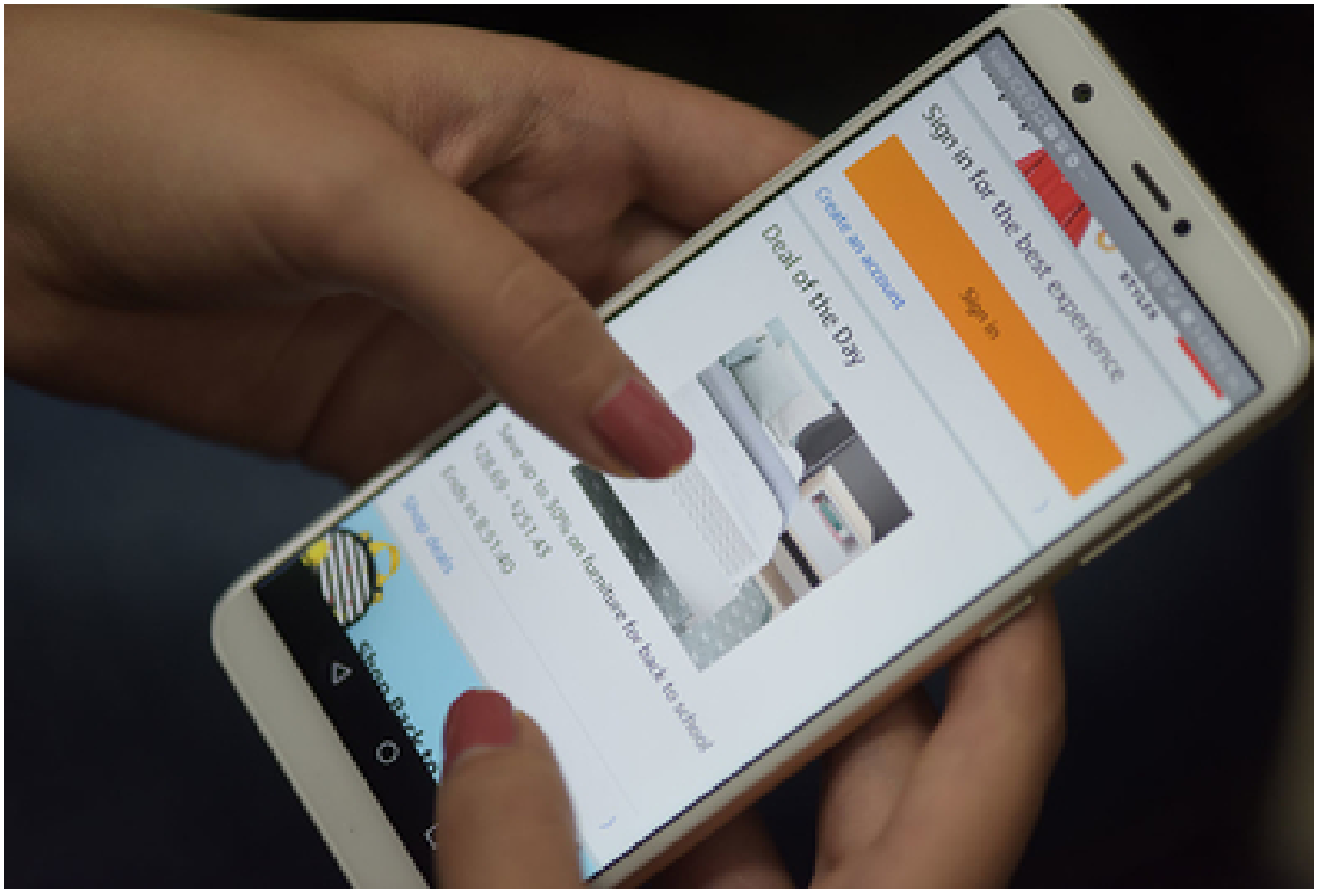
UNIVERSIDAD DE COSTA RICA

La pornografía infantil está entre los delitos informáticos que más crecen en Costa Rica

Las Jornadas 2018 Prosic-UCR abordaron la actualidad nacional en materia de ciberdelitos

29 AGO 2018 Ciencia y Tecnología



Las compras por Internet incrementaron en los últimos años. Esto ha agilizado el servicio para los proveedores y los usuarios, pero también genera mayores retos en términos de ciberseguridad para ambas partes. Foto: Anel Kenjekeeva.

Publicar fotos personales y familiares, conversar con amistades fuera del país por medio de teléfonos inteligentes, hacer compras en línea, sacar dinero de los cajeros automáticos, realizar trámites bancarios, solicitar transporte o comida a domicilio son acciones que realizan millones de personas diariamente. Sin embargo, todas y cada una de ellas requiere de la toma de medidas de seguridad para evitar los llamados **ciberdelitos**.

La responsabilidad de evitar los delitos en Internet no solo le corresponde a los proveedores de productos o servicios, sino también a **los usuarios, quienes deben tener cuidado al publicar o brindar datos**, que eventualmente pudieran ser utilizados por otras personas para cometer crímenes informáticos.

LEA TAMBIÉN: Informe Prosic-UCR 2018 Costa Rica da pasos esperanzadores en materia de Tecnologías de la Información y el Conocimiento

Esta fue una de las llamadas de atención hechas en las Jornadas 2018 sobre Ciberseguridad, del Programa Sociedad de la Información y el Conocimiento de la Universidad de Costa Rica (Prosic-UCR), realizadas durante los días 27 y 28 de agosto.

> "Estamos fascinados, estamos muy contentos de tener en nuestros celulares, en nuestros dispositivos, todo en la mano. Tenemos un celular que conecta remotamente, tenemos los bancos, tenemos los videojuegos, tenemos todas las páginas, tenemos bibliotecas. Estamos muy hipnotizados con el Internet, pero, nos hemos olvidado de darles medidas de seguridad a nuestros hijos, a nosotros mismos. Ahí es donde vienen los problemas que nos han afectado y han influenciado nuevos crímenes, y los delitos que vemos en la Institución, los cuales nos llevan a nosotros a realizar investigaciones", expresó Federico Vásquez Campos, de la Sección de Delitos Informáticos del Organismo de Investigación Judicial (OIJ).

Lamentablemente, uno de los delitos que más crece en los últimos años es el de pornografía infantil por vía dispositivos conectados a Internet. En este caso, el OIJ se enfrenta a diversas modalidades como la tenencia, producción, difusión, corrupción, seducción o encuentros con menores por medios electrónicos, informó Vásquez. En ese sentido, en el 2014 se investigaron 36 casos, mientras que en 2015 fueron 68. Y en adelante el promedio es de más de 40 casos por año, en los cuales se logra encontrar prueba; pero, se reportan muchas más situaciones en las que se investiga pero no se consigue recopilar los indicios necesarios para una acusación formal.

Otros delitos que se cometen por estos medios son la **estafa informática**, la **extorsión**, la **violación de correspondencia o comunicaciones**, la **suplantación de identidad**, la **violación de datos personales**, la **clonación de tarjetas.** El Organismo ha concluido que muchos de los crímenes podrían evitarse, al establecer medidas como tener mayor vigilancia sobre los menores de edad, no brindar datos sensibles a extraños, tener cuidado con lo que se publica en redes sociales, vigilar las tarjetas de débito o crédito, tener cuidado al visitar cajeros automáticos y similares.

Costa Rica a la vanguardia en materia legal

A pesar del aumento de la ciberdelincuencia, Óscar Serrano, fiscal de juicio y miembro de la Comisión de Derecho Informático, del Colegio de Abogados, considera que en Costa Rica se cuenta con una legislación robusta para hacer frente a este tipo de delitos, lo cual, incluso, según su criterio, pone al país a la vanguardia en este campo.

En ese sentido, el país es parte del Convenio de Budapest y del Convenio de Nassau, cuenta con la Ley de Delitos Informáticos del 2012, reformada en el 2013, y ya desde 1995

incluye en diferentes leyes de los ámbitos tributarios, de aduanas y de administración financiera, aspectos relacionados con estos temas.

ADEMÁS: Costa Rica logra reducir la brecha digital

Igualmente, se cuenta con cooperación internacional en el campo de la ciberdelincuencia de organizaciones como la Interpol, organizaciones especializadas en España, Colombia, República Dominicana y del FBI de los Estados Unidos, según reporta Vásquez.

Servicios financieros en el medio digital

La competencia internacional y las necesidades de los clientes hace que cada vez se brinden más productos y servicios por vía Internet y a través de distintos dispositivos como computadoras, tabletas, teléfonos inteligentes y otros, que le brindan a los usuarios una mayor facilidad y rapidez para hacer compras, trámites, obtener servicios y otros.

Esta tendencia no es ajena al sector bancario y más bien la gama de servicios que se brindan por Internet aumenta cada día, generando tanto en las entidades financieras, como en los usuarios una gran responsabilidad en el manejo de los datos que se acceden por los diferentes canales, sean cuentas bancarias, cajeros automáticos o tarjetas de crédito.

Para Roberto Valerio, jefe de Seguridad de la Información del Banco Nacional, existe una gran presión de la banca externa a la banca nacional, que se ve obligada a desarrollar productos y servicios en línea. "O te conviertes en un banco digital o estás fuera", expresa.

Empero, no solo la competencia aligera estos procesos sino también las necesidades de los clientes que, según Valerio, "quieren poder ser capaces de realizar cualquier transacción, desde cualquier dispositivo, en cualquier momento, en cualquier lugar. Ojalá sea un dispositivo móvil, ojalá sea desde la computadora, pero primero desde cualquier lugar, desde cualquier dispositivo, en un tiempo mínimo. Es decir que sea rápido, además, yo no quiero tener ningún tema de *back office*, yo no quiero que me atiendan por un canal digital y luego tener que ir al banco a finalizar un proceso".

Todo ello llama la atención a las entidades financieras sobre las medidas de seguridad que deben brindar a sus clientes en los servicios y productos que les ofrecen por Internet. Esto toma mayor relevancia si se toma en cuenta que **de acuerdo con datos del Foro Económico Mundial, del 2017, los ciberataques afectaron a personas en un trillón de dólares**.

En el ámbito financiero, todos los procesos se están moviendo hacia las plataformas digitales, "es una transformación del negocio a la parte digital", dice Valerio, quien considera que ello va a generar mucho más volumen, mayor tráfico y más transacciones no solo dentro del mismo banco sino en relación con el Banco Central y otras entidades financieras del país, a través de Sinpe. Esto hace que la superficie de ataque se amplíe, lo cual implica nuevos riesgos que no estaban contemplados cuando el servicio se brindaba en las propias oficinas.

Aparte de ello, se debe considerar si los clientes están preparados para poder afrontar este cambio vertiginoso que va del servicio en ventanilla al ofrecido en línea a través de dispositivos móviles o fijos.

Ante ello, las instituciones bancarias recomiendan a sus clientes no brindar ningún tipo de información personal por vía telefónica, fijarse que en los cajeros automáticos no haya objetos extraños en la ranura donde se inserta la tarjeta, y en el caso del pago en

comercios con tarjetas de débito y crédito no perderlas de vista, sino levantarse e ir a ver dónde se hace la transacción de pago.

Otras medidas que pueden tomar los usuarios de servicios financieros y específicamente de medios de pago, es el uso de tarjetas virtuales o la división del monto de crédito de la tarjeta, en varias tarjetas. También se recomienda revisar siempre los estados de las cuentas, sean estos de ahorro o de crédito, para verificar que no existan cargos erróneos, además de que se puede solicitar a los bancos la activación de alertas, de modo que les avisen cada vez que se use alguno de estos dispositivos de pago.

Para los bancos, el llamado es a efectuar análisis de riesgo y diseño de herramientas, y a realizar pruebas en sus sistemas, para brindar mayor seguridad a los clientes en el desarrollo de sus transacciones.

Nidia Burgos Quirós
Periodista, Oficina de Divulgación e Información
nidia.burgos@ucr.ac.cr

Etiquetas: prosic, universidad de costa rica, ciberdelitos, internet.