Número 70

Agosto de 2016
Año 10

Notibytes

Universidad Distrital Francisco José de Caldas - Facultad Tecnológica
Proyecto Curricular Tecnología en Sistematización de Datos e Ingeniería en Telemática.

EDITORIAL

Siga estos consejos para crear contraseñas seguras

El Día Mundial de la Contraseña nació para promover el uso de contraseñas seguras, pues a pesar de que cada día hay más conciencia por parte de las personas acerca de la ciberdelincuencia y sus graves peligros, contraseñas como 12345, 12345678, 0000, password y otras combinaciones fáciles de recordar siguen siendo las más utilizadas para acceder a cuentas bancarias, correos electrónicos y redes sociales.

En el marco de la celebración de este día, la empresa de seguridad informática ESET lanzó un comunicado en el que da algunos consejos para crear contraseñas seguras.

El primer paso es añadir palabras para crear una frase que entre más específica sea, mejor. Uno de los ejemplos que da la compañía informática es que si le gusta la lectura puede usar una frase como 'amo leer'. Es un buen comienzo, pero la idea es ser más específico.

El segundo paso es agregar mayúsculas para darle énfasis a la frase e hincapié a cada palabra. Por ejemplo: 'AmoLeerNovelasDeAventuras'.

Luego de incluir la frase personal y mayúsculas, debe agregarle signos de puntuación o exclamación de manera creativa. La idea es que invente una contraseña visual en la que los signos son un elemento decorativo. Pueden ir al principio y al final de la contraseña. Por ejemplo:¡AmoLeerNovelasDeAventuras!

El cuarto paso tiene que ver con dejar espacios entre las palabras para lograr mayor complejidad. Ejemplo: ¡Amo Leer Novelas De Aventuras!

Para finalizar, el quinto paso para lograr una contraseña segura es reemplazar las letras de la frase por números o símbolos. Puede cambiar la 'a' por un @ o la 'e' por un 3. Lo que se le pueda ocurrir. Así, por ejemplo, nuestra contraseña quedaría: ¡@mo L33r Novelas De @v3nturas!

Hay gran cantidad de aplicaciones móviles diseñadas para guardar, de manera segura, todas las contraseñas y así evitar tener que aprenderse todas las combinaciones que escogió para cada cuenta.

Si luego de seguir estos pasos sigue dudando de la confiabilidad de su contraseña puede dirigirse a las siguientes páginas para saber si su contraseña es segura:(http://password.social-kaspersky.com/es), (http://www.passwordmeter.com/), (https://howsecureismypassword.net/).

Resumen tomado de: El Tiempo, Tecnosfera, el 6 de Mayo de 2016: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/dia-de-la-contrasena/16584251?ts=21

Comité Editorial:
Carlos Alberto Vanegas, Sonia Alexandra Pinzón, Edwin Ávila.

Los hackers ya pueden apoderarse hasta de su casa

Una ejecutiva líder de un conglomerado financiero llega a su apartamento de corte futurista en una noche de invierno. Es un hogar inteligente. Las luces, el televisor, el termostato, el sistema de sonido y hasta el calentador de agua se encuentran conectados a una red. No hace falta acercarse a un interruptor para encender las bombillas, tan solo cabe presionar un botón en una aplicación móvil. Es un sueño hecho realidad. La ejecutiva se despoja de sus prendas y empieza a disfrutar de un baño caliente. De improviso, la temperatura del torrente se eleva hasta resultar insoportable. Camina con premura para revisar la configuración del sistema. Las luces se apagan. El termostato deja de funcionar. La calidez de la temperatura perfecta da paso a un frío que cala hasta los huesos. El sueño se ha transformado en pesadilla. El hogar inteligente se ha enloquecido. A pocos metros de la construcción, un grupo de 'hackers' goza con el sufrimiento de su víctima y aguarda a que abandone su hogar para infiltrarse.

La escena descrita ocurre en una de las series de moda: 'Mr. Robot'. Aunque suena a ficción, le podría pasar a cualquiera en el futuro. Vivimos en un mundo donde cada día hay más equipos electrónicos con capacidad de procesamiento, almacenamiento y conexión a internet: desde televisores, carros, cafeteras y termostatos hasta equipos médicos transcendentales para la vida de los pacientes, como los marcapasos. Y la lista crece sin tregua. ¡Es el florecimiento de la era digital!.

En la actualidad existen alrededor de 5.000 millones aparatos conectados, y la cifra se quintuplicará en los próximos cincos años (hasta 25.000 millones), según la consultora Gartner. El mundo se está inundando de aparatos inteligentes. Y cualquier aparato inteligente es susceptible de un ataque.

"Prevenir el fraude en el mundo del internet de las cosas resulta particularmente tan complejo como esencial. Al tratarse de 'máquinas hablando con máquinas', es necesario crear algoritmos, llaves de cifrado,sistemas de autenticación mutua, sistemas de almacenamiento seguro y sistemas que eviten suplantación de identidades para que esta industria pueda crecer hasta donde los analistas pronostican", señala el experto de Gemalto Daniel Cuéllar.

Durante la conferencia Black Hat (orientada a hackers), llevada a cabo a inicios de este mes en Las Vegas, varios expertos dieron ejemplos de las posibilidades que un mundo conectado ofrece a los ciberdelincuentes.

Una ponencia que dejó boquiabierta a la audiencia fue la de Andrew Tierney y Ken Munro, dos expertos en seguridad, de la firma Pen Test Partners. Crearon un programa malicioso capaz de tomar el control de un termostato. Si el usuario quiere que el aparato funcione de nuevo (algo esencial en países donde se viven fríos intensos u olas de calor insoportables), debe pagar un monto de dinero. Es como un secuestro por el que piden rescate.

Charlie Miller y Chris Valasek, conocidos como los 'hackers' de Jeep. El dueto fue capaz de tomar el control de una Cherokee y manipularla a distancia para que frenara de sopetón o acelerara sin previo aviso. Además, lograron girar el timón con precisión quirúrgica en las curvas, ¡aterrador! Si pueden lograr eso con ese tipo de vehículos, lo mismo podría conseguir con cualquier otro modelo cuya operación incluya componentes electrónicos.

Continúa al respaldo……..

CONOZCAMOS NUESTROS PRINCIPIOS...

Tecnología en Sistematización de Datos

Visión:
El proyecto curricular de Tecnología en Sistematización de Datos deberá consolidarse como un programa académico de reconocimiento local, nacional e internacional, caracterizado por el aporte permanente al desarrollo tecnológico e investigativo, soportados en el uso de las herramientas tecnológicas suficientes para mantenernos ubicados en la frontera del conocimiento de los sistemas modernos de procesamiento y transmisión de información

Misión:
Formación de Tecnólogos íntegros, críticos e idóneos, altamente calificados en el área de los sistemas informáticos, capaces de identificarlos y mejorarlos empleando la ciencia y la tecnología para optimizar su funcionamiento.

Ingeniería en Telemática

Visión:
El proyecto curricular de Ingeniería en Telemática deberá consolidarse como un programa académico de reconocimiento local, nacional e internacional, caracterizado por el aporte permanente al desarrollo tecnológico e investigativo, soportado en la capacidad de convertir sistemas convencionales de comunicaciones en otros que puedan calificarse de avanzados, tanto por sus características teleinformáticas actuales como por sus proyecciones de mejoramiento y crecimiento.

Misión:
La misión del Proyecto curricular de Ingeniería en Telemática constituye la formación de profesionales con un alto nivel académico e investigativo, humanamente formados, científicamente fundamentados y tecnológicamente calificados en el área de telemática, capaces de servir a la sociedad y dar soluciones convenientes a sus requerimientos y necesidades mediante la creación, desarrollo y adaptación de tecnologías, promoviendo el cambio y la innovación

Recomendaciones de seguridad

Intel Security recomienda actualizar el 'software' de cualquier dispositivo inteligente de forma constante. Instale todos los parches de seguridad disponibles. "Esto le ayudará a protegerse contra virus y 'ransomware', en incluso de drones que se usen a distancia para atacar su lugar de trabajo", señalan los expertos de la firma.
Camilo Gutiérrez, de Eset, recomienda conectar los dispositivos a redes wifi seguras y conocidas, "de esta manera el usuario puede tener mayor control sobre el tipo de tráfico que pasa por la red", indica. "Por otra parte, solo instale aplicaciones que estén avaladas por el fabricante para reducir la posibilidad de verse afectado".
Por último, muchos códigos maliciosos, entre ellos los gusanos, se pueden propagar a través de dispositivos de almacenamiento USB o de tarjetas MicroSD. No introduzca memorias de origen desconocido. Nunca utilice una USB que se haya encontrado en la calle o el parqueadero de su oficina: un 'hacker' podría haberla puesto ahí para que usted la inserte en sus aparatos y se infecten.
Resumen tomado de: El Tiempo, Tecnosfera (Edgar Medina), el día 21 de Agosto de 2016.

http://www.eltiempo.com/tecnosfera/novedades-tecnologia/metodos-para-protegerse-de-los-hackers/16678826?ts=43

Cuidado con el ransomware, una modalidad de secuestro digital.

El cibercrimen se ha convertido en una actividad ejercida por agrupaciones internacionales cuyo principal móvil es el robo de información y dinero.
"En la comunidad de crimen digital hay desde quienes llevan a cabo ataques por reconocimiento y no por dinero (obran por motivaciones políticas, religiosas, ambientales o personales) hasta quienes operan por encargo para la obtención de información confidencial de grandes compañías", indica Daniel Cuellar, vicepresidente de Gemalto para el Pacto Andino y el Caribe. "Pero, los que más abundan, en la actualidad, son los que quieren obtener ganancias financieras de forma rápida, a través de 'phishing', ingeniería social o código malicioso, logrando el robo de identidad y la obtención de datos financieros o dinero", añade el experto.
Una de las modalidades para captar botines de potenciales víctimas es el 'ransomware'. Este término en inglés se refiere a las palabras 'ransom' (rescate en español) y 'ware' (en referencia a software). Este tipo de programas maliciosos bloquean el acceso a los archivos del equipo de cómputo o al dispositivo móvil. Una vez se encuentra activado esta clase de software, el usuario no puede ingresar a su equipo o a fragmentos específicos del sistema de archivos. Algunos tipos de 'ransomware', como por ejemplo la variante denominada Cryptolocker, cifran los archivos más relevantes del equipo, como aquellos relacionados con documentos de texto, hojas de cálculo, e incluso videos e imágenes. A cambio de devolver el acceso a los archivos cifrados, el programa malicioso solicita un monto de dinero. Este suele ser relativamente pequeño (no superior a 500 dólares) que se deben pagar en bitcoines. El monto solicitado no es de gran cuantía porque así resulta más probable que la víctima se muestre dispuesta a pagar por su información digital.

El primer troyano de tipo 'ransomware' fue identificado en 1989, se llamaba AIDS (siglas de SIDA en inglés). No obstante, McAfee Labs solo advirtió un incremento en las muestras de este tipo de programas maliciosos a partir del segundo trimestre de 2002. Lo que frenó su uso, en ese entonces, fue la inexistencia de un método de pago anónimo, como la moneda bitcóin, y ello dificultaba el pago del rescate.
El 'ransomware' de nueva generación incluye muestras como CryptoWall 3, CTB-Locker y CryptoLocker, los cuales pueden cifrar los archivos secuestrados con algoritmos de clave pública RSA de 2.048 bit y ataca, sobre todo, archivos de Microsoft Office, PDF de Adobe y formatos de imágenes como JPG y PNG.
En el cuarto trimestre de 2015, Intel Security reveló un incremento de 26 por ciento en este tipo de códigos maliciosos.

"El 'ransomware' está funcionando y eso está llevando a que existan cada vez más variantes de este código malicioso. Hay casos en que los cibercriminales han diseñado el software de acuerdo con las características de la víctima", le contó a Tecnósfera Mauricio Vergara, especialista en ciberseguridad de NEC.

¿Qué hacer si fue infectado por 'ransomware'?

La firma de seguridad Eset recomienda crear una copia de seguridad de los archivos de su equipo de cómputo o dispositivo móvil y nunca pagar el rescate solicitado por los cibercriminales. "Esto es esencial porque no suele ser común que se puedan descifrar los archivos afectados", explicó Federico Pérez Aquisto, gerente general de Eset Latinoamérica a Tecnósfera.
Para computadores de escritorio, Eset sugiere desactivar el Protocolo de Escritorio Remoto (esto facilita que los cibercriminales tomen control del equipo desde otro lugar). También puede optar por cambiar el puerto por defecto (3398). Además, use autentificación de dos factores y desactive los macros en Microsoft Office (estos también permiten que el atacante tome control del sistema).

Resumen tomado de: El Tiempo, Tecnosfera (Edgar Medina), el día 22 de Junio de 2016.
http://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/que-es-ransomware-y-como-prevenirlo/16626416?ts=29

Pare Oreja

Dicen que….

- **Las fechas límite para la captura de notas son:**
  - Primer corte: Octubre 8 de 2016.
  - Segundo corte: Diciembre 3 de 2016.
  - Examen final: Diciembre 17 de 2016**.**
- **Finalización del primer semestre:** Diciembre 3 de 2016**.**

Link de Interés:

- **Los riesgos de poner a cargar el celular en lugares públicos:** **http://www.eltiempo.com/tecnosfera/novedades-tecnologia/riesgos-de-poner-a-cargar-celulares-en-lugares-publicos/16684991**
- **Line introduce nuevo botón para encriptar mensajes** **http://www.eltiempo.com/tecnosfera/novedades-tecnologia/line-introduce-nuevo-boton-para-encriptar-mensajes/16682055?ts=57**
- **Ministerio TIC contribuirá a la pedagogía por la paz** **http://www.eltiempo.com/tecnosfera/novedades-tecnologia/proceso-de-paz-ministerio-tic-contribuira-a-la-pedagogia-por-la-paz/16683130?ts=70**

SI QUIERES FORMAR PARTE DE LA ELABORACIÓN DE ESTE BOLETÍN PREGUNTA EN LA COORDINACIÓN DE LA CARRERA tecsistematizaciondatos@udistrital.edu.co