Alertas sobre fraudes y estafas en tiempos del COVID-19 ("coronavirus")

El COVID-19 creó consecuencias impensadas para nuestra sociedad. El crimen organizado rápidamente respondió, creando campañas armadas a gran escala para defraudar a clientes de entidades financieras y otras, y robar datos personales, abusando del miedo y de la ansiedad relacionados con el COVID-19.

Marzo de 2020

En estos tiempos difíciles y de gran incertidumbre, los defraudadores abusan del miedo, la necesidad y el estado de imprevisibilidad creado por la emergencia de la salud pública, buscando obtener un beneficio a partir del deseo de la sociedad de volver al estado de seguridad y protección.

Alrededor del mundo, hemos visto un creciente aumento en las estafas asociados al COVID-19. Si bien en Argentina no se conocen casos denunciados sobre estafas virtuales relacionadas con el COVID-19, en el resto del mundo sí están sucedido y con cifras en ascenso. Las víctimas son típicamente contactadas vía teléfono, email o redes sociales.

Adicionalmente, como los gobiernos se encuentran preparando paquetes de medidas en respuesta a la pandemia, y están comenzando a proporcionar apoyo fiscal a la sociedad, el riesgo de ser defraudado por estafas relacionas con el COVID-19 probablemente continuará en crecimiento.

Algunas de las estafas relacionadas al COVID-19 incluyen:

— **Phishing:** defraudadores simulando ser miembros de una autoridad de salud nacional o internacional, como ser el Ministerio de Salud de la Nación o de las Provincias, Centro de Control y Prevención de Enfermedades de Estados Unidos ("CDC" por su sigla en inglés), o la Organización Mundial de la Salud ("OMS" o "WHO" por su sigla en inglés), dirigiéndose a sus víctimas a través de emails con adjuntos maliciosos, links, o redireccionamiento a actualizaciones sobre la propagación del COVID-19, nuevas medidas de contención, mapas del brote o maneras para protegerse a uno mismo de la exposición al virus. Una vez abierto, la computadora puede ser infectada con un malware (software malicioso) o podemos exponer a un hacker la información personal o datos de tarjetas de crédito guardadas online.

— **Sitios webs fraudulentos del COVID-19:** ha existido un significativo incremento en nuevas tipologías de riesgos de fraude y, en

particular, aquellos relacionados con el gran número de registración de dominios de internet con el término "COVID".

— **Comprometer el email corporativo**: el aumento del trabajo remoto (o "home office"), acompañado de actualizaciones sobre el COVID-19 a toda la compañía, han abierto un camino a los defraudadores para atacar a las compañías y sus empleados. Utilizando emails encubiertos, como actualizaciones sobre el COVID-19, los defraudadores intentan engañar a los empleados para que entreguen sus credenciales solicitándoles el ingreso al portal de una compañía falsa de "COVID-19". Una vez que los empleados ingresaron sus credenciales, el defraudador puede tener acceso irrestricto a las cuentas de los empleados de la compañía y a su intranet.

— **Estafas de abastecimiento o suministro**: aprovechando de la escasez de ciertos productos, demoras en entregas y la desesperación de la población por recursos, los defraudadores establecieron tiendas online falsas que venden suministros médicos de gran demanda, tales como barbijos, máscaras, guantes de látex y desinfectantes de manos (alcohol en gel). Luego de que el pago es realizado para la compra de los productos, los defraudadores se apropian del dinero y nunca entregan los suministros.

— **Estafas en tratamientos**: el aumento del pánico por contraer el coronavirus ha creado un sector de la población en la búsqueda de cómo prevenir o curar el COVID-19. Utilizando las redes sociales o fórums online, los defraudadores promocionan productos falsos afirmando la prevención del virus y atraen a las víctimas con la promesa de vacunas, curas falsas y tratamientos no probados.

— **Estafa con proveedores**: los defraudadores se hacen pasar por doctores o administradores de hospitales, generalmente afirmando que han tratado con éxito a un amigo o un pariente con COVID-19, y solicitan el pago por dicho tratamiento.

— **Estafa de caridad**: en los tiempos de crisis, es muy común que los individuos sientan una sensibilidad especial sobre la responsabilidad de ayudar para reducir el impacto en la comunidad. Los defraudadores se encuentran a la caza de ese deseo, solicitando donaciones de organizaciones benéficas que no existen para ayudar a los individuos, grupos o áreas afectadas por el coronavirus, o para contribuir en el desarrollo de una vacuna.

— **Estafas vía aplicaciones para celulares**: los defraudadores se encuentran desarrollando o manipulando aplicaciones para celulares, las cuales externamente aparentan seguir la dispersión del COVID-19. Sin embargo, una vez instalada, la aplicación infecta el dispositivo con un malware que puede ser utilizado para obtener información personal, datos sensibles, cuentas de banco o datos de tarjetas de crédito.

— **Estafa en inversiones**: continuando con la tradición de la clásica estafa a través de inversiones, este esquema tiene un giro, pretendiendo generar grandes retornos de una inversión en una compañía que posee servicios o productos que pueden prevenir, detectar o curar el COVID-19.

Hay muchas maneras y formas de protegerse uno mismo, a nuestros seres queridos y a los negocios de ser víctima de las estafas relacionadas con el COVID-19. Para reducir la vulnerabilidad, es crucial y primordial asegurar que la gente, los equipos y la sociedad estén alerta y advertidos sobre cómo los criminales están intentando tomar ventaja de esta crisis global de la salud.

Entonces, ¿qué podemos hacer para protegernos?

— Ser cautelosos de emails fraudulentos que afirman que son de expertos que tienen información clave relacionada con el coronavirus. No hacer click en los links o abrir adjuntos de personas desconocidas o no verificadas.

— Verificar las direcciones de emails de fuentes que dicen poseer información relacionada con el COVID-19 sobre irregularidades, tales como errores ortográficos o símbolos. Los defraudadores suelen utilizar direcciones que sólo poseen diferencias mínimas de aquellas que pertenecen a las personas que intentan imitar.

— Ser cuidadosos de comercios/tiendas online falsos que usan métodos/medios de pago no tradicionales, como ser money order (giro postal), gift cards, transferencias de fondos o crypto-monedas.

— Hacer búsquedas de antecedentes antes de realizar donaciones a cualquier organización benéfica o campañas de financiamiento colectivo.

— Asegurar que los programas (software) antivirus y anti-malware instalados en los dispositivos estén actualizados.

— Estar informado sobre las tendencias en estafas relacionadas con el COVID-19.

— Para obtener la información más actualizada sobre el COVID-19, visitar el sitio del Miniterio de Salud de la Nación.

Contactos locales

Diego Bleger
Socio Líder de Forensic Services
KPMG en Argentina

Ana López Espinar
Socia de Forensic Services
KPMG en Argentina

Hernán Carnovale
Socio de Forensic Services
KPMG en Argentina

Adriano Mucelli
Socio de Forensic Services
KPMG en Argentina