Seguridad Informática: qué nos dejó el 2020 y cuáles son los desafíos para el 2021

Desde el inicio del aislamiento social preventivo y obligatorio los delitos informáticos no pararon de crecer: casos de phishing, ciberacoso a niños y adolescentes, difusión de imágenes íntimas sin consentimiento con fines extorsivos, estafas digitales y tanto más. En paralelo, las denuncias en CABA también se incrementaron, según datos arrojados por la Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas (UFEDyCI) del Ministerio Público Fiscal de CABA.
El mayor uso de los dispositivos nos expuso a más vulnerabilidades y los ciberdelincuentes cada vez más agudizaron su ingenio para concretar los ataques. Se han valido del uso de la ingeniería social para llevarlos a cabo con una astucia inmejorable para engañar a sus víctimas y que sea más difícil descubrirlos.

Pero, dos cosas hemos aprendido de esta pandemia: la importancia de la concientización, y del uso responsable de nuestros dispositivos e internet, y de realizar las denuncias cuando ocurren este tipo de situaciones.

Los casos de phishing han estado, y están, a la orden del día. Más aun, el phishing bancario y los engaños a través de cuentas falsas en redes sociales. En las últimas semanas hemos conocido una fuerte campaña de difusión para alertar a todos los usuarios y clientes sobre los contactos falsos y la información que podemos compartir, pero fundamentalmente la que NO. De hecho, recientemente conocimos un fallo de la

Justicia platense a favor de una víctima de phishing bancario que dio lugar a un amparo para suspender los descuentos y retenciones de su cuenta.

Del mismo modo, nos alertamos por los crecientes casos de pornovenganza o extorsiones a partir de la divulgación de imágenes íntimas a raíz de compartir este tipo de contenidos con desconocidos o personas que no son de nuestra plena confianza. Situación que se agrava cuando el sexo virtual lo ponen en práctica adolescentes, quienes pueden ser engañados por adultos que comparten contenidos bajo la identidad falsa de un menor.

El delito de Grooming puso en alerta a adultos y niños, y destacó lo fundamental de hablar con nuestros hijos acerca de los riesgos que presenta internet y la práctica del sexting. Tal es así, que la discusión llegó al Congreso y hace tan solo unos días la Cámara de Diputados aprobó una nueva ley contra el ciberacoso que establece la creación de un Programa Nacional de Prevención y Concientización del Grooming o Ciberacoso contra Niñas, Niños y Adolescentes. A partir de ella, se busca prevenir, sensibilizar y generar conciencia en la población sobre la problemática del grooming o ciberacoso a través del uso responsable de las tecnologías de la información y la Comunicación, y de la capacitación de la comunidad.

¿Y las empresas?
La creciente digitalización de la información de las empresas ha permitido que durante la pandemia el home office haya sido una posibilidad para la gran mayoría de ellas. Pero, también planteó nuevos desafíos en torno a elevar sus niveles de protección, resguardo y concientización de los colaboradores.

Los ciberataques han sido muy frecuentes, sobre todo aquellos que han pretendido acceder a la información sensible digital. Por esta razón, que esté debidamente protegida y resguardada ha marcado un valor diferencial entre ellas. Otro desafío para las empresas lo ha planteado la readaptación necesaria para que sea posible el trabajo remoto, esto incluye contar con las herramientas y dispositivos necesarios; pero también, preparar a los colaboradores para que puedan hacerlo desde el punto de vista técnico y desde la seguridad de la información.

Dentro de las empresas generalmente estas áreas están manejadas por especialistas que se encargan de hacer respetar protocolos, detectar fallos y mantener los equipos resguardados. Pero, fuera de ella, en casa, la seguridad está a cargo de nosotros. Por eso, nuevamente, contar con un manual de buenas prácticas y capacitar habitualmente a los colaboradores en el buen uso de la información ha marcado la diferencia para hacerle frente a las intrusiones en esta época de Pandemia.

Perspectivas para el 2021
Para el año que viene es muy probable que los ataques sigan vinculados a la Pandemia y,

más aun, se incrementen. Nuevas amenazas de ransomware y malware en botnets serán los elegidos porque ya marcaron una tendencia en alza en 2020. Por eso, se plantea el desafío de que los dispositivos sean cada vez más seguros, sobre todo por la creciente cantidad que ya se encuentran, y se encontrarán, en uso.

El Covid-19 fue un acontecimiento de gran relevancia usado por los ciberdelincuentes para estar al acecho de nuevas oportunidades. Por esta razón, y aprendiendo de lo sucedido, hay que adelantarse y prepararse para adoptar medidas de seguridad de manera preventiva. Las empresas deberán proteger sus redes, los servicios en la nube, las aplicaciones y, sobre todo, la información.

Los usuarios no quedan exentos de estos peligros. Para estar alertas, todas las noticias vinculadas a la Pandemia pueden ser nuevamente un “gancho” utilizado por los ciberdelincuentes para engañarlos y convertirlos en sus víctimas. Por eso, una vez más enfatizo en la importancia de la educación y aprender a tomar conciencia sobre los riesgos a los que nos exponemos. Ser ciudadanos digitales cada vez más responsables del uso que hacemos de internet, de los dispositivos, y de la información que volcamos en ellos, es la clave para poder hacerle frente a ello.

Fuente: Ambito

(*) Perito Informático Forense, especialista en Seguridad – Socio del Estudio CySI de Informática Forense.