ISO
BOLETÍN

www.utrgv.edu/is

The University of Texas Rio Grande Valley™
Information Security Office

VOLUMEN I, PUBLICACIÓN IV MARZO 9, 2017

DENTRO DE ESTA PUBLICACIÓN:



EDITOR
Francisco Tamez
*ISO Security Analyst*

# Spring Break!

¡La Oficina de Seguridad Informática de UTRGV (ISO por sus siglas en inglés) desea desearte unas vacaciones de primavera excelentes y seguras! Prepárate para descansar y no olvides tomar decisiones educadas antes de empacar tus maletas y salir.

Sigue estos consejos de seguridad y recuerda compartirlos con tus amigos y familiares.

**1. Viajando**

- Para viajes por carretera recuerde: **NUNCA** deje objetos de valor en su automóvil (por ejemplo, celulares, iPads, laptops, etc.)
- Mientras espera a que llegue su avión, siempre sea consciente de su entorno y nunca deje sus maletas, laptop o iPad desatendido.
- En los aeropuertos sea precavido y no confíe en los cargadores públicos para celulares, el cable podría utilizarse para transferir y sincronizar sus datos a un delincuente, a esto se le conoce como "juice jacking". Para obtener más información sobre "juice jacking" visite: www.howtogeek.com/166497/
- Si se conecta al Wi-Fi del aeropuerto **NUNCA** realice transacciones financieras, envíe emails importantes, etc. ¡Este tipo de Wi-Fi público la mayoría del tiempo es inseguro y riesgoso!
- Mantenga una lista de su pasaporte o número de tarjeta de crédito, o tarjeta de débito en su casa con información de contacto de la organización correspondiente. Esto hará más fácil reportar estos artículos en caso de que sean robados.

**2. Quedándote en un hotel**

- ¡Sea cauteloso! Trate su internet del hotel como cualquier otra conexión Wi-Fi pública. Vea nuestro artículo de seguridad informática ¿"Wi-Fi gratuito es seguro?" Para obtener más información.
- Sea discreto mientras se registra en la recepción. Nadie fuera de su grupo de amigos necesita saber el número de su habitación.
- En su habitación recuerde comprobar que todas las ventanas y cerraduras de las puertas son seguras.
- Siempre cierre la puerta firmemente al entrar o salir de su habitación. ¡Algunas puertas tienen una liberación lenta y podrían permanecer abiertas!
- La mayoría de los hoteles ofrecen cajas fuertes. ¡Úsalos! Almacene artículos valiosos o artículos que sean fácil robar (por ejemplo, iPad, joyería, laptop, pasaporte, etc.) mientras que usted está fuera del hotel.

**3. No seas SMACked**

- ¡Comprueba tu configuración de privacidad en las redes sociales!
- Se precavido sobre lo que usted publica sobre otros y recuerde que las imágenes en línea duran toda la vida

# AVISOS DE SEGURIDAD

**¡Estafas de impuestos!**

El Internal Revenue Service (IRS, por sus siglas en inglés), las agencias tributarias estatales y la industria tributaria emitieron una alerta urgente a todos los empleadores de estafas del formulario W-2 ha evolucionado más allá del mundo corporativo y se está extendiendo a otros sectores, incluyendo el sector educativo. Los estafadores están combinando sus esfuerzos para robar información de los empleados, tales como su número de Seguro Social (SSN), fecha de nacimiento, depósito directo, y ¡mucho más!

Así es como funciona la estafa: Los delincuentes usan varias técnicas de spoofing para disfrazar un correo electrónico (a esta técnica se le conoce como phishing) para que aparezca como si fuera de un ejecutivo de la organización. El correo electrónico se envía a un empleado de la nómina o departamentos de recursos humanos, solicitando una lista de todos los empleados y sus W-2.

La estafa W-2 es sólo una de varias nuevas variaciones que han aparecido en el año pasado que se centran en los robos a gran escala buscando información fiscal de los preparadores de impuestos, empresas y compañías de nómina. Los contribuyentes individuales también pueden ser blancos de estafas de phishing, pero los delincuentes parecen haber desarrollado sus tácticas para centrarse en robos de datos masivos.

**Es usted un Phish?**

El phishing es una forma de fraude en la que el delicuente trata de aprender información engañándote como una entidad o persona de confianza a través de correo electrónico, sitios web o llamadas telefónicas.

Cosas que puedes hacer en este tipo de correos electrónicos:

- ¡Cuidado con los enlaces en los correos electrónicos! **NUNCA** haga clic en ellos.
- **NUNCA** descargue ni abra ningún archivo adjunto.
- Pasa el mouse sobre los enlaces: Simplemente coloca el mouse sobre el enlace para ver la dirección web. (Los vínculos también podrían llevarte a archivos .exe. Estos tipos de archivos son conocidos por propagar software malicioso.)
- Pueden incluir amenazas. Por ejemplo:
  - ◊ "Su cuenta se cerrará si no responde con su nombre de usuario y contraseña."
- Los estafadores utilizan imagenes en correos electrónicos que parecen estar conectados a sitios web legítimos.

Si recibe un correo electrónico con su dirección de correo electrónico UTRGV y usted sospecha que puede ser un mensaje de phishing, envíe un correo electrónico a: itdns@utrgv.edu

Para obtener más información sobre cómo denunciar un mensaje de phishing, siga estas instrucciones del sitio web de IT: www.utrgv.edu/it/how-to/report-phishing-messages

Para obtener más información sobre el phishing, visite: www.utrgv.edu/is/en-us/resources/trainings/phishing-page/

# ¿Que aguarda este Semestre?

**Solución de cifrado para Mac**

La versión actualmente instalada de SecureDoc, la solución de administración de cifrado de UTRGV para Mac OSX, no es compatible con la última versión de OSX Sierra. IT está investigando una mejor solución para gestionar el cifrado OSX y la administración de estas Macs, incluyendo OSX e iOS.

**Retiro de dominios UTB y UTPA**

Las credenciales UTPA y UTB se retirarán este verano y ya no podrás iniciar sesión con estos dominios heredados. En el caso de que todavía usted está utilizando estas credenciales, póngase en contacto con el Centro de ayuda de IT.

## 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.

**Apple QuickTime para Windows**

Apple anunció que ya no admitirá QuickTime para Windows. Los equipos con Windows instalados con QuickTime pueden ser vulnerables al malware. La ISO recomienda que todos los usuarios de Windows desinstalen QuickTime inmediatamente.

**Productos EOL del día de hoy**

Actualice si está utilizando los siguientes productos con estas versiones o anteriores.

| Producto | Versión | Producto | Versión |
|---|---|---|---|
| Windows | 8.0 | Adobe Acrobat | 9.x |
| Safari for Windows | Any | Adobe Flash Media | 4.5 |
| Adobe Acrobat X | 10 | Adobe Flash Player | 19 |
| Adobe Reader | 9.x | Java SE | 7 |

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

# ISO destacó a:

ISO destacó a: es una entrevista de un individuo que forma parte de UTRGV o juega un rol en la seguridad informática. En este boletín, conoceras a Cesar Pastore, *Information Security Analyst*.

***Cesar Pastore* MBA**
***Information Security Analyst***
**The University of Texas Rio Grande Valley**

**1. ¿Cómo es que llegaste al campo de seguridad informática?**
Llegué al campo de seguridad a través de mi trabajo como administrador de sistemas, analista de negocios y análisis de datos.

**2. Los tres logros mas importantes en su vida:**
- Conseguir mi primer trabajo a tiempo completo después de la universidad.
- Cuando recortaron personal en mi trabajo y me despidieron (aunque no lo creas esto te enseña mucho)
- Mudarme a Texas desde California.

**3. La gente se sorprendería saber que:**
Crecí en la costa oeste de California.

**4. ¿Qué CD tiene usted en su coche? ¿O qué estación de radio te gusta escuchar?**
Escucho a NPR.

**5. Si pudieras entrevistar a una persona (viva o muerta) ¿quién sería?**
Me entrevistaría con mis padres o abuelos a mi edad. De la misma manera, me gustaría poder entrevistar a mis hijos o nietos a mi edad.

**6. ¿Si se le da la oportunidad, quien le gustaría ser por un día?**
Cualquier persona con la que he estado en desacuerdo, creo que ganar perspectiva es algo importante en la vida.

**7. ¿Cuál es el mejor consejo que has recibido y que ha utilizado?**
Siempre mantenga un ojo en el futuro y tratar de evitar la dependencia en lo familiar.

**8. ¿Cuál sería su consejo para un nuevo profesional en la seguridad informática?**
Concéntrese en desarrollar habilidades prácticas que le mantendrán relevante en la fuerza de trabajo. No tengas miedo de intentar algo nuevo o de entrar en nuevas áreas de tecnología en las que no tengas antecedentes directos.

## *Artículo destacado*

*Por Jonas Del Angel*
*UTRGV Security Analyst*

### Exploit Kits

**¿Qué es?**

Los kits de explotación son un término relativamente desconocido en los entornos empresariales actuales. En pocas palabras, los kits de explotación son herramientas utilizadas por los delincuentes cibernéticos para explotar las vulnerabilidades de los sistemas informáticos. Analizan su máquina para obtener software anticuado y herramientas de protección de seguridad. Ellos se conocieron por primera vez en 2006 cuando fue descubierto como el método de entrega de exploits en Microsoft Windows, Mozilla Firefox y aplicaciones Java para distribuir malware. Esto generalmente se hace por spam o anuncios comprometidos en sitios web legítimos. Los sitios web que se enfocan en el compromiso incluyen bancos, noticias, foros web, WordPress y otros. Con el tiempo los kits de explotación han evolucionado y son conocidos por proporcionar actualizaciones a sus proveedores que incluyen: exploits para vulnerabilidades recién descubiertas, evasión mejorada de detección de antivirus y métricas de análisis de datos para determinar tasas de éxito de infección. Sin saber que han sido comprometidos debido a las técnicas de evasión utilizadas por los kits para evitar la detección. Sin embargo, generalmente se descubren y se fijan en un día para que ya no puedan infectar a los usuarios.

**¿Cómo se dirige a los sistemas?**

Ransomware se ha convertido en la carga útil favorecida en el uso de hoy de kits de exploit debido a su capacidad de permanecer sin ser detectado por antivirus y su tasa de éxito es extremadamente alta en la infección de máquinas. Al escanear una máquina, estos kits buscan la versión del navegador, complementos de navegador e incluso software antiguo. Cuando se detectan plugins vulnerables, encontrará una vulnerabilidad para usar contra esta vulnerabilidad específica y entregará una carga útil que puede contener malware, troyanos o ransomware. Los destinos de software favorecidos para escanear tienden a incluir plugins de Adobe Flash Player, Adobe Reader y Java desactualizados. Todo este proceso se produce sin el conocimiento del usuario porque la descarga e instalación se produce en segundo plano mediante el uso de un marco web oculto después de que se haya detectado una vulnerabilidad. Si no se encuentran vulnerabilidades o si las herramientas de software de seguridad son suficientes, el kit exploit ignorará la máquina y buscará otro objetivo. (bit.ly/2IV908J)

**Conciencia**

Una de las principales razones por las que los kits de explotación continúan evolucionando se debe a los datos analíticos recogidos de los kits de exploits que indican que los usuarios siguen siendo víctimas de un ransomware que se considera altamente rentable. El método furtivo de descargar e instalar el malware cuando se realiza como una unidad de descarga también añade a su éxito ya que se produce sin que el usuario sea consciente.

**¿Qué pasa con los usuarios de Mac OS X y Linux?**

Uno normalmente piensa que las posibilidades serían significativamente más bajas si cualquiera de estos son sus sistemas operativos preferidos. Sin embargo, debido a que los kits de exploit están aprovechando los navegadores web para escanear máquinas y entregar software malicioso, cualquier sistema operativo es un objetivo. Las vulnerabilidades de Adobe Flash Player se encuentran entre las más altas para la mayoría de los éxitos según los informes de tendencias de 2015 y 2016. (bit.ly/23wr6C3)

**Prevención**

Entonces, ¿cómo podemos tomar mejores precauciones para no caer víctima de ransomware que se entregó con un kit de exploit? Algunos consejos básicos de seguridad para estar al tanto de ello sería:

- Mantenga actualizado todo su software, navegadores y complementos.
- Realice un respaldo de sus datos con regularidad en un disco duro externo que no deje regularmente conectado a su máquina.
- Instale el software de bloqueo de anuncios para su navegador web de su elección. Los kits de aprovechamiento a menudo encuentran maneras en las máquinas porque usan anuncios de sitios web como medio de escanear la máquina de destino.

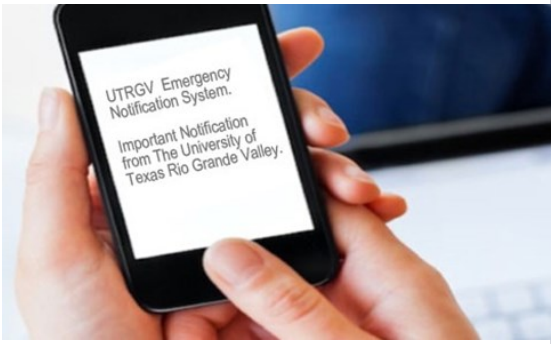
Los kits de explotación son un problema creciente que ha ido en aumento en los últimos años y continúa creciendo. La razón de esto es debido a su uso clave en la entrega de malware y ransomware. Ya no se trata sólo de sospechar de correos electrónicos o archivos adjuntos. Vigilancia contra los correos electrónicos de phishing es sólo una forma de evitar ser víctima de un delito cibernético, el otro significa permanecer fiel a la práctica común de mantener nuestro software actualizado. Más información sobre la protección contra amenazas de seguridad como esta se puede encontrar aquí: (bit.ly/2IZZ5iV)

# ISO - Invitado


## Acerca de UTRGV Preparación para emergencias

La Oficina de Preparación para Emergencias está comprometida con el proceso continuo de preparación, respuesta, recuperación y mitigación de posibles pérdidas por desastres naturales, tecnológicos o causados por el ser humano que puedan afectar negativamente a estudiantes, profesores, personal, visitantes e instalaciones en La Universidad de Texas de El Valle del Río Grande.

## Notificación de Alerta de Emergencia




La comunicación rápida y oportuna a la comunidad universitaria durante las emergencias es crítica. El Sistema de Alerta de Emergencia (EAS por sus siglas en inglés) de UTRGV provee comunicación masiva, urgente y oportuna usando múltiples métodos para notificar rápidamente a los estudiantes, al personal docente y al personal de una emergencia activa o incidente de alto riesgo en el campus principal a través de:

- Correos electrónicos
- Mensajes de texto
- Mensajes de voz
- Alertas por computadoras personales que son propiedad de la Universidad
- Página de Facebook de la Policía Universitaria @UTRGVPoliceDepartment

Los estudiantes, profesores y personal se registran automáticamente en Alertas de Emergencia de UTRGV con la información de contacto contenida en Banner (estudiantes) y Oracle (profesores y personal).

## Notificación de Alerta de Emergencia

Cuando la Policía Universitaria o la Seguridad del Campus determinan que hay una emergencia activa en la cual la seguridad pública de la escuela puede estar en riesgo, se iniciará una notificación urgente a través del Sistema de Alerta de Emergencia de UTRGV. Por ejemplo:

- Cuando hay una persona disparando un arma
- Cuando se pronostica que un tornado o tormenta severa con vientos esperados de más de 70 millas por hora impactará un área del campus
- Cuando un gran derrame de material peligroso o una emergencia de alto riesgo afectan una gran parte del campus

## Medio Ambiente Costero

- Si usted está atrapado en una corriente, mantenga la calma y no luche contra la corriente
- Nade paralelo a la orilla hasta que esté fuera de la corriente. Una vez que esté libre, gire y nade hacia la orilla.
- Manténgase al menos a 100 pies de distancia de los muelles y embarcaderos. A menudo este tipo de corrientes existen cerca de estas estructuras
- En la playa, verifique las condiciones antes de entrar en el agua. Compruebe si hay señales de advertencia o pregúntele a un salvavidas sobre las condiciones del agua, las condiciones de la playa o cualquier otro tipo de peligro

## Seguridad en el agua

- Nadar en áreas designadas bajo la supervisión de salvavidas
- Nunca deje a un niño pequeño desatendido cerca del agua y no confíe en la vida de un niño a otro niño; Enseñe a los niños a pedir permiso para ir cerca del agua
- Si tiene una piscina, asegúrela con las barreras adecuadas. Muchos niños que se ahogan en las piscinas caseras estaban fuera de la vista por menos de cinco minutos y en el cuidado de uno o ambos padres en ese momento
- Disponer de equipos adecuados, tales como chalecos salvavidas y un botiquín de primeros auxilios

## La Oficina de Preparación para Emergencias

Promueve una base para la gestión de emergencias y proporciona el marco para los esfuerzos efectivos de preparación a través del Plan de Operaciones de Emergencia y anexos relacionados;

- Mantiene, desarrolla y alinea metas y objetivos de manejo de emergencia alcanzables con la visión, misión y propósito de La Universidad de Texas de El Valle del Río Grande.
- Define los procedimientos pertinentes a la ejecución del Programa de Manejo de Emergencias;
- Identifica y mantiene buenas relaciones de trabajo con socios de gestión de emergencias internos, externos y con las partes interesadas;
- Fortalece la continuidad y la viabilidad del programa proporcionando capacitación y ejercicios.

## Contacto de La Oficina de Preparación para Emergencias

**Teléfono:** (956)665-2658
**Correo electrónico:** emergencypreparedness@utrgv.edu
**Página web** www.utrgv.edu/emergencypreparedness

## Contactos de Emergencia

**Policía Universitaria**
Brownsville:
(956)882-8232 (principal)
(956)882-2222 (Emergencia)

Edinburg:
(956)665-7151

Harlingen:
(956)882-8232(principal)
(956)882-2222 (Emergencia)

**Medio ambiente salud, seguridad y gestión de riesgos**
(956)882-5930 (Brownsville)
(956)665-3690 (Edinburg)

**Operaciones de Instalaciones**(956)665-2770

**Emergencia 911**

# Asociación estudiantil sobresaliente

En este espacio podrás conocer a una asociación estudiantil sobresaliente que forma parte de UTRGV. En este boletín, conocerás a la Asociación de Profesionales en Tecnología de la Información.

## Asociación de Profesionales en Tecnologías de la Información

La Asociación de Profesionales en Tecnología de la Información es una organización que se compromete a proporcionar a sus miembros con experiencia que mejorará sus carreras académicas y profesionales; Con actividades tales como participación comunitaria, capacitación práctica y competiciones. Como organización aquí en la Universidad de Texas - Rio Grande Valley, proporcionamos a nuestros miembros temas de discusión durante nuestras juntas generales para informarles sobre los temas más comunes e interesantes relacionados con nuestra carrera como análisis de protocolos, exploración de puertos, hacking de google , Eliminación de malware y líneas de comandos.

Visite nuestro Facebook para contactarnos (www.facebook.com/UTRGV.AITP)
Todas las carreras son bienvenidas a unirse.

**Protéjase de los delincuentes cibernéticos durante las vacaciones de primavera**

***Por: AITP***

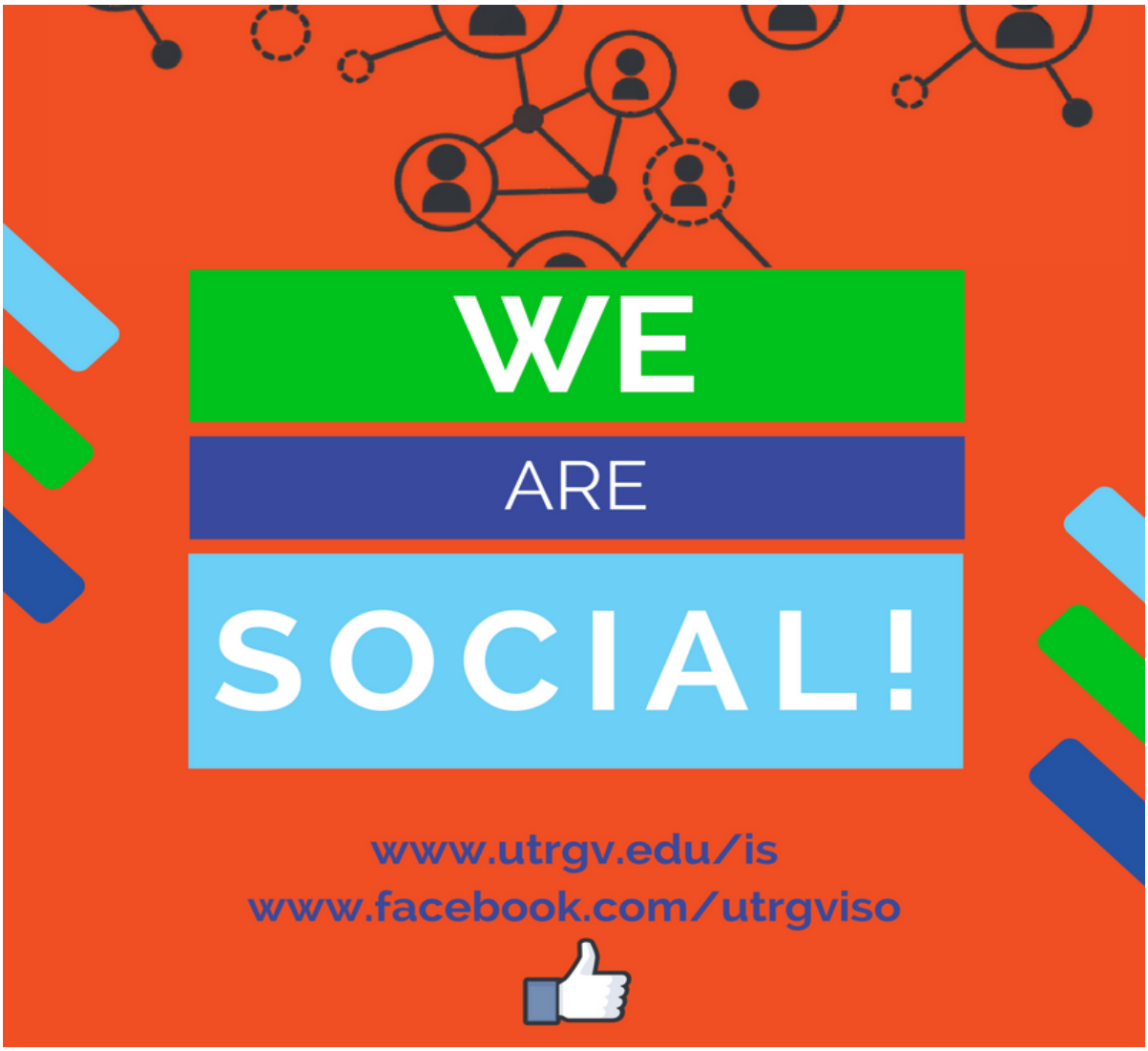
Las vacaciones de primavera se acercan rápidamente, lo que significa que son vacaciones para millones de estudiantes universitarios en todo el país. Por desgracia, esto da la oportunidad a los hackers y estafadores de aprovecharse de aquellos estudiantes desprevenidos y sus familias. A continuación encontraras tres métodos populares que los atacantes usan para estafar a los estudiantes, y maneras sencillas de protegerse durante las vacaciones de primavera.

1. **Clonación de tarjetas** – En este método utilizan lectores de tarjetas maliciosos que roban datos de la banda magnética de la tarjeta conectada a los terminales de pago como en los cajeros automáticos. Los clonadores de tarjetas han representado más del 80 por ciento en fraudes en los cajeros automáticos. La mejor manera de protegerse es hacer una pequeña investigación en cualquier cajero automático que vaya a utilizar. Siempre compruebe si hay alteraciones, si ve que algo se ve diferente, como un color diferente, material o gráficos extraños, NO use ese cajero automático. Además, no tenga miedo de mover el lector de tarjetas, ya que debe ser construido muy robusto e incapaz de romper fácilmente.

2. **USB infectados** - Este es un viejo método de los estafadores que han estado utilizando durante mucho tiempo, especialmente en lugares populares de vacaciones de primavera. Los estafadores dejarán un USB infectado en un estacionamiento, vestíbulo o incluso en un lugar de entretenimiento, con la esperanza de que alguien lo recoja y conecte a su computadora. La consecuencia de esto es la instalación involuntaria de malware o virus en su computadora. Esto puede ser muy dañino, ya que sin saberlo puede instalar un troyano que puede permitir a los delincuentes cibernéticos que se conecten de manera remota a su computadora y son capaces de controlar y espiar su dispositivo. La mejor manera de evitar esto es ignorar cualquier USB que encuentres incluso si está etiquetados con algo tentador como "Fotos de trajes de baño" o "Contenidos Clasificados".

3. **Phishing** - Es una estafa popular que los atacantes utilizan para obtener información personal, como números de tarjetas de crédito, contraseñas, nombres de usuario, etc. Esto se hace disfrazándose como una entidad confiable generalmente a través de correo electrónico. Así que si usted recibe correos electrónicos de cadenas de hoteles populares que ofrecen descuentos especiales de primavera que parece demasiado buenos para ser verdad, probablemente son falsos. Recuerde que organizaciones reales nunca utilizarán el correo electrónico para solicitarle que responda con su contraseña, número de seguro social u otra información confidencial. Siempre desconfíe de cualquier mensaje de correo electrónico que le pida que verifique información personal. Nunca responda a estos mensajes y, por supuesto, nunca haga clic en el enlace.


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


WE
ARE
SOCIAL!
www.utrgv.edu/is
www.facebook.com/utrgviso

# ARTÍCULOS DE SEGURIDAD INFORMÁTICA

**Hospital de Texas penalizado $ 3.2 millones por violaciones de HIPAA**
Se determinó que el Centro Médico Infantil de Dallas utilizó dispositivos móviles no codificados, entre otros incumplimientos en los esfuerzos por proteger los datos de salud del cliente. (bit.ly/TEXAShospital-penalized)

**Nuevo sitio web es la cámara de compensación para vulnerabilidades de dispositivos medicos**
Un sitio web administrado por la Salud Nacional ISAC servirá como centro de intercambio de información sobre vulnerabilidades de seguridad en dispositivos médicos. (bit.ly/NEWwebsite-NationalHealthISAC)

**Proteja sus dispositivos portátiles**
Proteja sus dispositivos portátiles como laptops, iPads o smartphones contra la pérdida o el robo (www.utrgv.edu/is/en-us/resources/how-to/protect-devices)

**Wi-Fi gratuito: ¿Que tan seguro es?**
Tres de cada cuatro personas se conectan a los servicios gratuitos de Wi-Fi en el extranjero, y el 82% de los viajeros se conectan a redes gratuitas, pero inseguras en lugares públicos como aeropuertos, cafeterías y hoteles. Por desgracia, esta práctica común te puede poner en riesgo. (er.educause.edu/blogs/2016/10/wi-fi-gratuito-que-tan-seguro-es)

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.

**Oficina:**
Sugar Road Annex (ESRAX) Building
R –167 Rusteberg Hall (BRUST) Building (*por cita*)

**Phone:** (956)665-7823
**Email:** is@utrgv.edu

Servicios que proporcionamos:

**CONCIENCIA, RIESGO Y CUMPLIMIENTO**

**ACTIVOS Y ADMINISTRACIÓN DE LAS VULNERABILIDADES**

**INGENIERÍA Y RESPUESTA A INCIDENTS**

**CONCIENCIA, COMUNICACIÓN Y DIFUSIÓN**

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

¡Danos tu opinion!
bit.ly/utrgvisonewsletterfeedback