Número 81

Notibytes

1

Enero de 2018
Año 12

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

EDITORIAL

Buscan a los 35 jóvenes más brillantes e innovadores de Latinoamérica.

Si usted es menor de 35 años y se considera un joven brillante e innovador, la convocatoria que lanzó la revista MIT Technology Review en español es de todo su interés.

Con el respaldo del prestigioso Instituto Tecnológico de Massachusetts (MIT), en Estados Unidos, esta publicación se encuentra en la búsqueda de los latinoamericanos con los proyectos tecnológicos más destacados del continente.
Las áreas que abarcan esos proyectos, cuyo trabajo tendrá un importante impacto en la sociedad, tienen que ver con biotecnología, nanotecnología, electrónica, robótica, informática, inteligencia artificial, internet, materiales, medicina, telecomunicaciones, energía y transporte.
Concursar es muy sencillo, solo debe tener menos de 35 años y haber nacido en alguno de estos países: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay y Venezuela.
Así mismo, **el aspirante debe haber desarrollado un proyecto tecnológico, de emprendimiento e innovación.**
Los interesados pueden postularse hasta el 5 de marzo a través de la página https://challenges.opinno.io/.

'Innovadores Menores de 35' premia desde hace más de 10 años a los emprendedores más destacados en tecnología e innovación de todo el mundo, y entre los galardonados de la región están la plataforma de participación democrática confiable y transparente a través de la tecnología blockchain del argentino Santiago Siri y la aplicación Blooders que conecta pacientes, donantes y hospitales que quieran donar o conseguir sangre, creada por el mexicano César Esquivel.

Resumen tomado de: eltiempo.com, tecnosfera, 23 de Enero/2018
http://www.eltiempo.com/tecnosfera/novedades-tecnologia/abren-convocatoria-para-buscar-a-los-35-jovenes-mas-innovadores-de-la-region-174296

Seis técnicas de persuasión que usan los estafadores en Internet y como identificarlas.

Puede que alguna vez haya leído o escuchado la expresión "ingeniería social", pero ¿sabe lo que significa?
En ciencias políticas, el término se usa para hablar sobre las influencias y acciones que emplean ciertos gobiernos y clases de poder sobre la sociedad para intentar cambiarla.
Pero en seguridad informática, la expresión se refiere a las técnicas de manipulación psicológica que usan los ciberdelincuentes para tenderles trampas a los internautas.

La ingeniería social es el arte del engaño.

El objetivo puede ser diverso, desde obtener información hasta realizar fraudes o acceder de manera ilegítima a ciertos documentos. Para lograrlo, los estafadores se valen de una serie de métodos y herramientas con las que buscan confundir al usuario. Estas son algunas de ellas.

1. **Principio de simpatía**

A través de la observación de los movimientos que hace cuando navega por la red o de la información que hay publicada sobre usted, los estafadores pueden recopilar muchos datos, desde su dirección de correo electrónico hasta su número de teléfono, el nombre de su mascota o su lugar de residencia. Conseguir datos puede ser más sencillo de lo que muchos piensan. Compruébelo usted mismo. ¿Qué tanto puede saber un extraño sobre usted analizando sus redes sociales?
La manipulación viene después: los hackers usan esa información para hacerse pasar por una persona de su confianza y tenderle trampas.
"El principio de simpatía, también traducido como de afición, gusto o atracción, nos señala algo que a primera vista puede parecer simple: estamos más predispuestos a dejarnos influir por personas que nos agradan, y menos por personas que nos producen rechazo", explica el psicólogo y escritor estadounidense Robert Cialdini, quien escribió en 1984 Influence: *The Psychology of Persuasion* ("Influencia: la psicología de la persuasión") y definió los seis principios.
Lo mejor es que evite dar demasiados datos sobre usted a quien no conoce. Tendemos a confiar más en extraños cuando navegamos por internet. Recuerde que más vale prevenir que curar.
La observación también puede referirse a los documentos que tiene en el equipo. Por eso, cuanta menos información dejes a la vista en el escritorio, mejor.
Un consejo: Si no quiere compartir demasiados datos sobre usted en internet, desactiva la geolocalización para que otros usuarios de internet no sepan dónde se encuentra. También es recomendable comprobar su perfil público o visitar directorios de internet para saber qué información tienen sobre usted.

2. Principio de escasez

"Date prisa". "Es urgente". "Cambia ya tu contraseña". "¡Llama ya!". Meter presión a los usuarios para lograr sus objetivos es una de las técnicas más habituales de los ciberdelincuentes. A través de esa presión buscan pasar inadvertidos, dándole menos oportunidad al usuario de que caiga en la trampa. Muchas veces usan ese sentido de urgencia para enviar "ofertas que no te puedes perder" y todo tipo de "oportunidades" que, en realidad, no son tan "exclusivas" como aseguran en esos emails o mensajes de texto.
Y esa urgencia está muy relacionada con lo que en psicología se define como el "principio de escasez", el cual nos hace estar más dispuestos acercarnos a algo si notamos que es escaso o difícil de conseguir.

3. Principio de autoridad

La amenaza a menudo viene de la mano de la urgencia. Por ejemplo: "Es urgente. Si no cambias ahora mismo tu contraseña, perderás tu cuenta para siempre". Y la amenaza viene de la mano de lo que se conoce como principio de autoridad.

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

Boletín Informativo

Según explica Cialdini, "estamos más predispuestos a dejarnos influenciar cuando somos interpelados por una autoridad".
No se trata de coaccionar o ejercer poder, sino con "el aura de credibilidad que la autoridad supone".
"Tendemos a creer que quienes están en posiciones de liderazgo tienen más conocimiento, más experiencia, o más derecho a opinar", añade en su libro el especialista.
Para ello, a menudo los hackers intentan hacerse pasar por una entidad o persona de confianza de la víctima. A esta técnica se la conoce como phishing.

4. Principio de reciprocidad

A través de una serie de preguntas de índole personal, los estafadores desarrollan los perfiles de sus víctimas.
Gracias a ello, logran establecer vínculos para identificar los temas hacia los que pueden reaccionar de manera más favorable para ellos.
Muchas veces, usan perfiles falsos para lograr el engaño. Este tipo de conexiones también se usan para fraudes de "sextorsión".
A través de estas estrategias aplican lo que se conoce en psicología como "principio de reciprocidad", el cual establece que tendemos a tratar a los demás de la misma manera en que nos tratan a nosotros.
Por ejemplo, si recibimos un regalo o beneficio, sentiremos la necesidad de devolver el favor.
La eficacia de este método psicológico es mayor si el regalo es percibido como algo personal.
Lo mismo ocurre si nos cuentan una confidencia o un secreto íntimo: es muy probable que queramos contar también algo nuestro.
Un consejo: No establezca diálogos con desconocidos sobre su vida personal. ¿Por qué le hace tantas preguntas? ¿Para qué necesita saber toda esa información?

5. Principio de compromiso y coherencia

Al haber observado sus comportamientos previos y saber sobre usted, los hackers son capaces de captar la atención de sus víctimas.
Si, por ejemplo, quieren que la persona tome una decisión de manera impulsiva, será más fácil lograrlo siendo coherente con el perfil de esa persona, con los gustos que tiene, con cómo se define...
Además, ese principio establece que cuando una persona se compromete con algo, tiene más probabilidades de cumplir con su compromiso, incluso cuando su motivación original haya desaparecido.
Por eso, a veces, los estafadores se valen de formularios y preguntas clave que te obligan a comprometerte con algo específico.

6. Principio de aprobación social

Este principio, al que también se denomina "consenso" o "seguir el rebaño", establece que tendemos a acomodarnos a lo que opina la mayoría de la gente.
Eso quiere decir que si mucha gente da algo por bueno, nosotros probablemente lo hagamos también (y viceversa).
Los estafadores intentan convencernos de que cierto antivirus (que en realidad es un programa malicioso que intentan vender en ventanas emergentes) es el que usa todo el mundo... y por eso lo "necesitamos" instalar nosotros también.
O que mucha gente participó en un sorteo y a mucha gente le tocó un precio: "¡Tú también puedes lograrlo!"
No se deje engañar.

Resumen tomado de: semana.com, Tecnología, 17 de Enero de 2018 http://www.semana.com/tecnologia/articulo/tecnicas-de-persuasion-que-usan-los-estafadores-en-internet-y-como-identificarlas/553918

Rapid Ransomware, la nueva amenaza que encripta los archivos de tu PC.

Desde finales de año el ransomware no ha hecho mucho ruido, pero la tregua de esta amenaza no ha durado mucho. Recientemente ha sido detectado un nuevo ransomware que tiene una característica bastante peculiar: después de llevar a cabo el encriptado inicial del ordenador infectado, continúa cifrando los archivos nuevos que se vayan creando en el equipo. El virus se llama Rapid Ransomware y es una de las pocas cepas que presenta este comportamiento.

De acuerdo con los informes de seguridad de ID-Ransomware, Rapid Ransomware ha infectado a más de 300 equipos desde el 3 de enero, aunque esta cifra corresponde solo a una pequeña muestra de las víctimas totales, ya que muchos usuarios infectados probablemente no emplearon esta herramienta para identificar el virus.

De momento se desconoce cómo se está propagando el malware, pero lo que sí sabemos es cómo actúa. Una vez instalado en el ordenador, al ejecutarse borra las copias generadas por Volume Shadow Copy Service (VSS), finaliza los procesos de la base de datos y desactiva la reparación automática.

Para evitar ser una víctima y no sufrir sus consecuencias, te recomendamos que sigas los consejos para protegerse del ranswomare que te dejamos a continuación:

- Utiliza un buen **programa antivirus** que cuente con funciones contra el ransomware.
- Guarda una **copia de seguridad actualizada de tus archivos en la nube** o un disco duro externo.
- Revisa con precaución el correo electrónico: evita descargar y abrir archivos adjuntos sospechosos y no sigas enlaces remitidos por desconocidos.
- Mantén el sistema operativo actualizado.

Resumen tomado de: computerhoy.com, Sandra Arteaga, Enero 24 /2018.
https://computerhoy.com/noticias/software/rapid-ransomware-nueva-amenaza-que-encripta-archivos-tu-pc-74859

Pare Oreja

Dicen que….

- **Inicio primer semestre de 2018: 1 de febrero.**
- **Entrega de Trabajos de Grado Culminado 02 y 05 de febrero de 2018.**
- **Entrega propuestas de trabajos de Grado (Anteproyectos) 09 y 12 de febrero de 2018.**
- **Las fechas límite para la captura de notas son:**
  - Primer corte: Abril 7 de 2018.
  - Segundo corte: Mayo 26 de 2018.
  - Examen final: Junio 9 de 2018**..**
- **Finalización del primer semestre:** Mayo 26 de 2018.

Link de Interés:

- **Así usaron el celular los colombianos en 2017**

  https://www.elespectador.com/tecnologia/asi-usaron-el-celular-los-colombianos-en-2017-articulo-735240

- Malware presente en 53 apps de Google Play roba las claves de Facebook **https://computerhoy.com/noticias/moviles/malware-presente-53-apps-google-play-roba-claves-facebook-74569**

- Buscadores basados en Blockchain, qué son y cómo funcionan

  https://computerhoy.com/noticias/internet/buscadores-basados-blockchain-que-son-como-funcionan-73893

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