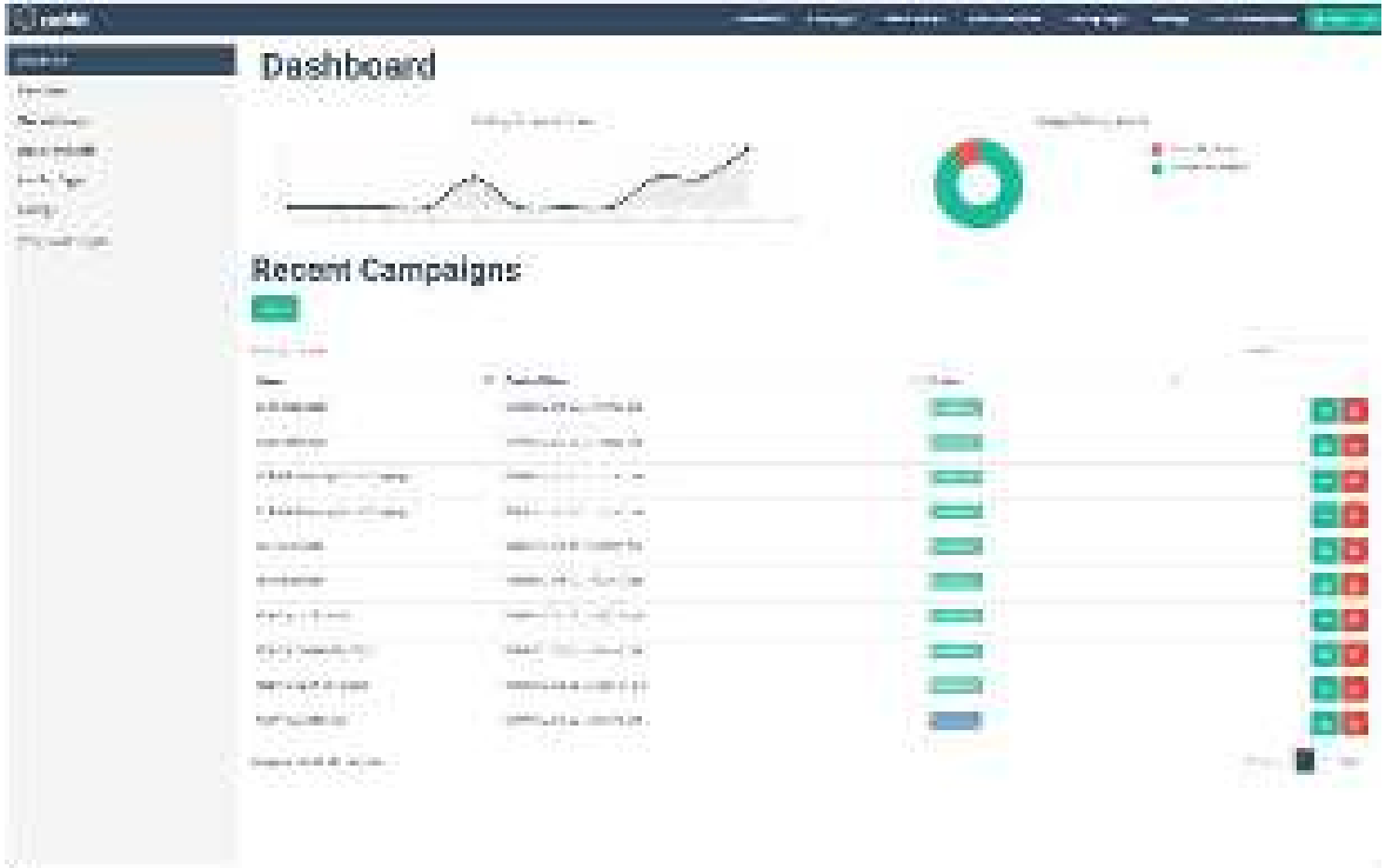
1. Fraude del CEO

NCN | ISACA

Brechas de seguridad en 2019:

- *Capital One: 106,000,000 Registros*
- *Facebook: 540,000,000 Registros.*
- *Zynga: 218,000,000 Registros.*
- *Canva: 140,000,000 Registros.*
- *Westpac: 98,000 Registros*
- *Amazon Japón: <Indeterminado>*

1. Fraude del CEO



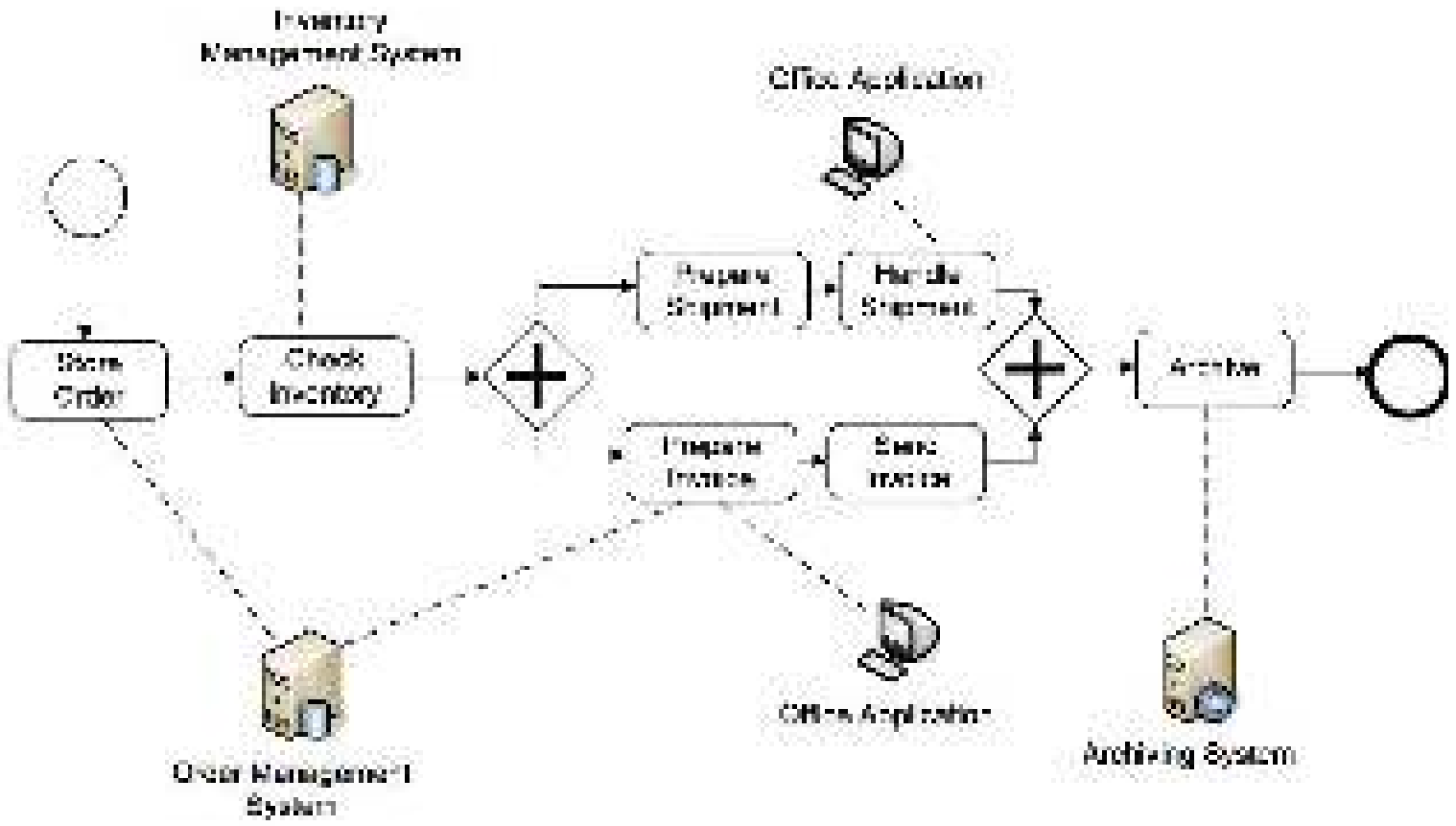
1. Fraude del CEO

1. Fraude del CEO

NCN | ISACA

PAYMENT WORKFLOW:

- *En el proceso de la línea de verificación suele haber una persona designada para agilizar el cobro de facturas.*
- *Los atacantes utilizan el nombre de una persona o de un departamento y envían mails a otra de otro departamento pidiendo información sobre una TRANSACCIÓN o PROCEDIMIENTO.*
- *Si consiguen recibir respuesta esta viene con documentos adjuntos que los utilizan para seguir pidiendo información.*
- *El atacante se hace un experto en PROCEDIMIENTOS y WORKFLOWS.*

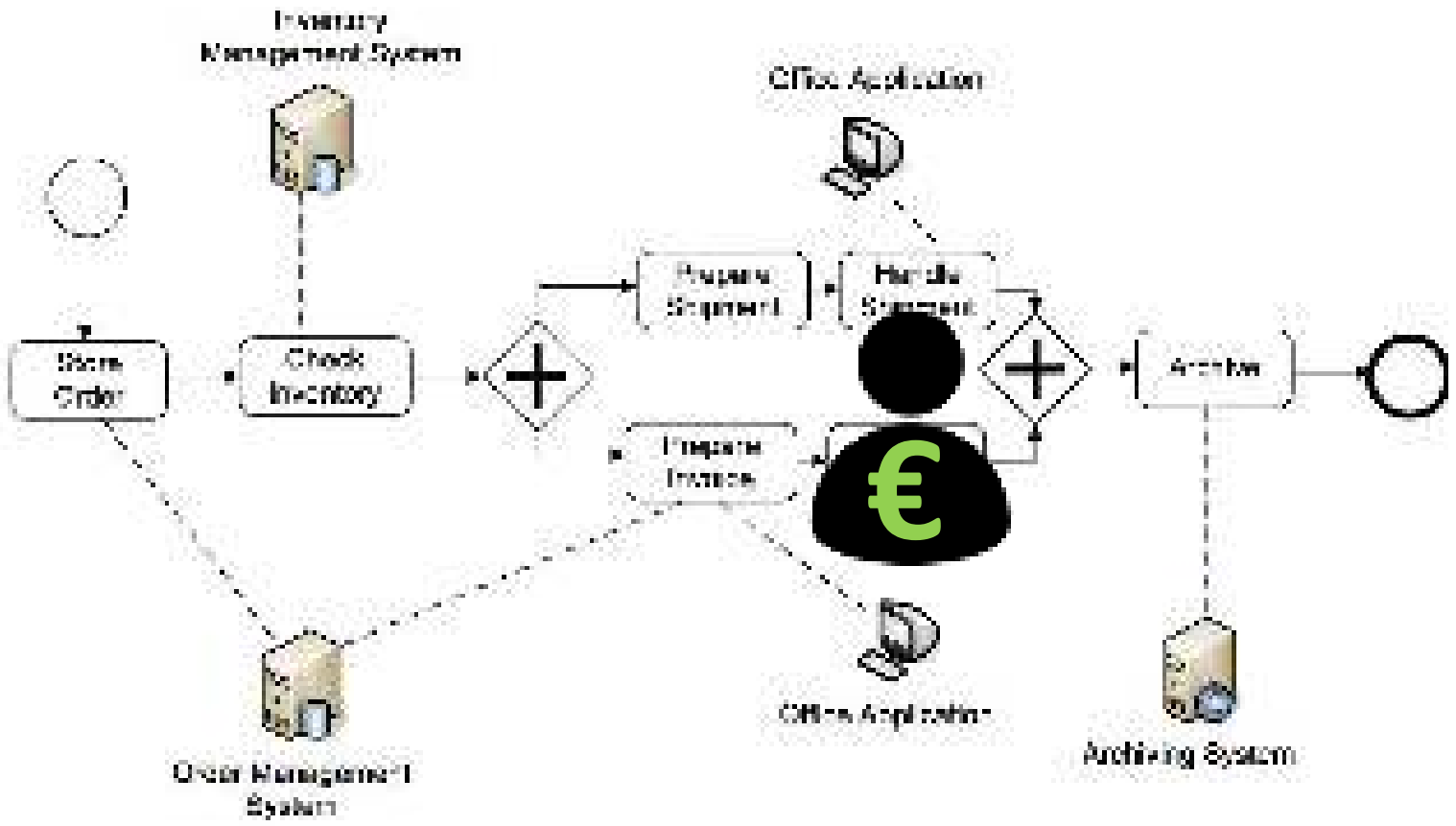


1. Fraude del CEO

NCN | ISACA

PAYMENT WORKFLOW:

- *En el proceso de la línea de verificación suele haber una persona designada para agilizar el cobro de facturas.*
- *Los atacantes utilizan el nombre de una persona o de un departamento y envían mails a otra de otro departamento pidiendo información sobre una TRANSACCIÓN o PROCEDIMIENTO.*
- *Si consiguen recibir respuesta esta viene con documentos adjuntos que los utilizan para seguir pidiendo información.*
- *El atacante se hace un experto en PROCEDIMIENTOS y WORKFLOWS.*



1. Fraude del CEO

1 Fraude del proveedor

El fraude del proveedor externo es uno de los fraudes más fáciles de ejecutar siguiendo el procedimiento explicado anteriormente:

- En primer lugar se consigue la lista de proveedores de la empresa atacada y las personas de contacto en el departamento de facturación / compras.
- Haciendose pasar por el proveedor se envía / modifica una factura cambiando el número de cuenta bancaria asociada al pago.

2 Fraude de las nóminas

El fraude de las nóminas es también uno de los más fáciles de ejecutar.

El atacante se hace pasar por el CEO y pide una lista de las tres últimas nóminas de los trabajadores y del número de cuenta donde se ingresa esta nómina.

Se contacta con una empresa de tarjetas de crédito y se solicita una tarjeta de crédito a nombre de cada trabajador (solamente se necesita un recibo, la nómina y el número de cuenta de donde la tarjeta procesará el pago a final de mes).

Por qué estos ataques tienen tanto éxito?

- Muchos esfuerzos para mitigar el riesgo se centran en la tecnología. Los antivirus, el IPS, el antispam, etc. Sin embargo toda esta tecnología tiene que estar bien protegida por lo que se llama el "Firewall Humano", las personas que trabajan en la organización.
- Unos empleados bien concienciados pueden marcar la diferencia entre ser comprometidos y no.
- Aunque el perímetro se encuentre bien defendido los atacantes siempre encontrarán una forma de traspasarlo y los empleados son el eslavón más débil de la cadena.

1. Fraude del CEO

3 Fraude del CFO / CEO / COO

El atacante se hace pasar por el CEO o un ejecutivo de alto nivel y envía ordines de pago/transferencias a personas responsables de compras, CFO, COO, etc:

- Se necesita obtener información mediante ingeniería social sobre como funcionan los métodos de pago/cobro y quienes son las personas responsables de ejecutar dichos pagos.
- En algunas ocasiones estas órdenes de pago se envían directamente a la gestoría contratada por la empresa o al director del banco directamente desde la cuenta del CEO.

4 Fraude del abogado falso

El atacante se hace pasar por un abogado que representa a una de las grandes firmas de auditoria emitiendo información falsa (membrete, sello, etc) y comunicando que el tema que tiene entre manos es algo confidencial y secreto reclamando la máxima urgencia para realizar una transferencia de dinero.

Por qué estos ataques tienen tanto éxito?

- Muchos esfuerzos para mitigar el riesgo se centran en la tecnología. Los antivirus, el IPS, el antispam, etc. Sin embargo toda esta tecnología tiene que estar bien protegida por lo que se llama el "Firewall Humano", las personas que trabajan en la organización.
- Unos empleados bien concienciados pueden marcar la diferencia entre ser comprometidos y no.
- Aunque el perímetro se encuentre bien defendido los atacantes siempre encontrarán una forma de traspasarlo y los empleados son el eslavón más débil de la cadena.

1

Fraude del CEO: Medidas de protección

1. Fraude del CEO: Medidas de protección

1 Identificar a los usuarios de alto riesgo

Los usuarios de alto riesgo incluyen ejecutivos, personal de recursos humanos, contabilidad y IT. Se deberían imponer más controles y salvaguardas en estas áreas. Por ejemplo, en las aprobaciones financieras para transferencias bancarias, estipule varios puntos de autorización y un período de tiempo que debe transcurrir antes de que se ejecute la transferencia.

Es aconsejable realizar una búsqueda de todos los usuarios de alto riesgo para ver qué tan expuestos están. Por ejemplo, los perfiles de LinkedIn y Facebook a menudo proporcionan información personal detallada o incluso lo que podría considerarse datos corporativos confidenciales, como la persona que tiene la autoridad de transferencia bancaria, así como las direcciones de correo electrónico y la lista de conexiones.

2 Establecer controles técnicos

Deben instituirse varios controles técnicos para evitar el éxito de los ataques de phishing. El filtrado de correo electrónico es el primer nivel pero está lejos de ser infalible. Se deben intensificar las medidas de autenticación. En lugar de un simple nombre de usuario y contraseña, donde existe una buena tasa de éxito, utilizar doble factor de autenticación (algo que tienes y algo que sabes). Esto hace mucho más difícil para los intrusos potenciales obtener acceso y robar los datos personales o la identidad de esa persona. Un llavero, tarjetas de acceso y el envío de un código a un teléfono móvil registrado son algunos de los métodos posibles.

La aplicación automatizada de la política de contraseña e ID de usuario es otra defensa inteligente. Acceso integral y La administración de contraseñas también puede minimizar los brotes de malware y ransomware. Revisar las técnicas existentes controles y tome medidas para tapar cualquier espacio.

1. Fraude del CEO: Medidas de protección

3 Políticas de transferencias electrónicas

Además de las políticas estándar también debe existir una política sobre transferencias electrónicas y el manejo de información confidencial. ***Nunca debería ser possible para un cibercriminal secuestrar una cuenta de correo electrónico corporativo y convencer a alguien de que transfiera una gran suma de inmediato.***

La política debe limitar tales transacciones a cantidades relativamente pequeñas. Cualquier cosa que supere ese umbral establecido debe debe requerir más autorizaciones. *Esto también aplica a la información confidencial como las nóminas donde debe haber una cadena de aprobaciones antes de liberar la información.*

Cada organización debe establecer una política de seguridad, revisarla regularmente para detectar lagunas, publicarla y asegurarse de que los empleados la siguen. Esta política debe incluir cosas como por ejemplo que los usuarios no abran ficheros adjuntos o hagan click en enlaces de una fuente desconocida, no usen unidades de USB en los ordenadores de la oficina, utilzar una buena política de contraseñas (no reutilizarlas ni utilizar post-its en la pantalla), establecer políticas para la wifi, sobretodo para los empleados externos a la organización y los socios de la misma.

4 Procedimientos para transferencias electrónicas

Además de las políticas hay que establecer procedimientos para prevenir contra el fraude del CEO. La autorización para realizer transferencias bancarías es algo que se debe mirar con lupa. ***Se recomienda configurar a nivel bancario que cualquier transferencia bancaria incluya más de una autorizacion antes de realizarla, así como una confirmación extra además del correo electrónico. Por ejemplo puede utilizarse el teléfono como segundo canal de confirmación pero es preferible el cara a cara.***

De esta manera se frustra un ataque de correo electrónico fraudulento siempre y cuando la confirmación se realice por un canal secundario a este. Si es por teléfono, siempre se utiliza un teléfono específico acordado previamente y nunca uno proporcionado por correo electrónico.

2

Sextorsión

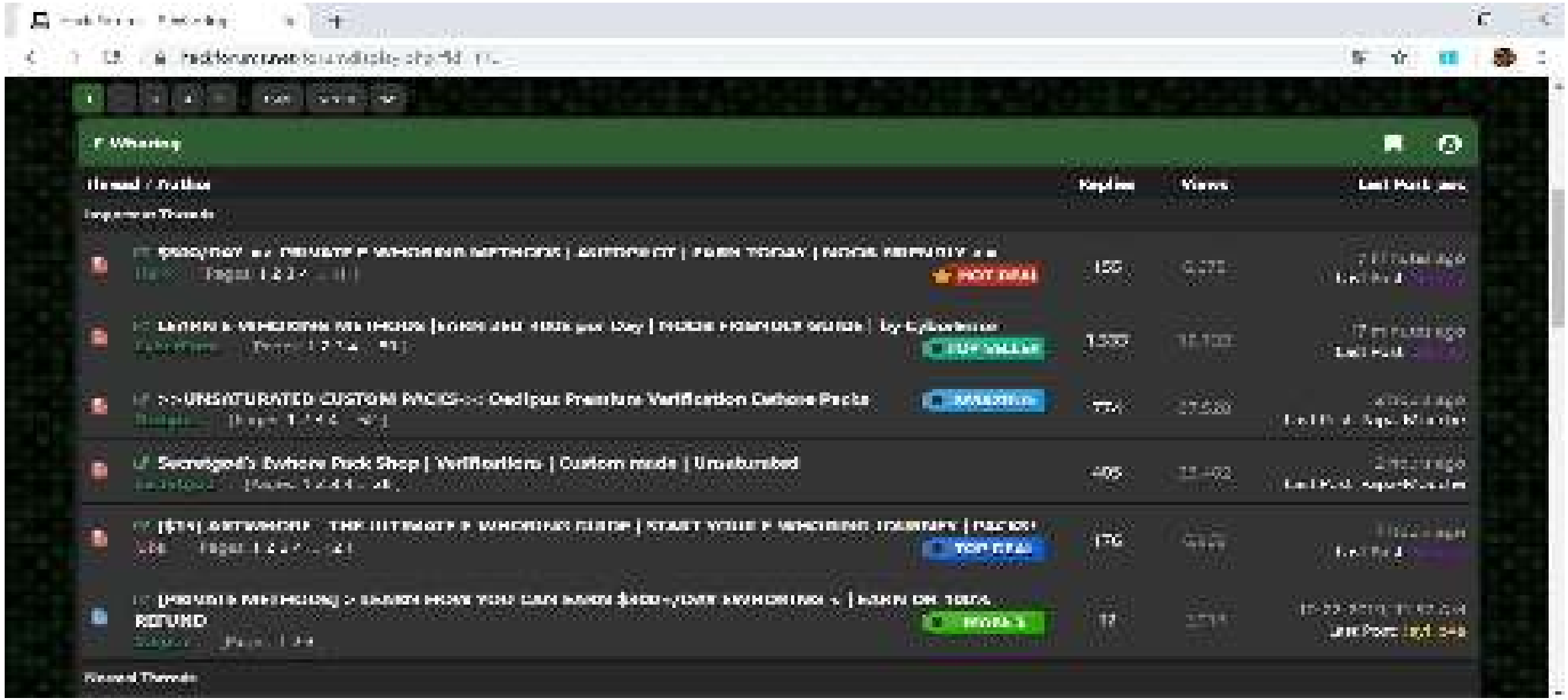
Ligar es más fácil que nunca con las nuevas tecnologías y aplicaciones disponibles en el mercado móvil.

Si no se utiliza Tinder, se utiliza POF, Adopta o alguna de las redes alternativas que hay.

Pero tener empleados con ganas de tener sexo puede suponer un problemas para las empresas, como veremos a continuación.

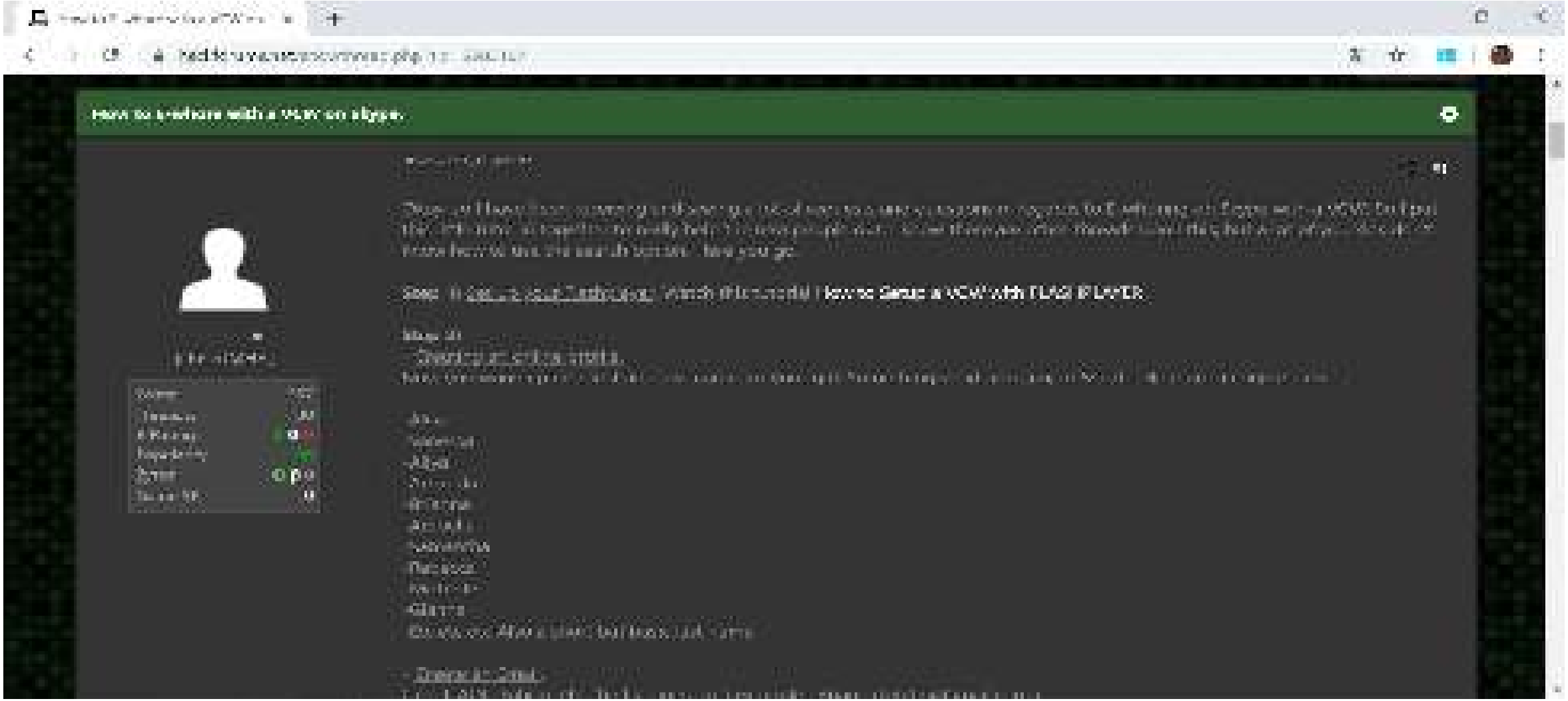
2. Sextorsión

2. Sextorsión

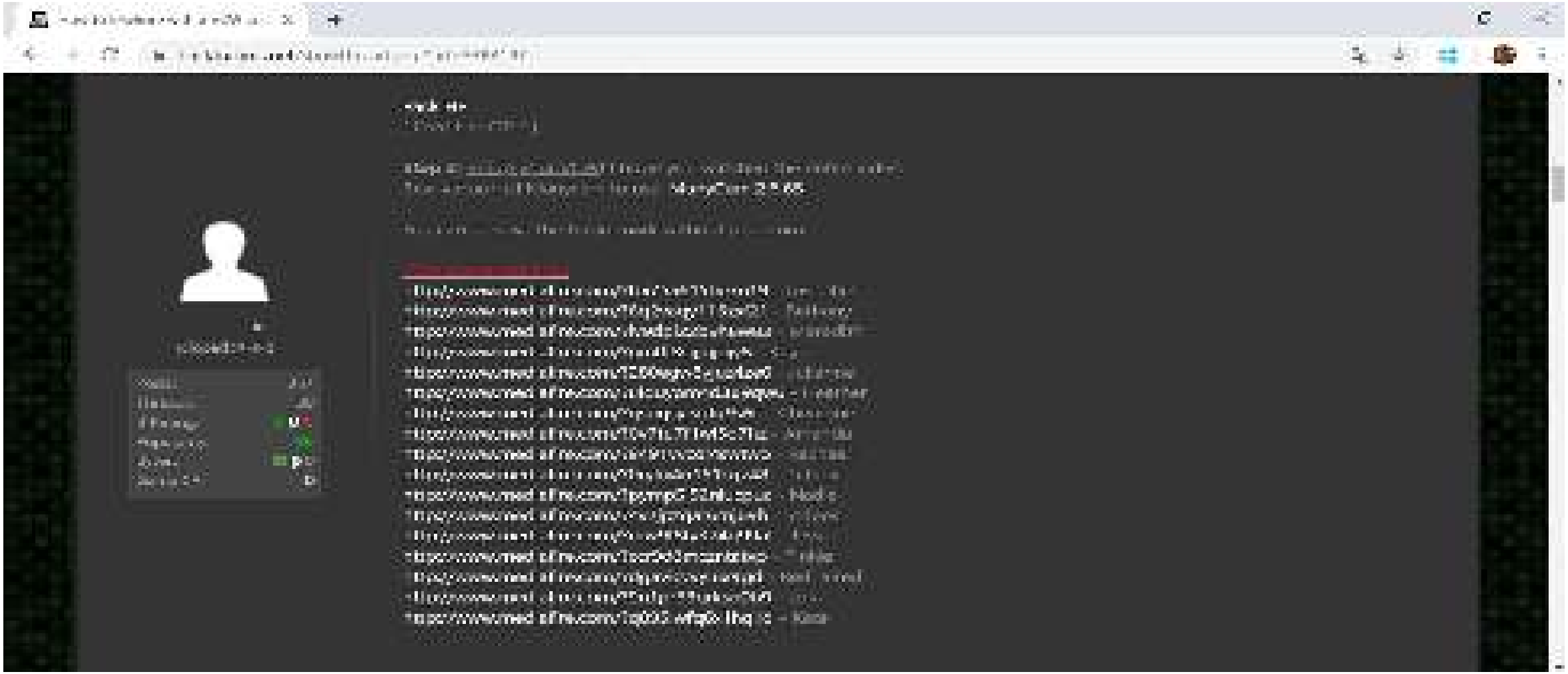


2. Sextorsión

2. Sextorsión



2. Sextorsión

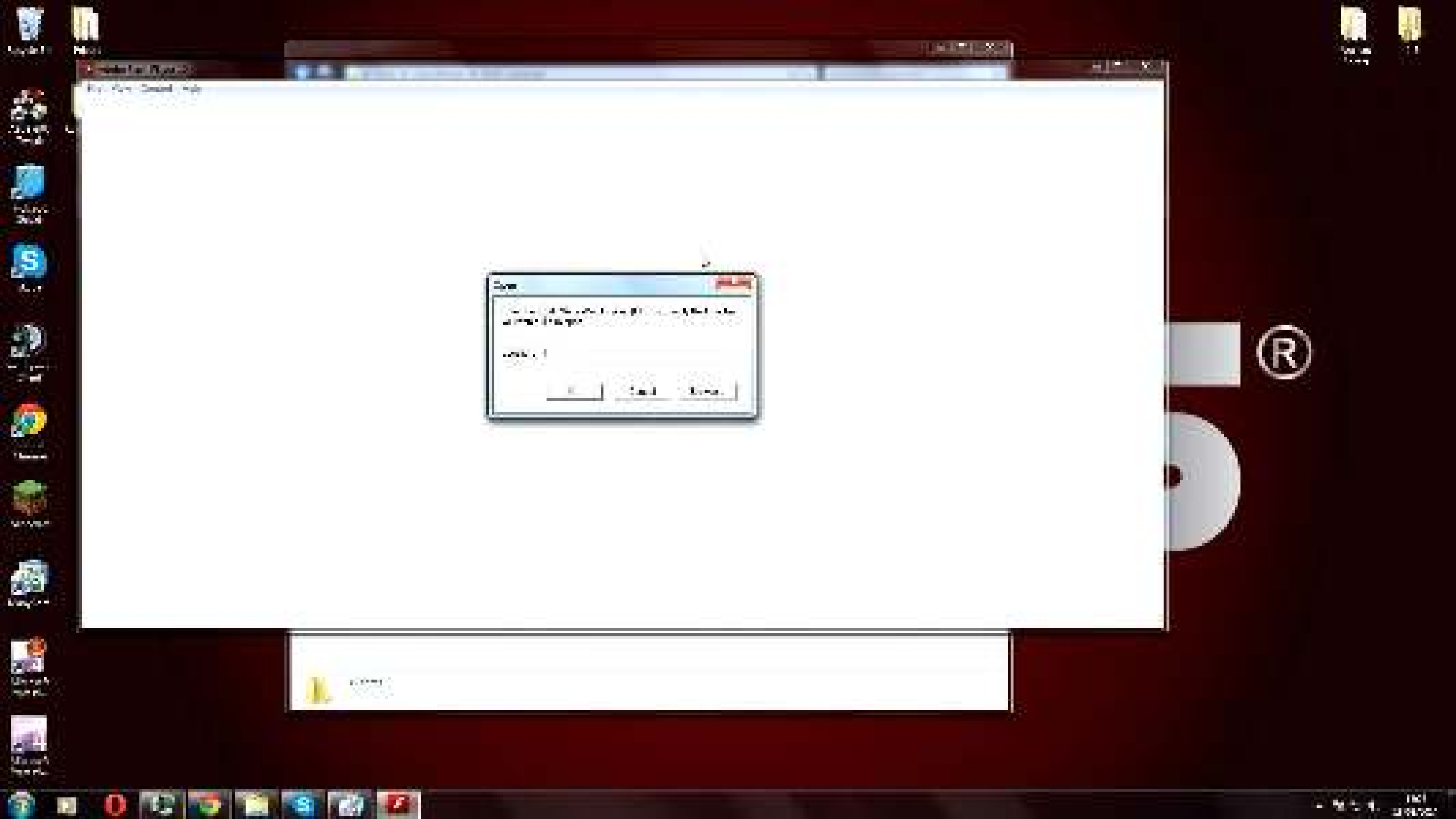


2. Sextorsión

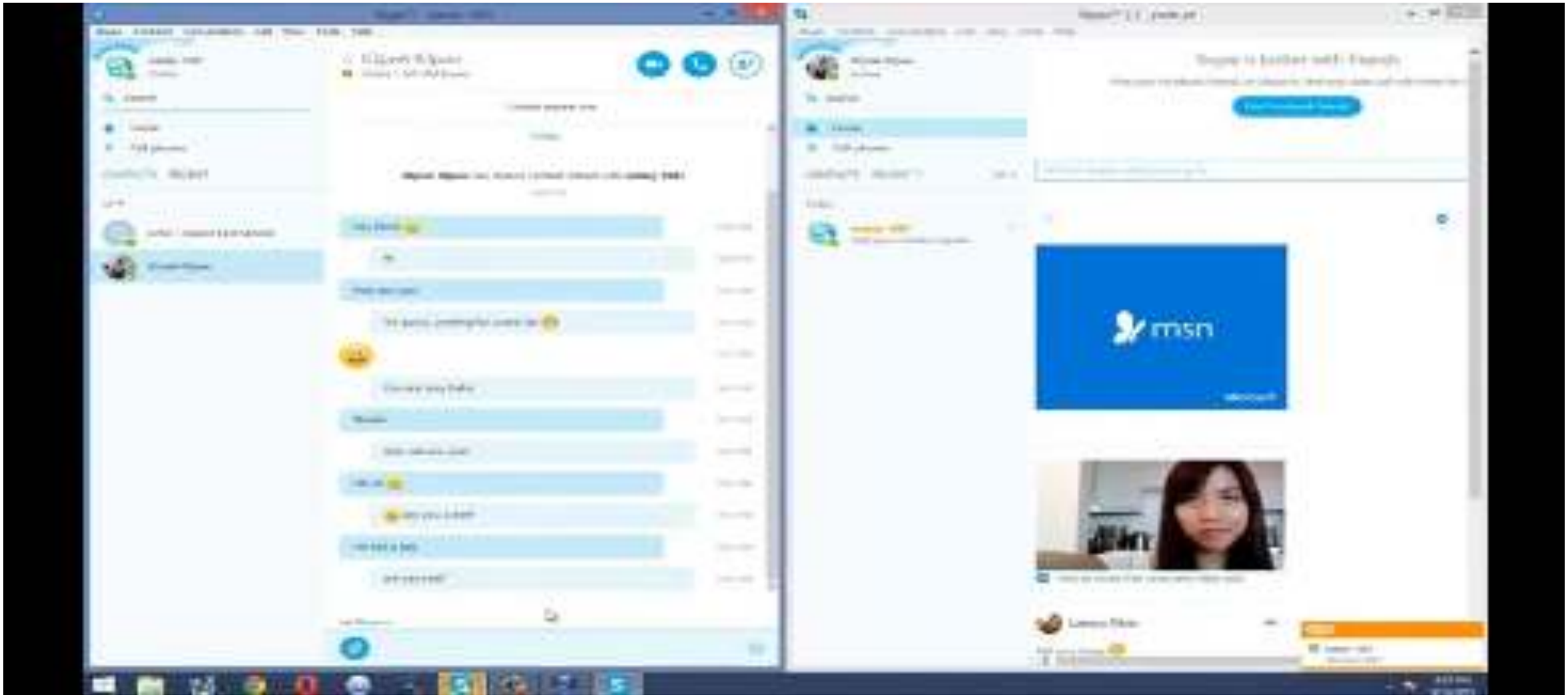
2. Sextorsión

BlueStacks es un emulador para Android que nos permite tener las aplicaciones del móvil en nuestro ordenador y de esta forma agilizar los procedimientos de Sextorsión. En el emulador podemos instalar las redes sociales AdoptaUnTio, POF, Tinder ,etc.

2. Sextorsión



2. Sextorsión



2

Sextorsión: Medidas de protección

Se recomienda…

1 **Hay que tener en cuenta la seguridad tanto dentro como fuera de la oficina.**

2 **En ningún momento hay que ceder ante un chantaje.**

3 **Conocer que están haciendo los atacantes nos permite defendernos de los mismos.**

3 Warranty Exploitation

--

3. Warranty Exploitation

3. Warranty Exploitation

NCN | ISACA

WARRANTY EXPLOITATION

Se basa en explotar grandes compañías para recibir productos de manera gratuita sin pagar por ellos.

Cuando los consiguen los venden obteniendo grandes beneficios que se traducen en pérdidas pequeñas para las compañías dado su gran tamaño.

3. Warranty Exploitation

Serial Number

3. Warranty Exploitation

3. Warranty Exploitation

3. Warranty Exploitation

NCN | ISACA

WARRANTY EXPLOITATION

Se basa en explotar grandes compañías para recibir productos de manera gratuita sin pagar por ellos.

Cuando los consiguen los venden obteniendo grandes beneficios que se traducen en pérdidas pequeñas para las compañías dado su gran tamaño.

3. Warranty Exploitation

3. Warranty Exploitation

3. Warranty Exploitation

3. Warranty Exploitation

3

Warranty Exploitation: Medidas de protección

Se recomienda…

1 **Comprobar la generación de los números de serie de los productos.**

2 **Realizar una mejor comprobación de las facturas y comprobantes de pago.**

3 **Realizar una mayor labor a la hora de comprobar la identidad del cliente que efectúa la reclamación.**

4 Ejemplos reales

--

4. Ejemplos reales

4. Ejemplos reales

4. Ejemplos reales

SOCIEDAD

La estafa a la EMT: una operación 'de manual' de los ciberciminales

4. Ejemplos reales

SOCIEDAD

La estafa a la EMT: una operación 'de manual' de los ciberciminales

THE WALL STREET JOURNAL.

Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case

4. Ejemplos reales

4. Ejemplos reales

ISACA®
Trust in, and value from, information systems
Barcelona Chapter