DIPUTADOS
ARGENTINA

PROYECTO DE RESOLUCIÓN

La Cámara de Diputados de la Nación

RESUELVE:

Solicitar al Poder Ejecutivo que, a través de los organismos que correspondan, implemente campañas masivas de comunicación donde se alerte a la comunidad del aumento de ciberdelitos desde el comienzo de la pandemia por COVID-19 y se articule el correspondiente asesoramiento acerca de la prevención y defensa.

DIPUTADOS
ARGENTINA

FUNDAMENTOS

Señor Presidente:

Desde el comienzo de la pandemia de COVID-19, la Organización Mundial de la Salud ha observado un extraordinario incremento del número de ciberataques dirigidos contra su personal, así como de las estafas por correo electrónico contra el público en general.

Cada minuto se registran 49 ciberataques en la Argentina. En la mayoría de los casos se trata del ardid conocido como phishing, un engaño digital con el que se intenta convencer a usuarios de registrar sus datos secretos en páginas falsas armadas por piratas informáticos. Los trucos básicos apuntan a duplicar páginas de entidades bancarias en procura de capturar claves. Otros esquemas son mas sofisticados en busca de atrapar información sensible mediante el uso de lo que se conoce como ingeniería social.

Para algunos, las crisis, como la del coronavirus, son la excusa perfecta para hacer de la suyas y perjudicar de ese modo al resto de las personas que no tiene o no puede tener conocimiento de lo que se enfrenta.

La Agencia de Ciberseguretat de Catalunya ha alertado ya en marzo de un incremento de la actividad cibercriminal aprovechando “la situación de excepcionalidad” por el Covid-19 para difundir campañas con el fin de obtener datos sensibles.

La OMS dio a conocer el caso en el que estafadores se hacen pasar por personal de ellos, a través de correos electrónicos, con intención de canalizar donaciones a un fondo ficticio y no al autentico

Fondo de Respuesta a la COVID-19. El numero de ciberataques que ha recibido la Organización hasta ahora es mas de cinco veces mayor al sufrido en el mismo periodo del año pasado.

Por otro lado, la oficina de Coordinación Cibernética (OCC) del Ministerio del Interior ha realizado un estudio en relación con los ciberdelitos más comunes en este momento y, de este modo, poder o intentar prevenirlos. Por tal motivo, no encuentro mejor manera de hacerlo que alertando a la población mediante una campaña de comunicación masiva.

El análisis hecho por la OCC se extiende del 13 de enero al 20 de abril y revela que el incremento de la cantidad de personas que llevan a cabo su ocupación laboral en el modelo teletrabajo ha provocado un cambio en la modalidad de los ciberataques. Las estafas, seguidas del robo de credenciales mediante phishing y de los ficheros maliciosos, encabezan la lista de los ataques más comunes detectados en todo el mundo.

La Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) informó sobre las nuevas modalidades de ciberdelitos que se detectaron durante el aislamiento social preventivo y obligatorio. Frente a ello, anuncio distintas recomendaciones para evitar ser victimas de las diferentes maniobras entre las que se destacan la práctica de "zoombombing" y de extorsión a través de envíos de mails, en donde los victimarios les hacen creer a sus victimas que accedieron al contenido de sus dispositivos digitales.

Otra de las prácticas que se sucedieron en los últimos días son las maniobras fraudulentas materializadas por medio de correos electrónicos, que se basan en la afirmación de haber accedido a los dispositivos de las victimas y registrado, mientras visitaban sitios de contenido para adultos, la pantalla y las imágenes captadas por sus

cámaras web. La estafa consiste en el envío de un mail a la víctima, en donde se incluye en el texto una contraseña utilizada en alguna oportunidad por el afectado, o simulando que el mensaje fue enviado desde su propio correo electrónico, con el fin de generar mayor nivel de convencimiento para después exigir un pago, bajo la amenaza de distribuir grabaciones o contenidos injuriantes entre sus contactos personales en caso de no cumplir.

Además, la UFECI identificó una variante novedosa de un fenómeno sobre el que ya había advertido, se trata de una modalidad en la que, por medio de llamados telefónicos, personas que simulan ser trabajadores de la ANSES u otros organismos públicos engañan a sus víctimas para recolectar información personal, financiera e, incluso, datos de sus tarjetas de crédito o débito. En ocasiones, se pide a los damnificados que se acerquen a un cajero automático y, una vez allí, los guían para que realicen transferencias a cuentas de terceros.

Desde que inicio la pandemia por el coronavirus, advierte la International Association of Internet Hotlines (Inhope), en el mundo, se triplicó el tráfico de material de explotación sexual de niños, niñas y adolescentes en Internet.

En un contexto donde la hiperconectividad volvió a todos, pero principalmente a los chicos y chicas mucho mas vulnerables, es necesario el rol de los adultos y del Estado en la prevención y detección temprana de todos los tipos de ciberdelitos que existen.

Por todos los motivos expuestos, solicito a mis pares acompañen el presente proyecto de resolución.