THE SHIELD

MARZO 12, 2018

VOLUMEN II, PUBLICACIÓN IV

The University of Texas Rio Grande Valley
Information Security Office

¡Tómate un descanso!

¡Esta primavera, esperamos que pueda tomarse un descanso y relajarse! La primavera es la estación perfecta del año para pasar por proyectos sin terminar, hacer una limpieza de primavera, relajarse con amigos y familiares, y esperar ansiosamente lo que traerá el verano. Para este problema, la Oficina de Seguridad de la Información (ISO) lo invita a considerar tomarse unos minutos para revisar los recursos de su computadora, la vida digital, ¡y también les da un buen descanso!
Siga estos consejos que lo guiarán para refrescar y renovar su vida cibernética, y recuerde compartirlos con sus amigos y familiares:

Limpia tus dispositivos:

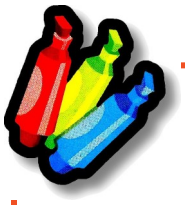
- ¡Los teléfonos inteligentes, tabletas, computadoras portátiles y computadoras requieren mantenimiento y la limpieza de primavera es la oportunidad perfecta para hacerlo! Borre las aplicaciones o el software no utilizado y borre todas las descargas que ya no esté utilizando. Compruebe si hay archivos antiguos que se pueden archivar o eliminar. Asegúrese de que el software de seguridad de su dispositivo funcione correctamente y de que todo el software esté parcheado y configurado para su actualización automática. ¡Recomendamos encarecidamente que haga una **copia de seguridad** de sus archivos e imágenes antes de actualizar su computadora!
- Por último, pero no menos importante, saca la basura. Literalmente. Las trituradoras de corte cruzado son la elección perfecta para triturar papeles sensibles. Además, puede haber dispositivos viejos en su casa u oficina que puedan reciclarse. Todos los discos duros de la computadora UTRGV deben eliminarse y desinfectarse para garantizar que cualquier información delicada o confidencial que contenga se borre de forma permanente e irrecuperable antes de que la computadora pueda enviarse al excedente.

Limpia tus cuentas digitales:

- Correo electrónico: las cuentas de correo electrónico recopilan desorden y puede haber información en sus cuentas que puede archivar en carpetas o eliminar. Una gran idea es establecer reglas, mediante el uso de reglas puede reducir las acciones manuales y repetitivas, estas pueden ayudarlo a mantenerse organizado. Haga todo lo posible para vaciar los elementos eliminados o la carpeta de la papelera de forma periódica.
- Redes sociales: Spring limpie sus cuentas de redes sociales siguiendo nuestra campaña "No recibir SMACKed". Revise la configuración de privacidad y seguridad en los sitios web que usa para asegurarse de que estén a su nivel de comodidad para compartir. Está bien limitar cómo y con quién compartir información.

EN ESTA EDICIÓN:

EDITOR
Francisco Tamez
Security Analyst



AVISOS DE SEGURIDAD

Las fallas críticas revelaron que afectan a la mayoría de los chips Intel desde 1995

En enero de 2018, los investigadores de seguridad revelaron los detalles largamente esperados de dos vulnerabilidades en procesadores Intel que datan de más de dos décadas. Estas dos vulnerabilidades críticas que se encuentran en los chips Intel pueden permitir que un atacante robe datos de la memoria de aplicaciones en ejecución, como datos de administradores de contraseñas, navegadores, correos electrónicos y fotos y documentos.

Los investigadores que descubrieron las vulnerabilidades, apodado "Meltdown" y "Spectre", dijeron que "casi todos los sistemas", desde 1995, incluyendo computadoras y teléfonos, se ven afectados por el error.

Los federales le cobran al creador de 'Fruitfly' por hackear miles de computadoras

El gobierno afirma que Phillip R. Durachinsky, de 28 años, ejecutó un plan de 13 años desde el 2003 hasta el 20 de enero de 2017 que infectó miles de computadoras con malware denominado "Fruitfly". Fruitfly, que atacó computadoras Mac, permitió a Durachinsky tomar el control completo de una computadora que enciende secretamente las cámaras y micrófonos para grabar video y audio.

¿Eres un Phish?

El phishing es una forma de fraude en el que el cibercriminal intenta aprender información engañándote como una entidad o persona confiable por correo electrónico, sitios web y llamadas telefónicas.

Cosas que debe buscar en los correos electrónicos:

- ¡Cuidado con los enlaces en los correos electrónicos! NUNCA haga clic en ellos.
- NUNCA descargue ni abra ningún archivo adjunto.
- Pase el mouse sobre los enlaces: simplemente coloque el mouse sobre el enlace para ver la dirección web. (Los enlaces también pueden llevarlo a archivos .exe. Se sabe que este tipo de archivos propaga software malicioso).
- Amenazas pueden ser incluidas. Por ejemplo:
    - ◊ "Su cuenta estaría cerrada si no responde con su nombre de usuario y contraseña".
    - ◊ Los estafadores utilizan gráficos en correos electrónicos que parecen estar conectados a sitios web legítimos.

Las redes sociales y la ingeniería utilizadas para difundir Tempted Cedar Spyware

Los ciberdelincuentes están utilizando las redes sociales y la ingeniería social para engañar a las víctimas y descargar el spyware Advance Persistent Threat disfrazado como la aplicación de mensajería Kik.

El spyware llamado "Tempted Cedar Spyware" está diseñado para robar información como contactos, registros de llamadas, SMS y fotos, así como información del dispositivo, como la geolocalización para rastrear usuarios y era capaz de grabar los sonidos circundantes, incluidas las conversaciones que las víctimas tenían mientras su teléfono estaba dentro del alcance

Estafa secuestra navegador Google Chrome, intenta obtener sus datos personales

Las estafas que secuestran al navegador más popular del mundo, Google Chrome, están circulando de nuevo. Comienza con un mensaje de error falso. Para los usuarios de computadoras, este es un problema molesto porque el código malicioso subyacente bloquea el navegador. "El error que desencadena es más que una molestia en el sentido de que hará que su navegador Chrome no responda", dijo a Fox News Jerome Segura, analista de inteligencia de Malwarebytes.

Estas y más noticias se pueden encontrar en: bit.ly/UTRGVisoNews

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:

Supported Products

Product	Version	Product	Version	Product	Version	Product	Version	Product	Version
Windows	7	OS X 10.11	El Capitan	Adobe Flash Player	26.0	Android	Jelly Bean	Java SE	8
Windows	8	OS X 10.12	Sierra	Adobe Reader	2017.012	iPhone	iOS 9.1	Internet Explorer	11
Windows	8.1	OS X 10.13	High Sierra	Adobe Acrobat X	2017.012			Google Chrome	60.2
Windows	10							Firefox	55.0.2

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]*

Día de privacidad de datos 2018

Por StafSafeOnline.org Data Privacy Day 2018 INFORMACIÓN GENERAL SOBRE LOS MEDIOS

Dirigido por la Alianza Nacional de Seguridad Cibernética (NCSA) en los Estados Unidos, el Día de Privacidad de Datos - celebrado cada año, el 28 de enero, conmemora la firma en 1981 del Convenio 108, el primer tratado internacional legalmente vinculante que trata de la privacidad y la protección de datos. Lanzado en Europa y adoptado en Norteamérica en 2008, Data Privacy Day reúne a empresas y ciudadanos privados para compartir las mejores estrategias para proteger la información privada de los consumidores.
Después de un año de violaciones masivas de datos en lugares como Equifax, Verizon, la NSA y Uber, es necesario que las personas aprendan cómo proteger mejor su información personal. Y con el 68 por ciento de los consumidores que dicen que no confían en que las marcas manejen su información personal de manera apropiada, el Día de privacidad de datos también alienta a las empresas a ser más transparentes sobre cómo recopilan y usan los datos.

POR QUÉ NOS DEBERÍAMOS PREOCUPAR POR LA PRIVACIDAD EN LÍNEA

Producimos una corriente de datos casi infinita en nuestra vida cotidiana. El 77% de los estadounidenses ahora posee teléfonos inteligentes, un aumento del 35% en 2011. Hoy llevamos a cabo gran parte de nuestras vidas en Internet y en nuestros dispositivos conectados, pero pocas personas entienden la enorme cantidad de información personal que se recopila y comparte desde nuestros dispositivos y los servicios que utilizamos en línea. Esta información puede almacenarse indefinidamente y nuestra información personal puede ser utilizada tanto de manera beneficiosa como no deseada. Incluso la información aparentemente inocuo, como sus restaurantes favoritos o los artículos que compra en línea, se puede utilizar para hacer inferencias sobre su estado socioeconómico, preferencias y más. La ausencia de fuertes leyes de protección al consumidor en línea en los EE. UU. Significa que muchas empresas tienen la oportunidad de monitorear el comportamiento personal de sus usuarios y clientes y vender los datos con fines de lucro. Los consumidores deben comprender el verdadero valor de su información y cómo se recopila, utiliza y comparte para tomar decisiones informadas y gestionar mejor sus datos personales.

¿CUÁL ES LA DIFERENCIA ENTRE LA PRIVACIDAD Y LA SEGURIDAD?

La seguridad se refiere a las formas en que nos protegemos a nosotros mismos, a nuestra propiedad e información personal. Es el primer nivel de defensa contra intrusos no deseados. La privacidad es nuestra capacidad para controlar el acceso a nuestra información personal. Aunque la Constitución de EE. UU. No define explícitamente la privacidad, las leyes de los EE. UU. Han llegado a reconocer que las personas tienen derecho a la privacidad en muchos contextos diferentes.

Las redes sociales como Snapchat, Facebook, Twitter, Instagram y LinkedIn son recursos increíbles que permiten conocer, interactuar y compartir con personas de todo el mundo. Sin embargo, con todo este poder, existen riesgos, no solo para ti, sino también para tu familia, amigos y relaciones de trabajo. En este boletín cubriremos los pasos clave para aprovechar al máximo las redes sociales de forma segura y sin peligros.

- Publicaciones—Ten cuidado y piensa antes de publicar algo. Todo lo que posteas se hará público en algún momento, lo que afectará tu reputación y futuro, incluso podría afectarte en la escuela a la que podrías asistir o los trabajos que podrías obtener. Si no deseas que tu familia o jefe lo vea, probablemente no debas publicarlo. También ten en cuenta lo que otros publican sobre ti. Puede ser que tengas que pedir a otros que eliminen lo que comparten sobre ti. Privacy—Almost all social media sites have strong privacy options. Enable them when possible. For example, does the site really need to be able to track your location? In addition, privacy options can be confusing and change often. Make it a habit to check and confirm they are working as you expect them to.

- Privacidad—Casi todos los sitios de redes sociales tienen opciones sólidas sobre privacidad, habilítalos cuando sea posible. Por ejemplo, ¿el sitio realmente necesita saber tu ubicación en todo momento? Además, las opciones de privacidad pueden ser conusas y cambian a menudo. Acostúmbrate a verificar y confirmar que están funcionando como realmente esperas.

- Frase de contraseña—Asegura tu cuenta de redes sociales con una frase de contraseña larga y única. Una frase de contraseña está compuesta por varias palabras, lo que te permite escribirla y recordarla fácilmente, pero es difícil de adivinar por los atacantes cibernéticos.

- Bloqueo de la cuenta—Aún mejor, habilita la autenticación de dos factores en todas tus cuentas. Esto agrega un código de un solo uso que se solicita en conjunto con tu contraseña cuando inicias sesión en tu cuenta. Esto es realmente simple y es una de las formas más poderosas de proteger tu cuenta.

- Estafas—Al igual que por correo electrónico, los actores maliciosos intentarán engañarte usando mensajes a través de las redes sociales. Por ejemplo, pueden intentar engañarte para obtener tu contraseña o información de tu tarjeta de crédito. Ten Consejos para el uso seguro de redes sociales cuidado en lo que das clic: si un amigo te envía lo que parece ser un mensaje extraño o no suena como ellos, podría ser un atacante cibernético que intenta hacerse pasar por tu amigo.

- Términos de los servicios—Conoce los términos de servicio de los sitios. Todo lo que publiques o subas a las redes sociales puede convertirse en propiedad del sitio.

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país. Sitio web: http://www.seguridad.unam.mx Síguelo en Twitter @unamcert

¿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/

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