THE SHIELD

OCTUBRE 2, 2017

VOLUMEN II, PUBLICACIÓN II

The University of Texas Rio Grande Valley
Information Security Office

El inicio de Otoño

La Oficina de Seguridad Informática de la UTRGV (ISO) espera que el comienzo del nuevo semestre y el año académico le vaya bien a usted. Desde el comienzo del semestre de otoño el campo de seguridad cibernética ha estado muy ocupado. El número de fraudes y malware aprovechando los usuarios de medios de comunicación social y las plataformas está en aumento. Del mismo modo, los ataques de phishing y las violaciones de datos tuvieron lugar a principios de septiembre. publicación

A continuación, examinaremos algunas maneras en que usted puede mantener sus cuentas escolares, personales y de redes sociales más seguras a través de prácticas en línea inteligentes.

Cómo Identificar Ataques

- Oportunistas - Puede haber actividades cibernéticas malintencionadas que buscan capitalizar el interés por huracanes, terremotos u otros desastres naturales (por ejemplo, el huracán Harvey)
- URLs reducidas - Éstas son tácticas comunes usadas por los scammers para ocultar donde los acoplamientos malévolos llevan puesto que algunos sitios sociales de los medios tienen un límite del carácter. Los vínculos utilizarán servicios de reducción de URL para ocultar el verdadero destino de enlace: un sitio malicioso que puede infectar su dispositivo.
- Cupones falsos - Los estafadores crean un cupón falso que requiere que haga clic en un enlace para descargarlo y poner el cupón en un sitio web malicioso que puede infectar su dispositivo con malware.
- Clics maliciosos - Haga clic en cebo es cuando hay un "teaser" para que haga clic en el enlace. Por ejemplo, podría sugerir una promesa de un "regalo". Esta es otra manera de un estafador puede obtener su información o instalar malware en su computadora.

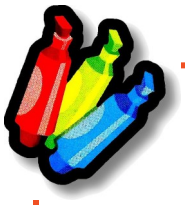
Cómo prevenir ataques

Si recibe un correo electrónico sospechoso o encuentra una publicación cuestionable en las redes sociales, por favor:

- No haga clic en ningún vínculo o enlace abreviado
- Nunca responda con información personal (por ejemplo, nombres de usuario, contraseñas, etc.)
- Tenga cuidado al abrir archivos adjuntos de correo electrónico
- Verifique la legitimidad de cualquier solicitud de correo electrónico poniéndose en contacto con la organización directamente a través de un número de contacto de confianza.

INSIDE THIS ISSUE:

EDITOR
Francisco Tamez
Security Analyst



AVISOS DE SEGURIDAD

El Departamento de Seguridad Nacional de los Estados Unidos (DHS) emite una directiva operacional obligatoria sobre los productos Kaspersky

El 13 de septiembre de 2017, el Departamento de Seguridad Interna de los Estados Unidos (DHS) publicó la Directiva Operacional Obligatoria (BOD) 17-01, ordenando a las agencias federales que eliminaran o discontinuaran el uso de productos, soluciones y servicios proporcionados por AO Kaspersky Lab o entidades relacionadas. La DBO ordena que las agencias federales identifiquen los productos de Kaspersky Lab en los sistemas de información federales dentro de los próximos 30 días, desarrollen planes detallados para remover y descontinuar el uso de los productos dentro de 60 días e implementar esos planes de remoción / interrupción dentro de 90 días. Esto sigue a la decisión del 11 de julio de 2017 de la Administración de Servicios Generales (GSA) de quitar a Kaspersky Lab de su lista de proveedores aprobados debido a presuntos vínculos entre la compañía y los servicios de inteligencia rusos.
bit.ly/CISecurity-DHS-BOD

Gestores de contraseñas

Uno de los pasos más importantes para protegerte en línea es utilizar una clave única y fuerte para cada una de tus cuentas y aplicaciones. Desafortunadamente, es muy probable que no puedas recordar todas tus contraseñas para tus diferentes cuentas. Esta es la razón por la cual tantas personas reutilizan la misma.

Desafortunadamente, la reutilización de tus llaves de acceso para diferentes cuentas es peligrosa porque una vez que alguien compromete tu contraseña, puede acceder a todas tus otras cuentas que utilizan la misma. Una solución simple es usar un gestor, a veces llamado "bóveda de contraseñas". Estos son programas que almacenan de forma segura todas tus claves, por lo que es fácil tener una iferente para cada cuenta. Los gestores de contraseñas hacen esto sencillo porque en lugar de tener que recordar todas tus llaves de acceso, solo tienes que recordar una.
bit.ly/SANSSeptemberN

Huracán Harvey estafas de Phishing

US-CERT advierte a los usuarios que deben permanecer vigilantes por actividades cibernéticas malintencionadas que buscan capitalizar el interés en el Huracán Harvey. Se aconseja a los usuarios que tengan cuidado al manejar cualquier correo electrónico con línea de asunto, adjuntos o hipervínculos relacionados con el huracán Harvey, aunque parezca que proviene de una fuente de confianza. Los emails fraudulentos suelen contener enlaces o archivos adjuntos que dirigen a los usuarios a sitios web de phishing o malware. Los correos electrónicos que solicitan donaciones de organizaciones de caridad duplicadas aparecen comúnmente después de grandes desastres naturales.
bit.ly/US-CERT-HarveyPhishing

Equifax Violación de datos: 143 consumidores estadounidenses afectados

Durante la violación de datos de Equifax, la información a la que se accedió incluye principalmente nombres, números de Seguro Social, fechas de nacimiento, direcciones y, en algunos casos, números de licencia de conducir. Los delincuentes también accedieron a números de tarjetas de crédito para aproximadamente 209.000 consumidores estadounidenses, y ciertos documentos de disputa con información de identificación personal para aproximadamente 182,000 consumidores estadounidenses.
www.equifaxsecurity2017.com/frequently-asked-questions/

Software con fin de vida

EOL Software
Las aplicaciones de software tienen un ciclo de vida. El ciclo de vida comienza cuando el software se libera y termina cuando ya no es compatible con el proveedor, también llamado Fin de vida (EOL por sus siglas en inglés). Cuando el software deja de ser soportado por el proveedor, ya no recibe actualizaciones de seguridad.

EOL OS
Windows XP y Apple OSX 10.8 y anteriores son EOL. Si actualmente utiliza uno de estos sistemas operativos (OS por sus siglas en inglés) de EOL, debe actualizar su sistema operativo para mantener la seguridad de su computadora y sus datos. Las computadoras pertenecientes, arrendadas o administradas por UTRGV deben cumplir con el estándar de seguridad informática (bit.ly/UTRUTRGVISOComputerSecurityStandard), que requiere que ejecuten sólo sistemas operativos compatibles con proveedores. Vista será EOL en Abril del 2017, por lo tanto planee actualizar este sistema operativo pronto.

Actualice si está utilizando versiones **anteriores** de cualquiera de los siguientes productos:

Producto	Versión	Producto	Versión	Producto	Versión	Producto	Versión
Windows	8	MacBook Pro	OS X 10.7	Java SE	8	Firefox	55.0.2
Windows	8.1	Adobe Flash Player	26.0	iPhone	iOS 8.1	Google Chrome	60.2
Windows	7	Adobe Reader	2017.012	Android	Jelly Bean	Internet Explorer	11
Windows	10	Adobe Acrobat X	2017.012				
iMac	OS X 10.7						

Para actualizar correctamente al sistema operativo más reciente, necesitará los siguientes requisitos de sistema. En el caso de que el hardware del equipo no sea capaz de soportar el último sistema operativo, entonces de acuerdo con el estándar de seguridad informática, el equipo tendrá que pasar por el excedente y una nueva con hardware capaz tomará su lugar.

Si utiliza para su actividad laboral una computadora que es propiedad universitaria con un sistema operativo con EOL, inicie sesión en my.utrgv.edu y envíe un ticket a través de Service Now o póngase en contacto con IT Service Desk lo antes posible.

Brownsville / Harlingen / Isla del Padre Sur 956-882-2020
Edinburg / McAllen / Río Grande City 956-665-2020

Una recomendación amistosa para estudiantes, maestros y empleados de UTRGV que utilizan computadoras personales o portátiles: revise los siguientes requisitos de sistema, inicie sesión en my.utrgv.edu, visite la aplicación vSoftware y compre ($ 9.95 USD) Windows 10; Es muy recomendable que realice una copia de seguridad de todos sus archivos, fotos y otros documentos importantes antes de actualizar su sistema operativo. En el caso de que su computadora personal no sea compatible con el sistema operativo, considere actualizar su máquina.

Para obtener una lista con más software EOL, visite: bit.ly/list-EOL2017

ESCRITORIO LIMPIO

BUENA SEGURIDAD

PRÁCTICA

Un ejemplo de mala práctica

Una práctica de escritorio limpio asegura que todos los materiales confidenciales o sensibles se eliminan de un área de trabajo y se ponen bajo llave cuando los elementos no se usan o un empleado sale de su estación de trabajo. Es una de las principales estrategias a utilizar cuando se intenta reducir el riesgo de violaciones de seguridad en el lugar de trabajo. Utilice la lista de verificación a continuación para asegurarse de que su área de trabajo (o hogar) es segura, organizada y compatible.

- ☐ Las contraseñas no deben dejarse escritas en ninguna ubicación accesible.
- ☐ Asegúrese de que toda la información confidencial o sensible en forma impresa o electrónica esté segura al final de la jornada de trabajo o cuando usted se haya ido por un período prolongado.
- ☐ Las pantallas de las computadoras (portátiles, tablets, teléfonos, etc.) deben bloquearse cuando el espacio de trabajo esté desocupado.
- ☐ Los dispositivos portátiles, como las tabletas y teléfonos móviles, deben asegurarse en un lugar bajo llave cuando no se estén utilizando o al final de la jornada de trabajo.
- ☐ Los dispositivos de almacenamiento externo, como los CD, DVD o unidades USB, deben protegerse en un almacenamiento bajo llave cuando no estén en uso.
- ☐ File cabinets, drawers and storage lockers containing Confidential or Sensitive information should be kept closed and locked when not in use or not attended.
- ☐ Llaves utilizadas para acceder información confidencial o sensible no deben dejarse en un escritorio desatendido.
- ☐ Todas las impresoras y máquinas de fax deben ser despejados de los papeles tan pronto como se impriman; Esto ayuda a garantizar que los documentos confidenciales o sensibles no se dejan atrás para que la persona equivocada los recoja.
- ☐ Tras la eliminación*, los documentos confidenciales y / o sensibles deben ser triturados o colocados en contenedores confidenciales bajo llave.

**Aseúrese de que las políticas de gestión y retención de registros de UTRGV se sigan al deshacerse de cualquier registro oficial de UTRGV [HOP ADM-10-102]*

Seguridad Cibernética Expo 2017

Octubre es el mes nacional de concientización sobre seguridad cibernética (NCSAM).

En apoyo del Departamento de Seguridad Nacional (DHS) y el Stop.Think.Connect. , la Universidad de Texas Río Grande Valley y la Oficina de Seguridad de la Información están orgullosos de promover NCSAM y la importancia de la seguridad en línea.

A lo largo del mes de octubre, destacaremos la ciberseguridad en nuestro sitio web y en nuestros medios de comunicación social. Esperamos que se unan a nuestros esfuerzos para promover este tema y esperamos que pueda asistir a nuestra Expo de Seguridad Cibernética que se llevará a cabo el:

- Octubre 17, 2017 – Edinburg Student Union de 11:00 am to 2:00 pm
- Octubre19, 2017 – Brownsville Salon Cassia (BMAIN 2.402) de 11:00 am to 2:00 pm

En la Expo, usted encontrará:

- Consejos útiles y recursos que ayudarán a crear conciencia sobre la ciberseguridad
- Mapa en vivo de ataques cibernéticos
- Juegos + premios gratis
- Presentaciones y webinars

Para inscribirse necesitará:

1. Haga clic en el botón "registrar"
2. Si usted es:
    - Afiliado a la universidad, a continuación, iniciar sesión con su nombre de usuario UTRGV y contraseña
    - No afiliado a la universidad, a continuación, haga clic en "registrarse para una nueva cuenta"
1. Buscar la Expo 2017

NOTA: Asegúrese de registrarse en el campus al que puede asistir.

REGISTER

https://webapps.utrgv.edu/it/training/

¡Guarde la fecha y no olvide traer su tarjeta de identificación UTRGV!
Gracias,

La Oficina de Seguridad Informática

Cont'd from page 5

ROBO DE IDENTIDAD

EL ROBO DE IDENTIDAD es un **crimen** en el que un ladrón roba su información personal, como su número de seguro social, para cometer fraude. El ladrón de identidad puede usar su información para::

- Aplicar fraudulentamente crédito
- Falsificar impuestos
- Obtener servicios medicos

Estos actos pueden dañar su estado de crédito, y le costará tiempo y dinero para restaurar su buen nombre. Es posible que no sepa que es víctima de un robo de identidad hasta que experimente una consecuencia financiera (cuentas de misterio, cobros de crédito, préstamos denegados) en el camino de las acciones que el ladrón ha tomado con su identidad robada.

Protección de su identidad

Alertas de servicio activo: agregue una capa adicional de protección a los registros de crédito de los miembros del servicio mientras se despliegan.

Preguntas frecuentes sobre el congelamiento del crédito

Servicios de Protección contra Robo de Identidad- Otros servicios que usted puede comprar.
www.consumer.ftc.gov/topics/identity-theft

Prevenir el robo de identidad

Tome medidas para protegerse contra el robo de identidad:

- Asegure su Número de Seguro Social (SSN). No lleve su tarjeta de seguro social en su billetera o escriba su número en sus cheques. Solamente dé su SSN cuando sea absolutamente necesario.
- No responda a la solicitud no solicitada de información personal (su nombre, fecha de nacimiento, SSN o número de cuenta bancaria) por teléfono, correo o en línea.
- Guarde la información personal en un lugar seguro en su casa.
- Revise su tarjeta de crédito y sus estados de cuenta bancaria. Compare rápidamente los recibos con los estados de cuenta. Observe las transacciones no autorizadas.
- Crate una contraseña fuerte que los ladrones de identidad no pueden adivinar fácilmente. Cambie sus contraseñas si una empresa con la que hace negocios tiene un incumplimiento de sus bases de datos.
- Revise su informe de crédito una vez al año para estar seguro de que no incluye cuentas que no ha abierto. Puede solicitarlo gratuitamente en www.annualcreditreport.com
  - ⇒ La ley federal le permite obtener una copia gratuita de su informe de crédito cada 12 meses de cada compañía de informes de crédito.

VIOLACÍON DE DATOS

Si usted tiene un informe de crédito, hay una buena probabilidad de que sea uno de los 143 millones de consumidores estadounidenses cuya información personal sensible fue expuesta en una violación de datos en Equifax, una de las tres principales agencias de informes crediticios del país.
Hay pasos a seguir para ayudar a proteger su información de ser mal utilizada. Visite el sitio web de Equifax, www.equifax.com

- ♦ Haga clic en la pestaña "Impacto potencial" e ingrese su apellido y los últimos seis dígitos de su número de Seguro Social.

Estos son algunos otros pasos a seguir para protegerse después de un incumplimiento de datos:

- **Revise sus informes de crédito**
- **Considere colocar un congelamiento de crédito** en sus archivos. Un congelamiento de crédito dificulta que otra persona abra una nueva cuenta a su nombre. Tenga en cuenta que un congelamiento de crédito no impedirá que un ladrón haga cargos a sus cuentas existentes.
- **Monitoree cuidadosamente su cuenta de tarjeta de crédito y sus cuentas bancarias existentes** para ver los cambios que no reconoce
- **Coloque una alerta de fraude en sus archivos.** Una alerta de fraude advierte a los acreedores que usted puede ser una víctima de robo de identidad

Enlaces Útiles

Federal Trade Commission (FTC)
www.ftc.gov
www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do
www.consumer.ftc.gov/topics/identity-theft
www.consumer.ftc.gov/features/feature-0014-identity-theft

USA.gov
www.usa.gov/identity-theft
IdentityTheft.gov
www.identitytheft.gov/

¿Tienes una idea para un tema? ¿Desea incluir algo en particular en este boletín?
¡Cualquier comentario o sugerencia son SIEMPRE bienvenidos!

Siéntase libre de enviar su feedback visitando nuestro sitio web:
www.utrgv.edu/is/en-us/news-and-alerts/newsletter/newsl-feedback/


DON'T
GET
SMACked
Check your
Social Media
Access Controls
utrgv.edu/is/en-us/
resources/social-media


CyberAware
HAPPY
#CYBERAWARE
MONTH
STAYSAFEONLINE.ORG/NCSAM
National Cyber Security
Awareness Month
STOP | THINK | CONNECT

Si necesitas reportar un incidente:

Visite nuestro sitio web (www.utrgv.edu/is) si necesita reportar un incidente de seguridad . Algunos incidentes pueden requerir informar tanto a la ISO y al Departamento de Policía de UTRGV (PD) o de tecnología de la información (IT) . Por ejemplo, cualquier pérdida o robo de una computadora de propiedad de la Universidad (ej. estación de trabajo, ordenador portátil, celular, tableta) tiene que ser reportado a la ISO y a UTRGV PD. Del mismo modo, en caso de computadoras infectadas con ransomware deben de ser reportadas a ISO y a IT.

REPORTA UN INCIDENTE

The University of Texas Rio Grande Valley™

Information Security Office

La misión de la Oficina de la Seguridad Informática es proporcionar apoyo a la Universidad en la logro de sus objetivos, garantizando la seguridad, integridad, confidencialidad y disponibilidad de los recursos de información.

Oficinas:

- Sugar Road Annex (ESRAX) Building
- R-167 Rusteberg Hall (BRUST) Building (*by appointment*)

Teléfono: (956)665-7823

Email: is@utrgv.edu

Visitanos en la web y en las redes sociales!
www.utrgv.edu/is www.facebook.com/utrgviso

Servicios que proporionamos:

CONCIENCIA, RIESGO Y CUMPLIMIENTO

ADMINISTRACIÓN DE LAS VULNERABILIDADES

INGENIERÍA Y RESPUESTA A INCIDENTS

CONCIENCIA, COMUNICACIÓN Y DIFUSIÓN

¡Danos tu opinion!
bit.ly/utrgvisonewsletterfeedback