SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

JUAN G DEL VALLE VÁZQUEZ, ISSO

INFORMATION SYSTEM SECURITY OFFICER

HOSPITAL AUXILIO MUTUO

OBJETIVOS

- Proveer conocimiento básico sobre las amenazas a los Sistemas de Información
- Cómo detectar y protegerse
- Guías para orientar a su personal sobre cómo prevenir ataques y cómo responder a los mismos.

CONCEPTO ABARCADOR

Programa de Seguridad	Correo Electrónico	Virus/Malware/ Ransomware
Phishing	Contraseñas	Protección de la Información
Seguridad Física	Ingeniería Social	Medidas de Prevención

PROGRAMA DE SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

- Integración de las normas y procedimientos de seguridad de información con las reglas del negocio en cuestión
- Toda empresa debe implementar y documentar un programa de seguridad de sus sistemas de información.
- Los ejecutivos de la empresa establecerán cuál es la misión y los objetivos que el programa debe cumplir.
- Objetivo principal: cumplir con las leyes y regulaciones estatales y federales que le apliquen.

PROGRAMA DE SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

- Puntos a considerar dentro del Programa de Seguridad
  - Inventario y documentación de los equipos y aplicaciones que estén conectados a la red.
  - Realizar un análisis de riesgo para detectar las amenazas y vulnerabilidades
  - Manejar los riesgos ya sean mitigando la amenaza o transfiriendo el riesgo a un ente externo.

PROGRAMA DE SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

- La creación de un programa de manejo de incidentes para documentar todo lo relacionado a eventos de seguridad.
- La creación de un Disaster Recovery Plan (DRP), en caso de sufrir una pérdida de data ya sea por un ataque cibernético o eventos externos.

PROGRAMA DE SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

- Implementar controles de seguridad en los sistemas.
- Adiestramiento a los empleados.
- Realizar auditorías.

CORREO ELECTRÓNICO (EMAIL)

- Medio principal de comunicación
- Envío de documentos con información confidencial
  - seguro social, información de pacientes, financiera
- Medidas para proteger la información
  - cifrado del correo electrónico
  - contraseña al documento

CORREO ELECTRÓNICO (EMAIL)

- Evite abrir mensajes si
  - No conoce al remitente
  - Conoce al remitente pero no acostumbra intercambiar mensajes
- No haga clic en un enlace o descargue un archivo si no le es familiar

CORREO ELECTRÓNICO (EMAIL)

- ¿Qué hacer?
  - Repórtelo a su Dpto de Información y Tecnología
- Implicaciones
  - Robo de su identidad
  - Perder acceso a sus archivos y/o cuentas personales

MALWARE

- “Malicious Software”
- Estos programas se instalan en los equipos (computadoras, móviles, tablets) para tomar control y ganar así acceso al contenido de los mismos.
- Puede espiar lo que usted hace en el Internet, robar las credenciales que tenga grabadas en sus equipos y robar archivos que tenga en su computadora.
- Atacan toda clase de sistemas operativos y dispositivos
  - Windows y Android - los más atacados por ser los de mayor popularidad

MALWARE

- Virus: infectan archivos con el solo propósito de modificarlo o dañarlo.
  - ILOVEYOU: Propagado en el año 2000 través de correos electrónicos, dejo sobre $10 billones en pérdidas y se cree que sobre el 10% de las computadoras en el mundo fueron infectadas.
  - Melissa: Propagado en el año 1999 través de correos electrónicos. Causó sobre $80 millones en daños
  - Sasser: Descubierto en el 2004. Atacó una vulnerabilidad en el sistema operativo Windows. Los daños fueron estimados en sobre $18 billones y sobre un millón de computadoras infectadas.

MALWARE

- Adware: Este tipo de malware abre ventanas de publicidad de diferentes productos o servicios.
- Backdoors: Es un programa que abre un puerta trasera en sistema operativo permitiendo que un atacante entre a su computadora sin que usted se percate. El atacante tendrá control total de su computadora, podrá ver todo lo que usted hace e incluso puede borrar sus archivos, copiarlos y hasta encender su webcam.

MALWARE

- Botnet: Infectan todo tipo de equipos que estén conectados en el internet, como las computadoras, cámaras de seguridad, televisores (SmartTV), etc. La función de este malware es utilizar los equipos infectados y lanzar ataques simultáneos para afectar servicios, extraer información, entre otros. Un ejemplo reciente es el Botnet llamado Mirai que afecto cientos de equipos y paginas de Internet en todo el mundo.
- Ransomware

MALWARE

- Esta es la cuota del mercado de los sistemas operativos en las computadoras, según la pagina www.netmarketshare.com:
- Windows (NT,XP,Vista, 7, 8, 8.1,10): 87.92%
  - MAC OS X: 9.46%
  - Linux: 2.03%
- Esta es la cuota del mercado de los sistemas operativos en los celulares:
  - Android: 70.12%
  - iOS: 28.53%
- Esta es la cuota del mercado de los sistemas operativos en las tablets:
  - Android: 51.17%
  - iOS: 48.82%

PHISHING

- El Phishing es un ataque empleado por ciber-criminales con el objetivo de engañar y hacer que la persona revele información personal o que realice ciertas acciones en su equipo.
- Estos ataques comienzan cuando un criminal envía un mensaje haciéndose pasar por una persona o una entidad que conoces como, por ejemplo, un amigo, tu banco, portales de video como Netflix, o una tienda online.

PHISHING

- Estos mensajes llegan con algún tipo de instrucciones para que entres a un link y entres tu información personal, ya sea tus credenciales de tu cuenta de banco o tus credenciales de tu cuenta de la tienda online como por ejemplo, Amazon o EBay.
- El contenido de los mensajes es bastante elaborado con el fin de que el mensaje se vea lo más cercano a un comunicado oficial de la tienda, banco, etc.
- Este tipo de ataque no se limita a mensajes de correos electrónicos, también se usan los programas de mensajería instantánea como Whatsapp o por las redes sociales.

EJEMPLOS DE PHISHING


NETFLIX

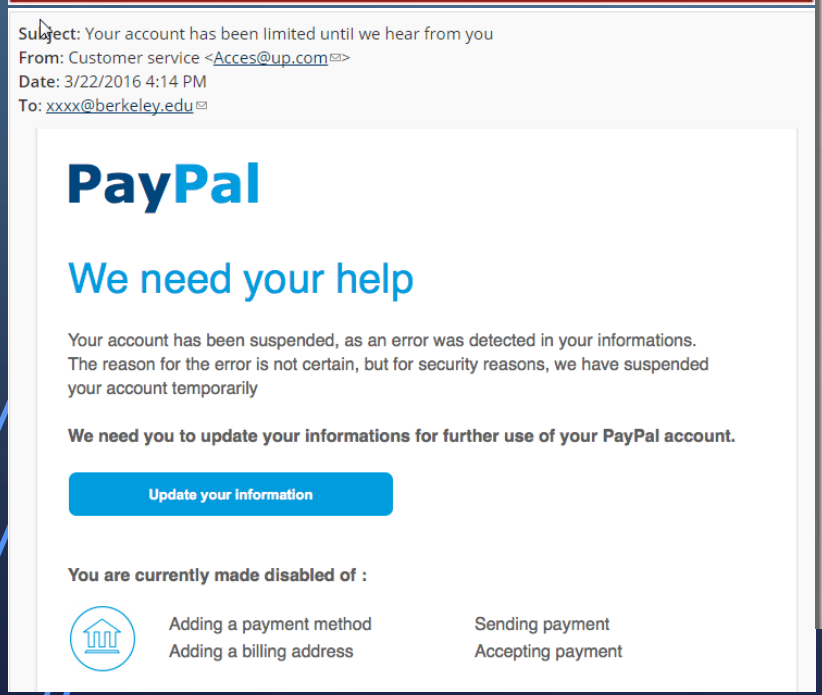
Your Account | Queue | Help

Your Account Has Been Suspended

Dear Netflix,

We are sending this email to let you know that your credit card has been expired. To update your account information, please visit Your Account.

-Your friends at Netflix


Subject: Your account has been limited until we hear from you
From: Customer service <Acces@up.com>
Date: 3/22/2016 4:14 PM
To: xxxx@berkeley.edu

PayPal

We need your help

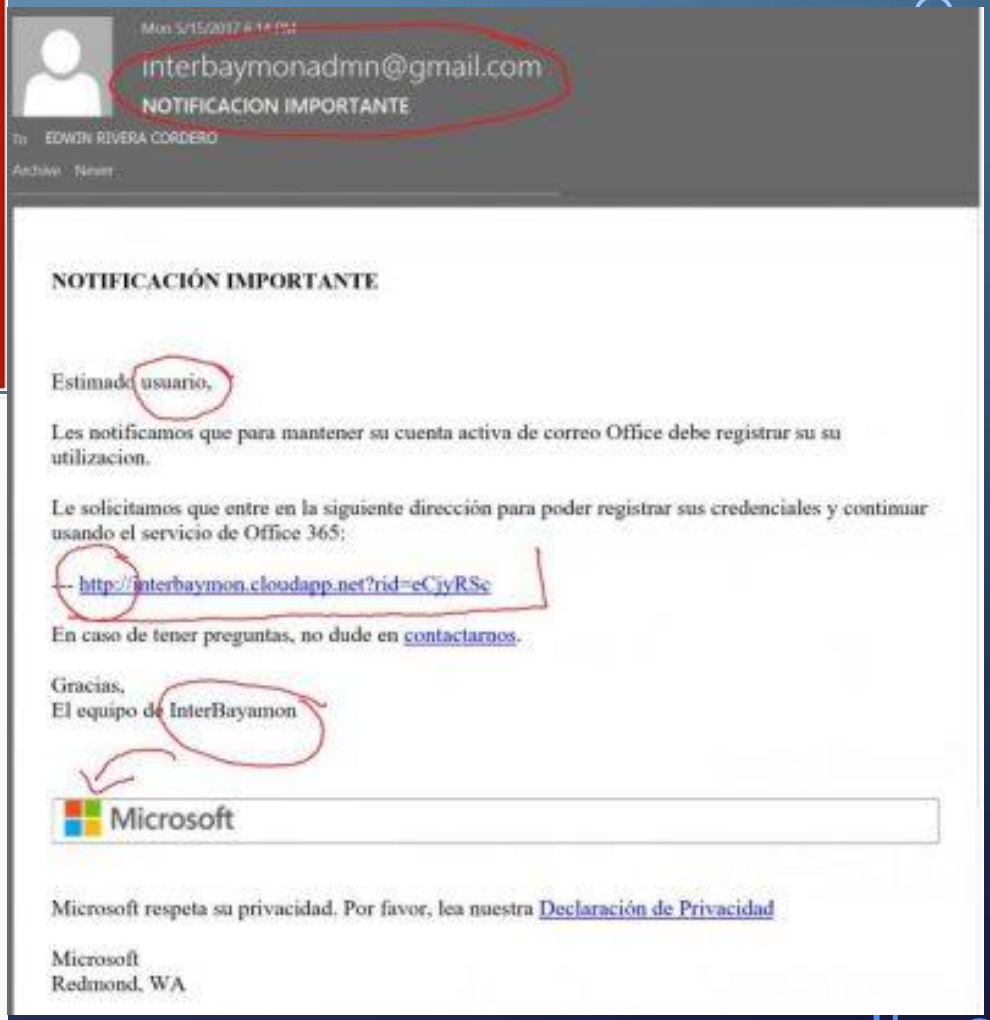
Your account has been suspended, as an error was detected in your informations. The reason for the error is not certain, but for security reasons, we have suspended your account temporarily

We need you to update your informations for further use of your PayPal account.

Update your information

You are currently made disabled of :

Adding a payment method
Adding a billing address
Sending payment
Accepting payment


interbaymonadmn@gmail.com
NOTIFICACION IMPORTANTE
To EDWIN RIVERA CORDERO

NOTIFICACIÓN IMPORTANTE

Estimado usuario,

Les notificamos que para mantener su cuenta activa de correo Office debe registrar su su utilizacion.

Le solicitamos que entre en la siguiente dirección para poder registrar sus credenciales y continuar usando el servicio de Office 365:

http://interbaymon.cloudapp.net?rid=eCjyRSc

En caso de tener preguntas, no dude en contactarnos.

Gracias,
El equipo de InterBayamon

Microsoft

Microsoft respeta su privacidad. Por favor, lea nuestra Declaración de Privacidad

Microsoft
Redmond, WA

EJEMPLOS DE PHISHING

Blocked Incoming Messages

This message(s) below have been blocked by your [redacted] administrator due to validation error.
There are new messages in your Email Quarantine messages will be automatically removed from quarantine after 7 day(s).

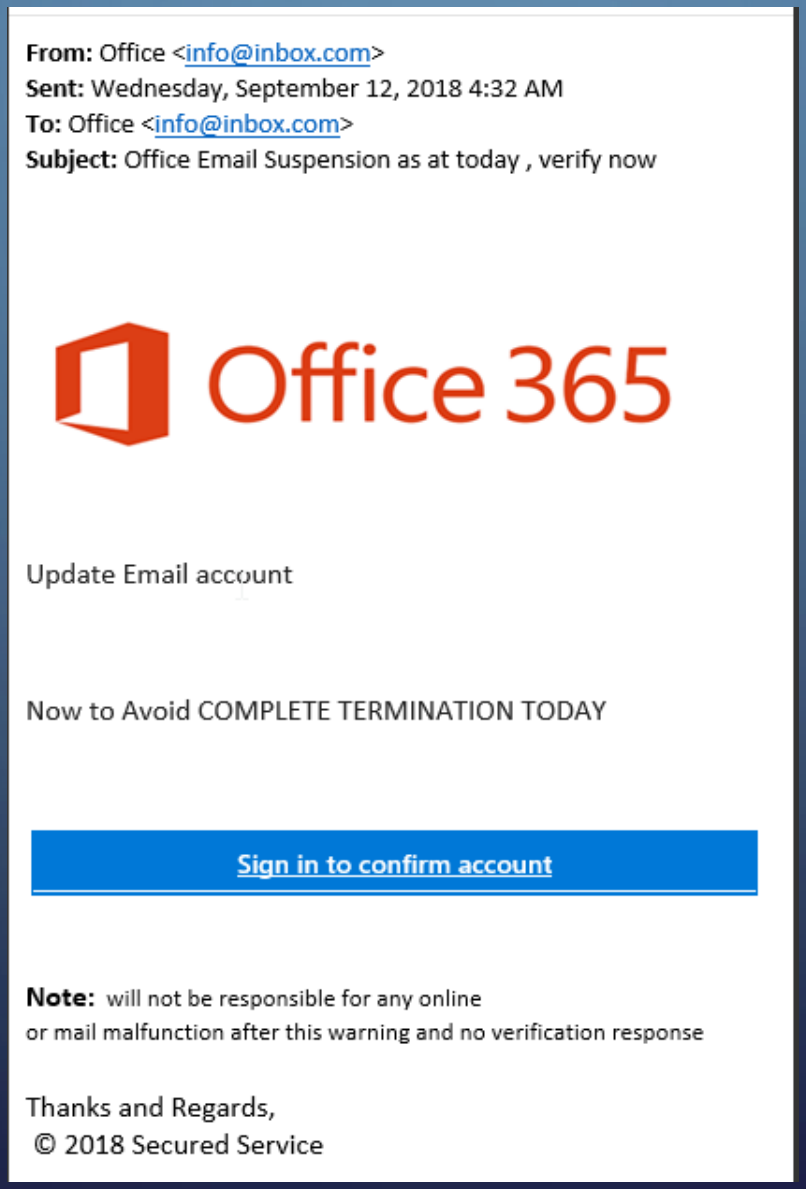
To see all quarantined messages view your email quarantine and release to inbox

Quarantined email			
	Recipient:	Subject:	Date:
Releahe	[redacted]	Incoming Transfer from Sale@.... [HSBC]	%DATE%
Release		Re: Re: Contract | INVOICE COPY |	%DATE%
Release		Re: SALES ORDER CONFIRMATION SO: 0057528	%DATE%
Release		Dhl Express Shipment 889000787 Notification	%DATE%
			Open all messages

Note: This message was sent by the system for notification only. Please do not reply

If this message lands in your spam folder, please move it to your inbox folder for proper interrogation:

EJEMPLOS DE PHISHING



From: Office <info@inbox.com>
Sent: Wednesday, September 12, 2018 4:32 AM
To: Office <info@inbox.com>
Subject: Office Email Suspension as at today , verify now

Office 365

Update Email account

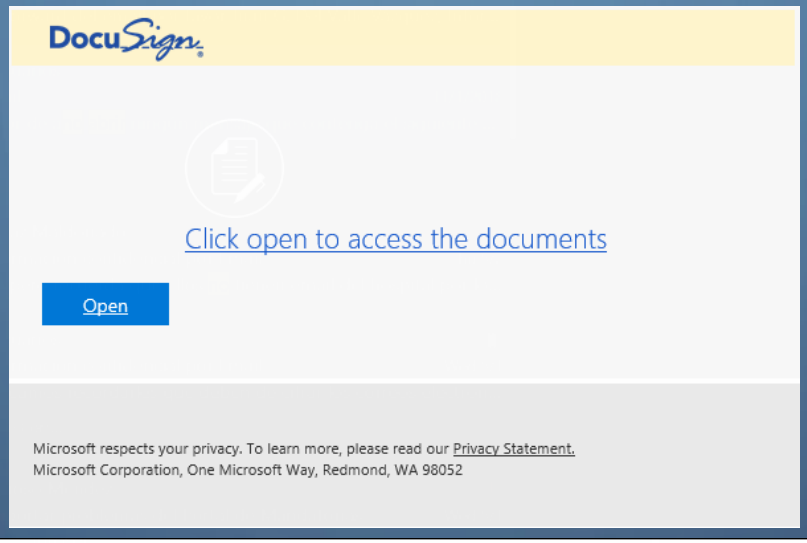
Now to Avoid COMPLETE TERMINATION TODAY

Sign in to confirm account

Note: will not be responsible for any online
or mail malfunction after this warning and no verification response

Thanks and Regards,
© 2018 Secured Service

EJEMPLOS DE PHISHING



From: Mail Service <fileserver@abakusbp.net>
Date: April 30, 2019 at 12:09:14 AM AST
To: <[redacted]
Subject: Mail Security Notice!

Mail Verification Setup

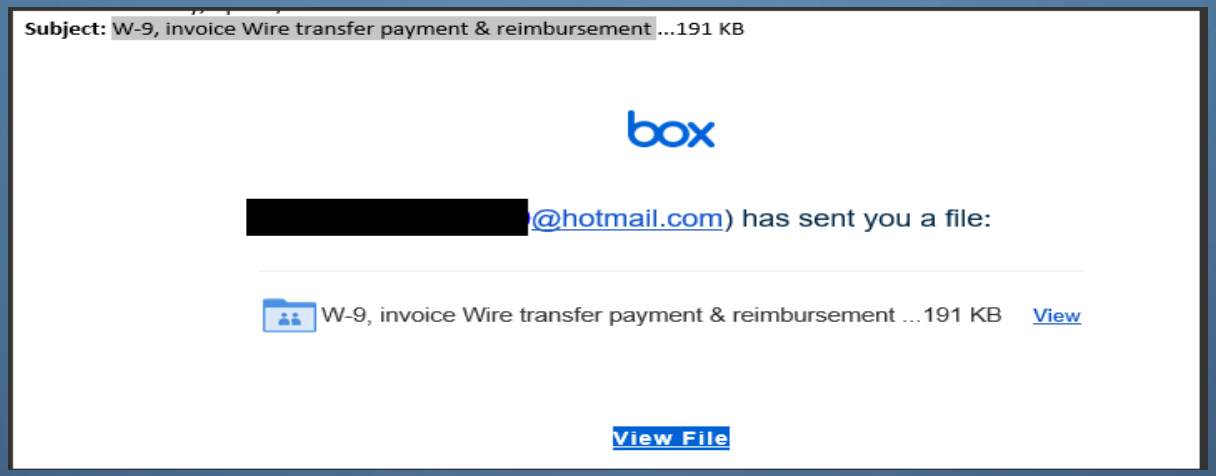
Your account [redacted] profile has been disabed due to suspecious activity notice

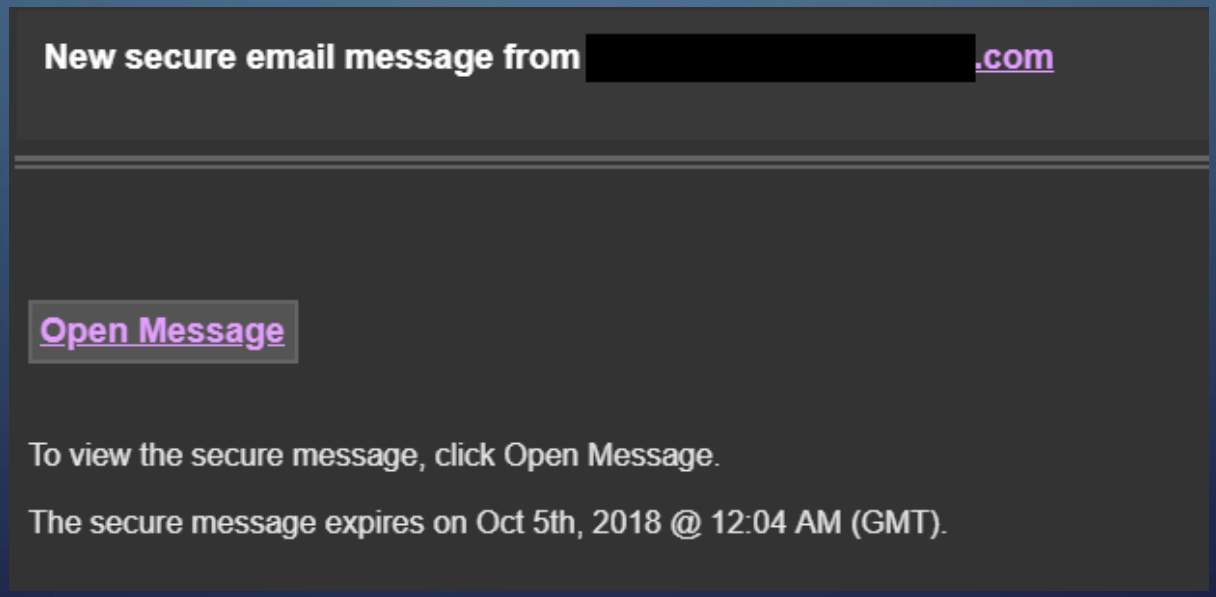
Activate below.

[Activate profile]

®Mail Service Team

EJEMPLOS DE PHISHING





COMO IDENTIFICAR UN ATAQUE DE PHISHING

SANS SECURING THE HUMAN PHISHING

¡NO MUERDAS EL ANZUELO!

¿QUÉ ES EL PHISHING?

El phishing es un ataque psicológico empleado por ciber criminales con el objetivo de engañarte y hacer que reveles determinada información o que realices cierta acción. Originalmente, el término phishing se empleaba para describir ataques a través de correo electrónico ideados para robar tu nombre de usuario y contraseña de algún servicio online. Sin embargo, el término ha evolucionado y actualmente se refiere a casi cualquier ataque basado en mensajes. Estos ataques comienzan cuando un criminal envía un mensaje haciéndose pasar por una persona o una entidad que conoces, como un amigo, tu banco o una tienda online popular.

En estos mensajes, tratan de persuadirte para que realices una acción, como hacer click en un enlace malicioso, abrir un archivo adjunto infectado o responder a una estafa. Normalmente, los delincuentes elaboran estos correos con una apariencia convincente y después los envían a millones de personas en todo el mundo. Aunque no conocen la identidad de sus víctimas, saben que cuantos más emails envíen, a más personas podrán engañar. Estos ataques no se limitan al correo electrónico, también usan otros métodos como la mensajería instantánea o los mensajes en redes sociales.

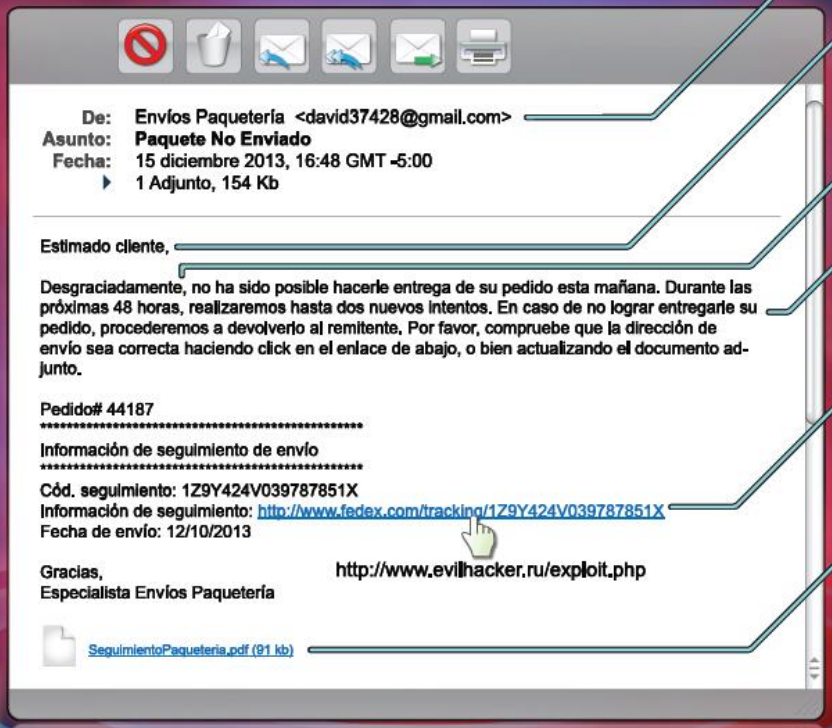
¿QUÉ ES EL SPEAR PHISHING?

El concepto es el mismo que el phishing, salvo que en lugar de enviar correos de forma indiscriminada a millones de víctimas potenciales, los criminales dirigen sus ataques a una reducida selección de personas. Con el spear phishing, los atacantes investigan a sus víctimas, por ejemplo leyendo sus perfiles de LinkedIn o Facebook o cualquier mensaje que hayan escrito en foros o blogs públicos. Después, basándose en esa investigación previa, los criminales escriben un email altamente personalizado y con un contenido relevante para su objetivo. De esta manera, es muchísimo más probable que una persona caiga en el engaño.

Este póster ha sido desarrollado como un proyecto comunitario. Han contribuido: Cheryl Conley (Lockheed Martin), Tim Harwood (BP), Tonia Dudley (Honeywell), Ellen Powers (MITRE Corporation), Shanah Johnson (Reserve Bank of Atlanta) and Terri Chihota.

¿POR QUÉ ME DEBE IMPORTAR ?

Quizás no seas consciente de ello, pero eres un objetivo del phishing tanto en el trabajo como en casa. Tus cuentas, tu información y tus dispositivos valen una enorme cantidad de dinero para los ciber criminales y ellos harán lo que puedan para hackearlos. TÚ eres la manera más efectiva de detectar y detener el phishing. Si sospechas que un email puede ser phishing o si te preocupa haber caído víctima de uno, ponte inmediatamente en contacto con tu servicio de soporte técnico o tu equipo de seguridad. Si deseas saber más sobre phishing o probar la plataforma para pruebas de phishing de SANS Securing the Human, por favor visita http://www.securingthehuman.org/phishing.



De: Envíos Paquetería <david37428@gmail.com>
Asunto: **Paquete No Enviado**
Fecha: 15 diciembre 2013, 16:48 GMT -5:00
1 Adjunto, 154 Kb

Estimado cliente,

Desgraciadamente, no ha sido posible hacerle entrega de su pedido esta mañana. Durante las próximas 48 horas, realizaremos hasta dos nuevos intentos. En caso de no lograr entregarle su pedido, procederemos a devolverlo al remitente. Por favor, compruebe que la dirección de envío sea correcta haciendo click en el enlace de abajo, o bien actualizando el documento adjunto.

Pedido# 44187
****
Información de seguimiento de envío
****
Cód. seguimiento: 1Z9Y424V039787851X
Información de seguimiento: http://www.fedex.com/tracking/1Z9Y424V039787851X
Fecha de envío: 12/10/2013

Gracias,
Especialista Envíos Paquetería

http://www.evilhacker.ru/exploit.php

SeguimientoPaquete.pdf (91 kb)

INDICADORES DE PHISHING

A Comprueba las direcciones. Si el email parece proceder de una organización legítima, pero en el "FROM" aparece una dirección de tipo personal, como @gmail.com o @hotmail.com, probablemente se trate de un ataque. Comprueba también los campos "TO" y "CC". ¿Se está enviando el email a personas que no conoces o con las que no trabajas?

B Sospecha de los correos en los que se dirigen a ti como "Querido cliente" o en los que usan otras fórmulas de saludo genéricas. Si una organización de confianza necesita ponerse en contacto contigo, deberían conocer tu nombre y otros datos. Pregúntate también ¿espero recibir un email de esta compañía?

C Sospecha de errores ortográficos y gramaticales; la mayoría de empresas revisan cuidadosamenre sus mensajes antes de enviarlos.

D Sospecha de cualquier email que solicite una "acción inmediata" o que cree un sentimiento de urgencia. Se trata de una técnica comúnmente utilizada para provocar que se cometan errores. Ten también presente que las organizaciones legítimas no te pedirán información personal.

E Sé cuidadoso con los enlaces y haz click sólo en aquellos que esperas recibir. Coloca el puntero del ratón sobre el enlace, sin llegar a hacer click sobre él. Esto te mostrará la verdadera dirección web que visitarías al click en el enlace. Si la verdadera dirección es distinta de la que se muestra en el correo, se trata de un indicador de un ataque.

F Sospecha de archivos adjuntos. Abre únicamente aquellos que esperabas recibir.

G Sospecha de cuaquier mensaje que suene demasiado bueno para ser cierto (No, ¡no has ganado la lotería!).

H El solo hecho de recibir un email de un amigo no significa que sea éste quien lo ha enviado. Puede ser que el ordenador de tu amigo haya sido infectado con malware o que su cuenta de correo haya sido comprometida. Si recibes un email sospechoso de un amigo o un colega de confianza, llámale por teléfono.

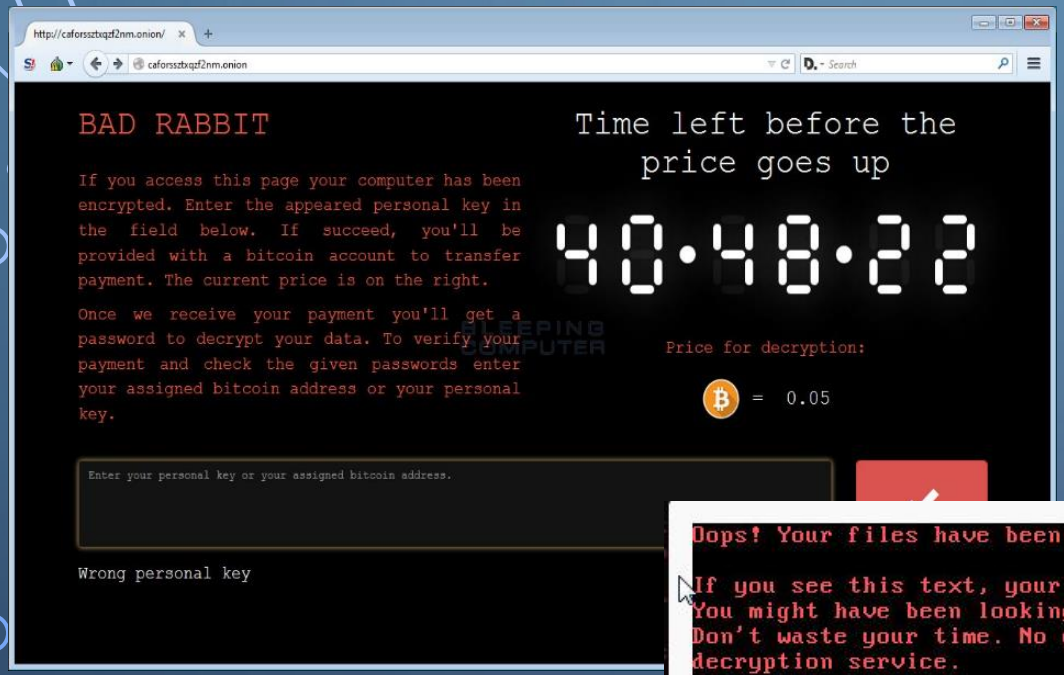
COMO EVITAR SER VICTIMA DE PHISHING

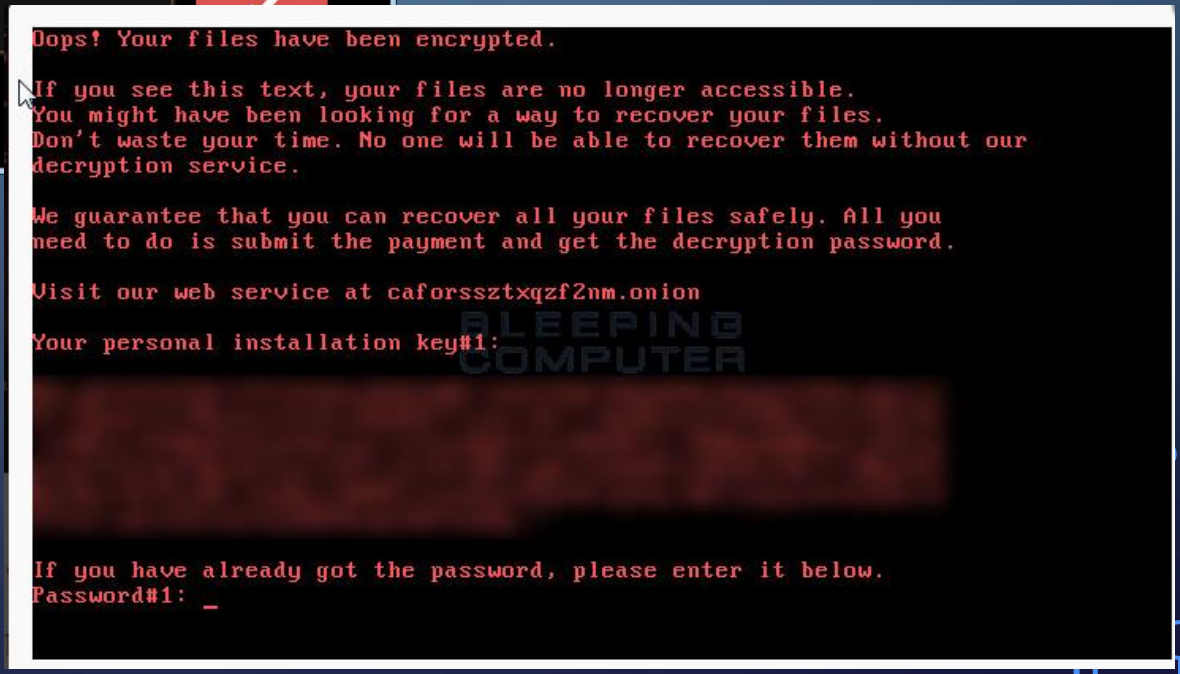
- No haga clic en ningún enlace (link) que tenga el mensaje
- No descargue ningún archivo que incluya el mensaje
- Borre el mensaje
- Mantenga su sistema operativo con todas las actualizaciones al día
- Mantenga actualizado y activado su antivirus
- Esto debe de aplicarse a todos los equipos, incluyendo Apple, Android, Windows, Linux, etc.
- ¡¡¡Oriente a sus empleados!!!

RANSOMWARE

- Tipo de malware que destruye documentos y archivos de la computadora.
- Infecta su computadora, encripta ciertos archivos o todo el disco duro, y le informa que debe de pagar una cantidad de dinero (usualmente en Bitcoins) para poder brindarle acceso a sus archivos.
- Se propaga a través de correos electrónicos, dispositivos de almacenamientos externos, etc.

RANSOMWARE “BAD RABBIT”





RANSOMWARE WANNACRY

CONTRASEÑAS

- Nunca comparta las contraseñas o códigos con nadie.
- Cambie su contraseña si descubre o sospecha que alguien la conoce.
- Nunca escriba sus contraseñas en papel, “post-it”, etc.
- Evite utilizar información que puedan saber de usted, como por ejemplo:
  - Fecha de nacimiento
  - Nombre de sus animales
  - Nombre de sus hijos o parientes cercanos

  - Cada usuario es el responsable de
  - lo que suceda con su cuenta

CONTRASEÑAS

- No utilice las mismas contraseñas para sus cuentas del trabajo y las personales.
- No reúse contraseñas, por ejemplo:
  - Francia1
  - Francia2
- Cambie sus contraseñas cada 60 a 90 días.

CONTRASEÑAS

- Trate de utilizar frases como una contraseña, como por ejemplo:
  - Mivi@jeenel2018fueestup3ndo
  - Mi@buelametirabaconlachanclet4
- Utilice contraseñas largas, complejas y únicas, como por ejemplo:
  - 9@kj*YbM25nGnl
  - Lq@6eNuQcwyMvW5C

ERES VULNERABLE

VERSIÓN EN ESPAÑOL

UNAM CERT

Aunque no te des cuenta, tú eres un blanco para muchos criminales cibernéticos. Tu computadora, tus dispositivos móviles, tus cuentas y tu información; todos tienen un gran valor. Este poster demuestra las diferentes maneras que tienen los criminales cibernéticos para ganar dinero al hackearte. Afortunadamente, solo con tomar un par de medidas simples, puedes protegerte a ti y a tu familia. Si quieres aprender más, subscríbete a OUCH!: un boletín informativo diseñado para ayudar a personas como tú.

www.securingthehuman.org/ouch

Nombres de usuario y contraseñas

Una vez que te han hackeado, los criminales cibernéticos pueden instalar programas en tu computadora que capturan las teclas que presionas y todas y cada una de las palabras que introduces en tu equipo, incluyendo tu nombre de usuario y contraseña. Esa información es usada para acceder a tus cuentas en línea, por ejemplo:

- *Tus cuentas financieras y/o bancarias, dentro de las cuales pueden robar o transferir tu dinero.*
- *Tus cuentas de iCloud, Google Drive, o Dropbox donde pueden acceder a todos tu datos confidenciales.*
- *Tus cuentas de Amazon, Walmart u otras cuentas de compras donde pueden adquirir bienes a tu nombre.*
- *Tus cuentas de UPS o DHL, donde pueden enviar bienes robados a tu nombre.*

Recolección de Email

Una vez que te han hackeado, los criminales cibernéticos pueden leer tu email en busca de información que pudieran vender a otros, por ejemplo:

- *Todos los nombres, direcciones de correo electrónico y números telefónicos de tu lista de contactos.*
- *Toda tu correspondencia electrónica personal o de trabajo.*

Bienes virtuales

Una vez que te han hackeado, los criminales cibernéticos pueden copiar y robar cualquier bien virtual que tengas y venderlo a otros, por ejemplo:

- *Tus personajes de juego en línea, los bienes que adquieres en el juego o el dinero virtual que usas para jugar.*
- *Cualquier licencia de software, números de licencia de sistemas operativos o licencias de juegos.*

Botnet

Una vez que te han hackeado, tu computadora puede ser conectada a toda una red de computadoras hackeadas controladas por los criminales cibernéticos. Esta red, llamada botnet, puede entonces ser usada para actividades como:

- *Envío de spam a millones de personas.*
- *Lanzamiento de ataques de denegación de servicio.*

Suplantación de identidad

Una vez que te han hackeado, los criminales cibernéticos pueden robar tu identidad en la red para cometer fraudes o vender tu identidad a otros, por ejemplo:

- *Tus cuentas de Facebook, Twitter o LinkedIn.*
- *Tus cuentas de correo electrónico.*
- *Tus cuentas de Skype u otras cuentas de mensajería instantánea.*

Servidores web

Una vez que te han hackeado, los criminales cibernéticos pueden convertir tu computadora en un servidor web, el cual pueden usar para cosas como:

- *Alojar sitios de phishing que roben nombres de usuario y contraseñas de otras personas.*
- *Alojar herramientas de ataque que hackearán las computadoras de las personas.*
- *Distribuir pornografía infantil, videos piratas o música robada.*

Finanzas

Una vez que te han hackeado, los criminales cibernéticos pueden revisar tu sistema en busca de información valiosa, por ejemplo:

- *Tu información de tarjeta de crédito.*
- *Tus registros de impuestos y antecedentes financieros.*
- *Información sobre tus planes de inversión y de retiro.*

Extorsión

Una vez que te han hackeado, los criminales cibernéticos pueden tomar el control de tu computadora y exigir dinero. Pueden hacerlo a través de:

- *Tomar fotos tuyas con la cámara de tu computadora y exigir un pago para destruir o no distribuir tus fotos.*
- *Cifrar toda la información en tu computadora y exigir un pago para poder recuperarla.*
- *Siguiendo todos los sitios web que visitas amenazando con difundir tu actividad.*

Este boletín informativo está basado en el trabajo original de Brian Krebs. Puedes aprender más acerca de los criminales cibernéticos en su blog: **http://krebsonsecurity.com**

AUTENTICACIÓN MULTIFACTORIAL (MFA)

Combina dos o más credenciales independientes

- lo que sabe el usuario (contraseña)
- lo que tiene el usuario (token de seguridad) y
- lo que es el usuario (verificación biométrica)

AUTENTICACIÓN MULTIFACTORIAL (MFA)

- Objetivo: crear una defensa por capas y hacer que sea más difícil para una persona no autorizada acceder a un objetivo, como una ubicación física, un dispositivo de cómputo, una red o una base de datos.
- Si uno de los factores se ve comprometido o se rompe, el atacante todavía tiene al menos una barrera más que romper antes de ingresar con éxito en el objetivo.

PROTECCIÓN DE LA INFORMACIÓN

Los ciber criminales buscan cualquier método para apropiarse de data confidencial. La información que mas buscan los criminales son las siguientes:

Información de salud, personal y financiera: (PHI, PII)

- Nombre Completo
- Todo identificador demográfico
- Fechas que identifiquen al individuo (fecha de nacimiento, fecha de admisión, etc.)
- Números de teléfonos y Fax
- Direcciones de correos electrónicos (email)
- Direcciones de Internet (URL)
- Numero de seguro social
- Direcciones IP
- Numero de expedientes médicos
- Identificadores de Biometría (huellas, voz, etc.)
- Numero de plan medico
- Fotografía del rostro
- Números de cuentas (Tarjetas de Créditos, Bancos, etc.)
- Numero de certificados o licencia.
- Cualquier otra característica que pueda identificar de manera única al individuo.

PROTECCIÓN DE LA INFORMACIÓN

Envíe información confidencial por correo electrónico de manera segura (encriptada).

No abra correos electrónicos que usted no esperaba o le parezcan sospechosos.

No imprima documentos con información confidencial si no hay la necesidad de hacerlo.

No copie ningún archivo a algún medio de almacenamiento externo (Pendrive, disco duro externo, CD's, etc.)

Evite navegar en páginas de Internet no relacionadas a sus funciones en horas de trabajo.

No entre a ver información de pacientes que usted no tenga asignados.

SEGURIDAD FÍSICA

- Asegurar el espacio físico donde se maneja información confidencial.
- Cuestione la presencia de toda persona extraña en áreas restringidas como las unidades de enfermería, cuartos eléctricos, cuartos de comunicaciones.
- Alerte a su supervisor y/o seguridad.
- Asegúrese de que todo personal tenga su identificación.
- Todo personal contratista que va a realizar algún trabajo debe de tener su identificación de la compañía. El personal del Hospital se debe asegurar de que esa persona este autorizada a trabajar en el área.

SEGURIDAD FÍSICA

- Siempre bloquee o saque su usuario de la computadora cuando se retira de la misma.
- No permita que otro usuario utilice su cuenta de usuario. Recuerde usted es el responsable de lo que suceda con su cuenta de usuario en el sistema.
- Nunca deje documentos con material confidencial desatendido.
- Tenga disponible las políticas y normas de uso del sistema en un lugar accesible y rápido de acceder como el intranet de su compañía.

INGENIERÍA SOCIAL

"La ingeniería social es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infectar sus computadoras con malware o abran enlaces a sitios infectados. Además, los hackers pueden tratar de aprovecharse de la falta de conocimiento de un usuario; debido a la velocidad a la que avanza la tecnología, numerosos consumidores y trabajadores no son conscientes del valor real de los datos personales y no saben con certeza cuál es la mejor manera de proteger esta información." (Ingeniería social: definición, 2018)

INGENIERÍA SOCIAL

Ejemplos de un ataque de Ingeniería Social:

- Ataques de Phishing: Refiérase a la sección de Phishing
- Recibe un correo electrónico que parece provenir de un empleado, el cual le indica que debe de descargar un archivo o presionar un enlace (link) que lo lleva a una pagina web donde le solicita sus credenciales.
- La victima puede recibir una llamada del atacante el cual pretende ser un empleado, vendedor, personal de ley (policía, agente federal, etc.) auditor, etc. El atacante le indica que su cuenta será desactivada o que está comprometida y para evitar que su cuenta se desactive le debe proveer sus credenciales (username y password) entre otra información personal.
- Atacante pretende ser empleado, espera por un empleado con acceso a un área restringida que requiere uso de código o biometría, le pide que aguante la puerta ya que se le olvidó el código, o la biometría no le funciona.

MEDIDAS DE PREVENCIÓN

- No deje ningún documento con información confidencial desatendido.
- Sea consciente del contenido cuando disponga de un documento.
- Siga las políticas y normas del uso del sistema y de Recursos Humanos.
- No permita que usen su cuenta de usuario. Usted es el responsable de lo que suceda con su cuenta.
- El que usted tenga acceso al sistema no le da derecho a acceder información de casos que no tenga asignados. Ejemplo: Usted pertenece a pediatría pero está navegando en cuentas de pacientes de Intensivo adulto.
- Sea precavido en abrir correos electrónicos de personas que no conoce o que no estaba esperando.
- No debe navegar por páginas de compras, banca, noticias, etc. en computadoras de la empresa si no está autorizado.
- No debe en enviar por mensajes de texto con información de pacientes.

MEDIDAS DE PREVENCIÓN

- No debe usar dispositivos de almacenamientos como Pendrive, discos duros externos, teléfonos, etc.
- No debe de instalar aplicaciones que no estén autorizadas por el Departamento de Información y Tecnología.
- Utilice contraseñas seguras (vea sección de Contraseñas)
- No habilite la opción de “Remember Password” en las páginas de internet que visita
- No escriba sus credenciales en papeles o notas.
- No coloque información confidencial de la compañía o personal en las redes sociales.
- Utilice en la medida que sea posible autenticación multifactorial (MFA).

FUGA DE INFORMACIÓN (BREACHES)

- Las multas a causa de fugas de información pueden rondar desde los miles hasta los millones de dólares.
- El total de multas en los últimos 3 años por entes reguladores (Office of Civil Rights) fueron las siguientes:
  - 2016: $23 millones
  - 2017: $20 millones
  - 2018: $28 millones (en este año se ha registrado la multa más alta en la historia a la aseguradora Anthem por $16 millones)

FUGA DE INFORMACIÓN (BREACHES)

- Además de las multas, hay otras consecuencias tales como:
  - Pérdida de confianza por parte de inversionistas
  - Pérdida de confianza por parte de los clientes
  - Demandas civiles y criminales
  - Pérdida de suplidores

SHARED

Stolen USB Drive Leads to $2.2 Million HIPAA Breach Penalty

The exterior of the U.S. Department of Health and Human Services in Washington, DC. 2006

Phishing Leads to Healthcare Breach

Experts Say More Employees Are Being Targeted

Marianne Kolbasuk McGee (HealthInfoSec) · April 23, 2015

Twitter Facebook LinkedIn Credit Eligible Get Permission

A **breach** affecting nearly 760 patients at **St. Vincent Medical Group** in Indiana is the latest example of a healthcare organization falling victim to an apparent upswing in phishing attacks targeting employees.

NEWS

3 phishing hacks breach 20,000 Catawba Valley patient records

by Jessica Davis | October 25, 2018

While investigating one phishing attack in August, medical center officials discovered a hacker had access to three accounts for more

NEWS

CMS responds to data breach affecting 75,000 in federal ACA portal

by Susan Morse | October 22, 2018

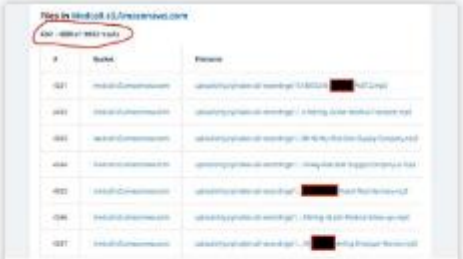
Open enrollment, which begins November 1, will not be negatively impacted, CMS says.

NEWS

Two phishing attacks on Minnesota DHS breach 21,000 patient records

by Jessica Davis | October 12, 2018

For more than a month, two separate employee accounts were compromised by the cyberattacks before the IT department



NEWS

Update: Misconfigured database breaches MedCall Advisors

by Jessica Davis | October 10, 2018

A researcher discovered the North Carolina-based tech vendor is leaking protected

NEWS

3 Massachusetts hospitals fined nearly $1 million by OCR for HIPAA violations

by Jessica Davis | September 21, 2018

Boston Medical Center, Brigham and Women's Hospital and Massachusetts General Hospital

NEWS

Employee error exposed Blue Cross patient data for 3 months

by Jessica Davis | September 21, 2018

An employee uploaded a file containing member information to a public-facing

Healthcare IT News

GLOBAL EDITION | TOPICS | SIGN UP | MAIN MENU

NEWS

Ransomware attack breaches 40,800 patient records in Hawaii

by Jessica Davis | September 13, 2018

The Fetal Diagnostic Institute of the Pacific was able to restore data from backups, and with help from a cybersecurity firm wipe the

NEWS

Phishing attack breaches 38,000 patient records at Legacy Health

by Jessica Davis | August 22, 2018

The hackers went undetected for several weeks at the Portland, Oregon-based health system.

NEWS

417,000 Augusta University Health patient records breached nearly one year ago

by Jessica Davis | August 17, 2018

The Georgia provider was hit by two cyberattacks in September 2017, but did not explain when the breach was discovered.

NEWS

Canadian pharmacist fined for routinely accessing health records of acquaintances

by Lynne Minion | August 13, 2018

She snooped in the EHRs of nearly four dozen people over two years.

NEWS

1.4M records breached in UnityPoint Health phishing attack

by Jessica Davis | July 31, 2018

This is the second breach for the health system this year, and the biggest health data breach of 2018 in the U.S.

NEWS

Third-party vendor error exposes data of 19K patients for 2 months

by Jessica Davis | August 02, 2018

Orlando Orthopaedic's transcriptionist vendor misconfigured access to a database during a software upgrade. The health center waited


LA
SEGURIDAD
ES RESPONSABILIDAD
DE TODOS

VIDEOS

- Phishing: https://www.youtube.com/watch?v=GHTq3RzQcKw
- Comprando en Internet: https://www.youtube.com/watch?v=3P6Kzwo5eZg
- Prevención en el uso de redes sociales: https://www.youtube.com/watch?v=Nrmz0wKC1i0
- Proteja sus Datos: https://www.youtube.com/watch?v=IhhEt5w4DNY

REFERENCIAS

- Ingeniería social: definición. (2018). Retrieved from Kaspersky: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering
- Rouse, M. (2014, Junio). Autenticación multifactor (MFA). Retrieved from SearchDataCenter en Español: https://searchdatacenter.techtarget.com/es/definicion/Autenticacion-multifactor-MFA
- Posters. (n.d.). Retrieved from www.sans.org: https://www.sans.org/security-resources/posters/
- Imam, F. (2018, Agosto 31). Top 10 Security Awareness Training Topics for Your Employees. Retrieved from https://resources.infosecinstitute.com/: https://resources.infosecinstitute.com/top-10-security-awareness-training-topics-for-your-employees/#gref
- Office for Civil Rights. (2015, Abril 16). The HIPAA Privacy Rule. Retrieved from www.hhs.gov: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
- Office for Civil Rights. (2017, Mayo 12). The Security Rule. Retrieved from www.hhs.gov: https://www.hhs.gov/hipaa/for-professionals/security/index.html

REFERENCIAS

- HIPAA Journal. (2017, October 26). Data Breach Highlights Danger of Using USB Drives to Store PHI. Retrieved from hipaajournal: https://www.hipaajournal.com/data-breach-danger-usb-drives-store-phi/
- Brown, A. (2017, January 20). Stolen USB Drive Leads to $2.2 Million HIPAA Breach Penalty. Retrieved from datacenterknowledge: https://www.datacenterknowledge.com/archives/2017/01/20/stolen-usb-drive-leads-to-2-2-million-hipaa-breach-penalty
- Commins, J. (2018, October 16). ANTHEM TO PAY BIGGEST HIPAA SETTLEMENT IN HISTORY. Retrieved from healthleadersmedia: https://www.healthleadersmedia.com/anthem-pay-biggest-hipaa-settlement-history
- Davis, J., Morse, S., Minion, L., & Jones Sanborn, B. (2018). The biggest healthcare data breaches of 2018 (so far). Retrieved from Healthcare IT News: https://www.healthcareitnews.com/projects/biggest-healthcare-data-breaches-2018-so-far
- Jamaluddin, A. (2017, June 18). 10 Most Destructive Computer Viruses. Retrieved from hongkiat: https://www.hongkiat.com/blog/famous-malicious-computer-viruses/
- Kolbasuk McGee, M. (2015, April 23). Phishing Leads to Healthcare Breach. Retrieved from databreachtoday: https://www.databreachtoday.com/phishing-leads-to-healthcare-breach-a-8154
- Krebs, B. (2018, September). Mirai Botnet Authors Avoid Jail Time. Retrieved from krebsonsecurity: https://krebsonsecurity.com/tag/mirai-botnet/
- Largest Healthcare Data Breaches of 2018. (2018, December 27). Retrieved from hipaajournal: https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2018/
- Mendoza, M. A. (2017, January 11). Cómo desarrollar y aplicar un programa de seguridad de la información. Retrieved from welivesecurity: https://www.welivesecurity.com/la-es/2017/01/11/desarrollo-programa-de-seguridad-informacion/
- Miao, Y. (2017, May 27). Update: Most Destructive Malware of All Time. Retrieved from OPSWAT: https://www.opswat.com/blog/most-destructive-malware-all-time