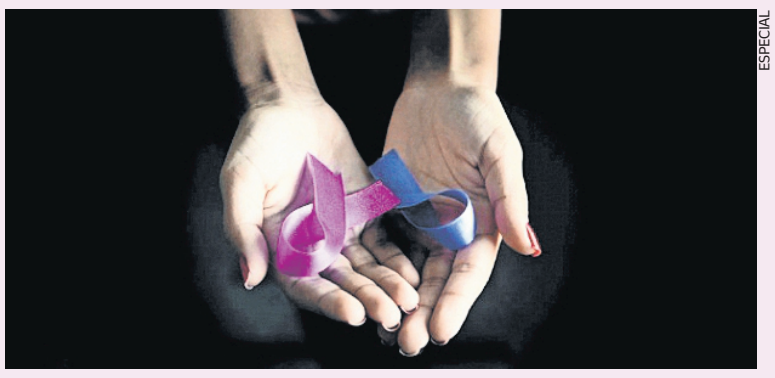
PROYECTO UNAM

Texto: **Roberto Gutiérrez Alcalá**
robargu@hotmail.com



ESPECIAL

Conferencia dentro del ciclo "Religión y Violencias"

El Instituto de Investigaciones Sociales de la UNAM, dentro del ciclo "Religión y Violencias", del Laboratorio de Observación del Fenómeno Religioso en la Sociedad Contemporánea, invita a la conferencia "Violencia simbólica en el discurso sobre la 'ideología de género'", que dictará Karina Bárcenas Barajas el 17 de mayo, a las 10:30 horas, en el Anexo del Auditorio del citado instituto, en CU. ●

Carne cultivada *in vitro*, opción alimentaria

De acuerdo con María Rubio, académica de la Facultad de Medicina Veterinaria y Zootecnia de la UNAM, con la producción de carne cultivada *in vitro* se busca una opción que provea de proteína de origen animal a los humanos y sea amigable con el medio ambiente y sin el costo del animal. Sin embargo, por el momento, esta innovación está en fase experimental y no se concretará en el corto plazo. "Más de 200 empresas en todo el planeta muestran interés en las investigaciones que buscan hacer de la carne artificial un proyecto viable y eficaz", señaló. ●

ESPECIAL

Formar niños felices, más que competitivos

Según Carime Hagg, académica de la Facultad de Psicología de la UNAM, formar niños felices, más que competitivos, debe ser lo primordial. También dijo que los niños de hoy son más independientes y aprenden a tomar decisiones con mayor rapidez que sus padres cuando eran pequeños. "La curiosidad natural les permite interactuar fácilmente con las nuevas tecnologías, que les ofrecen ventajas para desarrollar habilidades, pero como tienden a aislarse y dejan de lado el impulso de otras capacidades, éstas no deben ser utilizadas como 'nanas' modernas", añadió. ●

Guerra en Internet

Aunque es exagerado decir que los ciberataques podrían desatar una conflagración mundial, sí tienen la capacidad de propiciar situaciones en las que peligre la seguridad y la economía de una o varias naciones

ESPECIAL

La interconexión global conlleva no pocos riesgos.

UNAM La Universidad de la Nación

No sólo computadoras, tabletas y teléfonos inteligentes, sino también dispositivos tales como cámaras, alarmas, sensores de puertas, sensores biométricos, sensores médicos... están conectados a Internet. No por nada se habla del Internet de las cosas.

Ahora bien, en cuanto a capacidad de procesamiento y memoria, estos dispositivos están muy limitados, lo cual implica que sus medidas de seguridad sean muy limitadas también. Por eso, los ciberataques dirigidos a ellos pueden ocasionar daños muy severos.

"Debido a que resultan fácilmente manipulables, una vez que son programados como si se tratara de dispositivos *zombies*, siguen una instrucción muy simple que puede causar un verdadero desastre a nivel de comunicación en Internet", dice Fabián Romo, director de Sistemas y Servicio Institucionales de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación de la UNAM.

Aunque es exagerado decir que los ciberataques podrían desatar una conflagración mundial, sí tienen la capacidad de propiciar situaciones en las que peligre la seguridad y la economía de una o varias naciones.

"Por ejemplo, si los sistemas de salud, de protección civil y bancarios, que dependen de las comunicaciones vía Internet, fueran objeto de ciberataques, los servicios médicos, la seguridad pública y la economía estarían en riesgo de sufrir un colapso", comenta Romo.

El actuario universitario.

Medidas de seguridad en México

En opinión del actuario universitario, no todas las instituciones han implementado en nuestro país medidas de seguridad cien por ciento confiables.

"Los bancos, los organismos de seguridad pública y universidades como la UNAM cuentan con mucha seguridad en sus redes de comunicaciones y en su conexión a Internet. Para garantizar la protección de los datos y de los sistemas informáticos, así como la estabilidad de la operación en conjunto de los dispositivos conectados a Internet, estas instituciones siguen una serie de protocolos, normas y recomendaciones nacionales e internacionales. Otras instituciones, sin embargo, todavía son muy vulnerables a ciberataques porque en las redes públicas hay puntos desprotegidos."

Es importante que el usuario de Internet sea consciente de los riesgos que supone trabajar con sistemas de información a través de las redes públicas y privadas. Por lo que se refiere a la UNAM, desde hace mucho tiempo tiene un área específica de seguridad de la información que organiza congresos y seminarios, y publica documentos y revistas para tratar de cumplir esa labor concientizadora.

"En situaciones críticas, el hilo se rompe por la parte más delgada, y es precisamente el usuario de Internet el que a veces no pone en práctica todas las medidas de seguridad. Claro, la red a la que está inscrito o dónde está conectado tiene mucho que ver. A veces, también, peca de inocencia al aceptar información que no solicitó y acceder a archivos que pueden estar contaminados", señala Romo.

El fin de un *malware* o un virus informático que contamina archivos es violentar la seguridad de las computadoras, las tabletas y los teléfonos inteligentes, y abrir huecos de seguridad para que, cuando se orqueste un ataque global —conocido también como Ataque de Día Cero—, no haya capacidad de reacción si el usuario no activó ninguna medida de seguridad en su dispositivo, como un anti*malware* o un antivirus.

Así, la información y los datos del usuario se verán afectados; y su dispositivo podrá formar parte de un ejército cibernético que lance un ataque a sistemas centrales.

"A los atacantes les gustan estos sistemas centrales porque saben que, si los vulneran, afectarán muchos servicios, especialmente gubernamentales y bancarios."

"En situaciones críticas, el hilo se rompe por la parte más delgada, y es precisamente el usuario de Internet el que a veces no pone en práctica todas las medidas de seguridad"

FABIÁN ROMO
Director de Sistemas y Servicio Institucionales de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación de la UNAM

Nuevos riesgos

Por lo regular, los ciberataques son dirigidos a servicios que contienen directorios de usuarios, es decir, una gran cantidad de identificaciones de usuarios no sólo con una cuenta y una contraseña, sino también con nombres, apellidos y domicilios, y, en el caso de los sistemas bancarios, con números de cuenta, transacciones, saldos, etcétera.

El *hacker* entra en un sistema, recupera toda la información de algunos usuarios (o parte de ella), y elige a los que, por su naturaleza o algún objetivo muy puntual, le convengan; a continuación, los reemplaza, se mete con sus contraseñas en el sistema y usa sus datos personales para hacer fraudes.

"Puede robarle a una persona su cuenta de *Facebook*, ingresar en el sistema de esa red social como si fuera ella y hacer lo que se denomina ingeniería social: decirles a los contactos de esa persona que lo secuestraron y necesita que le depositen dinero en algún lugar; o pedirles a las mujeres tomarse una foto desnudas para apoyar un movimiento de lucha contra el cáncer de mama en el que él supuestamente participa; o bien, ingresar en los sistemas bancarios, vaciar totalmente los fondos de una persona y comprar criptomonedas para ocultar quién se los está llevando", explica Romo.

En relación con el minado de criptomonedas, es una actividad legal cuando el usuario pone en su computadora un *software* destinado a ello. El minado de criptomonedas es una labor que conlleva mucho gasto de energía y procesamiento: puede ocupar casi 100% de los recursos de una computadora.

"Con muchísima frecuencia, no obstante, un *malware* se mete en una computadora que mina criptomonedas, se instala sin la autorización de su usuario, comienza a minar criptomonedas en beneficio de otro usuario o grupo de usuarios que no tienen nada que ver con aquél, y hace cada vez más lenta la computadora, hasta que se paraliza por completo."

El desarrollo de nuevas tecnologías trae consigo nuevos riesgos. Una persona que tiene un celular austero que sólo sirve para hacer y recibir llamadas, y para mandar mensajes escritos, no de *WhatsApp*, que va a la ventanilla de un banco a depositar o sacar dinero, y que casi no utiliza su tarjeta de crédito, corre menos riesgos que quien está rodeado de tecnología y todo lo hace en línea, incluso la compra de la despensa semanal y sus citas con el médico.

"Pero la inteligencia artificial que anima a nuestras computadoras, tabletas, celulares y demás dispositivos debe ir aparejada de inteligencia humana; es decir, debemos saber cuáles son los riesgos que corremos al utilizarlos y, también, cuáles son las medidas que hay para prevenir daños, remediarlos o mitigarlos", finaliza Romo. ●