Número 82

Notibytes

1

Febrero de 2018
Año 12

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

EDITORIAL

Google también le ayudará a conseguir el trabajo de sus sueños<

El gigante tecnológico implementó una nueva herramienta con la que podrá encontrar las ofertas de empleo que más se acomoda a sus intereses.
Internet se ha convertido en el principal camino para buscar empleo. A través de la red se puede encontrar una gran cantidad de ofertas que no cumplen las condiciones que cada uno espera, lo que puede ser un tropiezo en el camino para poder hallar el trabajo soñado.
Para ello, Google -el buscador más utilizado en el mundo-, ha habilitado una nueva herramienta con la que se facilitará la experiencia de búsqueda de acuerdo a sus necesidades económicas, geográficas y de intereses particulares.
La herramienta ya está habilitada y a partir de este momento cuando realice búsquedas como "trabajos cerca de mí", "empleos para maestros" o consultas de empleo similares, tanto en su dispositivo móvil con Android como en la web, verá resultados detallados que le permiten explorar las ofertas de trabajo a lo largo de toda la web.
Otro de los inconvenientes que pueden encontrar quienes buscan un nuevo empleo es que muchas veces algunas personas sin escrúpulos se aprovechan de esta necesidad para hacer estafas a algunos incautos. Una forma de prevenir esta clase de situación es que a partir de ahora también se podrán ver comentarios y calificaciones del empleador de sitios de confianza, justo a un lado de la descripción del trabajo. Además también puede saber cuánto tiempo le tomaría llegar a algunos sitios de trabajo. En caso de haber iniciado sesión Google Maps le mostrará el tiempo estimado que puede gastar en diferentes medios de transporte.
Habilitando el filtro de "Ubicación podrá establecer la distancia que está dispuesto a recorrer hasta su posible trabajo, de 3 hasta 300 km o "cualquier lugar". Así solo verá los empleos entre esta rango de distancia ahorrando tiempo.
Todos estos criterios de búsqueda pueden quedar guardados para luego retomarlos en cualquier momento que desee. También podrá habilitar alertas y notificaciones cuando aparezcan nuevas ofertas que concuerden con sus necesidades.
Resumen tomado de: semana.com, tecnología, 31 de Enero/ 2018
http://www.semana.com/tecnologia/articulo/como-encontrar-trabajo-herramienta-google/555462

"Ciberataques con inteligencia artificial llegarían en menos de 5 años".

Más de 25 investigadores de las universidades de Cambridge, Oxford y Yale y expertos en materia de privacidad alertaron en un estudio sobre los riesgos de que la tecnología de inteligencia artificial (IA) sea utilizada con fines delictivos. Según los expertos los rápidos avances en IA están aumentando los riesgos de que ciberdelincuentes se valgan de esa tecnología para generar ataques automáticos de *hacking*, causar accidentes automovilísticos en carros de conducción autónoma o convertir drones comerciales en armas dirigidas.
Como lo han dicho campañas internacionales, como es el caso de la campaña Stop Killer Robots, el tiempo se agota. Los investigadores indicaron en el estudio que este tipo de desarrollos maliciosos son plausibles dentro de solo cinco años en el futuro. El uso malicioso de IA, según lo presentan los académicos podría generar "una amenaza inminente para la seguridad digital, física y política al permitir ataques a gran escala, altamente dirigidos y altamente eficientes".

Se acaba el tiempo para reglamentar los 'robots asesinos'
El documento de 98 páginas, publicado este miércoles 20 de febrero, advierte que el costo de los ataques militares se reduciría al utilizar la IA para completar tareas que de otra manera requerirían trabajo humano y experiencia. Pueden surgir nuevos ataques que serían imprácticos para los humanos solos para desarrollarse o que explotan las vulnerabilidades de los propios sistemas de inteligencia artificial.
Miles Brundage, investigador del Instituto Future of Humanity de Oxford, aseguró que todos los investigadores están de acuerdo en que hay muchas aplicaciones positivas de la inteligencia artificial, pero que hasta el momento "hubo un vacío en la literatura sobre el tema del uso malicioso".
Las capacidades de la IA para procesar millones de datos en poco tiempo y emular el razonamiento humano en la toma de decisiones o el procesamiento de todo tipo de información (texto, voz o imágenes visuales) ha hecho que esta tecnología sea vista como una fuerza poderosa para el cambio y la solución de problemáticas humanas en todo tipo de sectores. Sin embargo, los riesgos sobre si la automatización masiva podría resultar en un desempleo generalizado y en otro tipo de impactos que afecten la vida humana son una preocupación recurrente.
El estudio, llamado 'El uso malicioso de la Inteligencia Artificial: Predicción, Prevención, y Mitigación', tiene contribuciones de organizaciones internacionales sin ánimo de lucro como OpenAI (creada por Elon Musk), Center for a New American Security y la Electronic Frontier Foundation.

Resumen tomado de: eltiempo.com, Tecnosfera, 21 de Febrero de 2018,
http://www.eltiempo.com/tecnosfera/novedades-tecnologia/riesgo-de-que-la-inteligencia-artificial-sea-utilizada-por-el-mal-185394

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

"Un niño puede enseñar tres cosas a un adulto: a ponerse contento sin motivo, a estar siempre ocupado con algo y a saber exigir con todas sus fuerzas aquello que desea". Paulo Coelho

Boletín Noti-bytes

Cuando el terrorismo de Estado se vuelve digital.

Hace unos días, Tom Bossert, asesor de seguridad del presidente Donald Trump, acusó públicamente a Corea del Norte de estar detrás de Wannacry, uno de los mayores ataques contra la seguridad digital en la historia, que perjudicó a cientos de miles de computadores en prácticamente todo el mundo y desactivó sistemas vitales en hospitales, instituciones públicas y empresas.
Las sospechas acerca de la participación de Corea del Norte emergieron a los pocos días del ataque, cuando varios investigadores independientes lograron aislar parte del código del ataque y vincularlo con muestras de otros incidentes en los que había participado una unidad de élite vinculada con el gobierno norcoreano.

Uno de esos investigadores fue Matthieu Suiche, un analista francés con base en Dubái, fundador de la firma de seguridad digital Comae Technologies, quien aseguró en su momento que la participación de Corea del Norte en Wannacry significaría que "estaríamos ante el primer gran ataque de *ransomware* auspiciado por un Estado, pero con una particularidad: no se trata de conseguir dinero, sino de sembrar caos y de lograr una afectación política. El código está bien hecho, es profesional, aunque tiene unas fallas de diseño que resultan interesantes porque ha frenado la recaudación de fondos".

En otras palabras, lo que Suiche dice es que podría ser un acto de terrorismo de Estado, pero en el reino digital. Uno de los primeros, además, en utilizar la modalidad de *ransomware*, o secuestro de información a cambio de dinero.
Ahora, en justicia, no es la primera ocasión en que un Estado se mete en el mundo digital para operar contra otro país o contra blancos particulares. Y esto es lo preocupante: hay guías muy claras, o al menos más reconocidas, sobre lo que puede hacer un país en operaciones militares en el mundo lejos del teclado. Pero estas líneas son más difusas, grises a lo sumo, cuando se trata de internet.
El ejemplo clásico de una operación de estas es Stuxnet: un programa malicioso cuya autoría se les atribuye a los comandos cibernéticos de Estados Unidos e Israel y que fue desplegado para afectar el programa nuclear iraní. El virus fue descubierto en 2010, aunque hay reportes que sitúan su desarrollo en 2005, y aprovechaba cuatro vulnerabilidades no reportadas, conocidas popularmente como *zero day exploits*.

Stuxnet fue utilizado para desmantelar las centrifugadoras utilizadas por los iraníes para enriquecer el uranio que, según ellos, era para usos civiles, aunque prácticamente el resto del mundo aseguraba que iba para armas atómicas.
Lo problemático de este ejemplo es que se trató de una operación encubierta y, por lo tanto, sin mayores rastros sobre su proceso de toma de decisiones o la lógica detrás de atacar estos sistemas. Esto es complejo porque, más allá de las implicaciones y motivaciones políticas, se trata del uso militar de vulnerabilidades de software ampliamente utilizado por civiles.
De nuevo, más allá de la geopolítica y las motivaciones para irse a la guerra digital contra otro país o contra una corporación, lo que está en el medio es la seguridad digital de todas las personas cuya vida diaria depende de los mismos sistemas que un Estado en particular trata de vulnerar. Lo que sucede con este tipo de operaciones, con el desarrollo de armas para quebrar el software usado por civiles, es que al final suelen caer en otras manos, que resultan mucho peores que las de sus creadores.
Wannacry es el perfecto ejemplo de este mecanismo: el ataque fue posible gracias al robo de armas digitales desarrolladas por la Agencia Nacional de Seguridad de Estados Unidos (NSA, por sus siglas en inglés).

Se entiende que este tipo de instituciones, como la NSA, la CIA o el GCHQ británico, busquen obtener ventajas en ataque y defensa digital. De hecho, parte de su misión constitucional es ir a la vanguardia en estas técnicas. Pero estimular la creación y explotación de fallas en los sistemas de los cuales depende toda la vida moderna termina siendo un arma de doble filo contra la parte más débil del eslabón: los usuarios.

Durante la administración de Barack Obama, la Casa Blanca creó una suerte de protocolo para mediar entre la necesidad de encontrar fallas en los sistemas y publicarlas para proteger a los usuarios civiles en todo el mundo: si una agencia detectaba una vulnerabilidad inédita, lo indicado era compartirla con el fabricante para así proteger la seguridad de millones de usuarios. La única razón bajo la cual podían ocultarla era por motivos de seguridad nacional. Un comité de expertos incluso recomendó que esta utilización de la debilidad sólo podía hacerse por un tiempo determinado.

Pero los robos de arsenal digital sufridos por la NSA y la CIA y el ataque de Wannacry terminaron por mostrar que este proceso es ineficiente, por decir lo menos.
También vale la pena anotar que durante el gobierno Obama se ordenó un incremento en los ataques digitales para sabotear y retrasar el programa de misiles balísticos de Corea del Norte. Desde hace unos años, el comando de operaciones cibernéticas de Estados Unidos ha venido creciendo: se estima que su tamaño se ha quintuplicado y que el número de personal que trabaja en él puede ser de hasta 4.000 personas.

El incremento de la capacidad de los estados para atacar y defenderse en línea es, acaso, un producto normal de las aplicaciones y posibilidades de internet. Pero el asunto es que en el mismo medio coexisten criminales, países enemigos y usuarios civiles. Si el terrorismo de Estado ya era suficientemente complejo de tratar, y de castigar, en el mundo tangible, los augurios no son buenos en el reino digital. Y en la mitad de esas tensiones quedamos todos.

Resumen tomado de: www.elespectador.com, Tecnología, 9 de Enero 2018.
https://www.elespectador.com/tecnologia/cuando-el-terrorismo-de-estado-se-vuelve-digital-articulo-732459

Pare Oreja

Dicen que….

- **23 de marzo y 02 de abril de 2018, recepción de Anteproyectos y Proyectos Culminados.**
- **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**.**

Link de Interés:

- **Cómo arreglar una memoria USB rota en Windows** **https://computerhoy.com/paso-a-paso/hardware/como-arreglar-memoria-usb-rota-windows-75557**
- **Los temas tecnológicos más relevantes de la Conferencia de Seguridad de Múnich** https://www.elespectador.com/tecnologia/los-temas-tecnologicos-mas-relevantes-de-la-conferencia-de-seguridad-de-munich-articulo-739999
- **Aprenda a programar en 24 horas con esta 'app'** http://www.eltiempo.com/tecnosfera/apps/swift-una-aplicacion-para-ipad-para-aprender-a-programar-en-24-horas-185840

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