CHARLA INFORMATIVA SOBRE DELITOS INFORMATICOS REALIZADA CON LA DIVISION ESPECIALIZADA DE LA POLICIA DE LA CIUDAD EL JUEVES 29 DE JULIO DE 2021

La Superintendencia de Tecnología Informática realizó una reunión virtual el 29 de julio ppdo; con la intervención del Crio. Carlos Daniel Vrancovich, titular de la Dirección de Desarrollos Informáticos de la Policía de la Ciudad quien saludó a los participantes en la misma, informando que dicha dependencia es la encargada de realizar capacitaciones de tecnología informática así como de temas institucionales como también capacitaciones y charlas para los vecinos, centradas en la metodología de dichos delitos y dar herramientas para la prevención de los mismos. Informa que desde el comienzo de la pandemia, dichos delitos se potenciaron en un 5.000 %; señala que casi todos en este rubro se nutren fundamentalmente de información que es dada por los propios vecinos. -ello incluye distintos tipos de delitos- sobre los cuales expondrán los funcionarios a cargo de la charla -, Crio. Gastón Fecit y Sub-Crio. Sergio Ibarra , señalando el primero de ellos que hay que tener en cuenta que la misma está dirigida tanto a quienes usan tecnología como a quienes no la usan pero sin embargo, no van a ser ajenos a su uso. Se exhibe un cuadro demostrativo de la penetración de internet a nivel global; en enero de 2021 el 80% de la población usa internet, y que estamos sobre la media mundial: 59.5 %.
Otro ejemplo de uso son las redes sociales; entre las ofertas de esos servicios, aparece Instagram que es la red social más usada, pero está abajo de Facebook, You Tube, etc. En You Tube, hay mucha gente que ve tutoriales o películas, música, etc. Existe mucha gente que piensa que Internet es malo: Pero, que pasaría, si no la tuviésemos. 4.000.000 millones de personas en el mundo la utilizan. En Google, por ej. hay 80.000.- personas que trabajan a tiempo completo. Internet no es bueno ni malo; pero lo cierto es que simplifican nuestras necesidades cotidianas. Facebook tenía en 2018- 1.900 millones de usuarios y en 2020 , 2.300 millones mientras que e-commerce en los referidos años paso de 880.000 a 1,2 millones y Tic-Tok que en 2019 no era significativa, hoy ha pasado a serlo. Netflix: En 2018: 80.000 usuarios por hora y actualmente tiene 764.000 por hora.
Por ello, hay que tener en cuenta cuanta información damos al publicar en las redes sociales. Hay que pensar en lo que pasa con la gente que detrás de la pantalla accede a los perfiles de los entrevistados. El uso de la tecnología deja rastros que son como huellas en las distintas redes sociales que usamos y que hacen a la identidad digital. Hay 3 franjas que podemos distinguir entre los usuarios de Internet: 1) Millenial: 90,4%; Generación X: 77,5% y Baby Boomers: 48,2%. Uno de los aspectos más importantes a considerar es el referido a quienes conviven en las redes sociales. En los últimos días una candidata en las próximas elecciones- Sabrina Ajmetech, fue señalada por sus opiniones sobre temas muy sensibles en el pasado: su twist de 2013 "Haga patria, mate un judío" y otro mensaje más reciente “las Malvinas no existen para Argentina, les pertenecen a los ingleses” esto fue reflotado por Carlos Maslatón y Alicia Castro. Ahora EE.UU. para obtener la visa Norteamericana te requiere datos de tus redes sociales. El Sexting: No es un delito; se trata del intercambio voluntario por medios tecnológicos de imágenes o conversaciones de carácter erótico y sexual. Nada lo prohíbe y la constitución lo ampara, pero encierra Peligros potenciales: por ej. daños a la imagen, perdida de intimidad, chantaje, extravíos, sextorsión, acoso, ciberacoso. Delitos de pornografía infantil, es otra variante

de delito tecnológico. Suplantación de identidad es un ciber delito: una persona se apropia de datos de otras con el objetivo de acceder a información que puede utilizarse para distintos delitos cibernéticos. Grooming: acoso sexual a niños/as adolescentes, perpetrado por un adulto que se hace pasar por un menor para cometer delitos sexuales. En el caso de estas posibles víctimas, como padres es necesario que conozcamos que hace el niño o adolecente con los juegos electrónicos, hay que involucrarse con el control de su uso y que sepan que no hay que dar datos de identidad y si nuestro ser querido es engañado con esta modalidad hay que denunciar al groomer; cada uno tiene entre 1 y 17 perfiles que les permite acceder a entre 35 y 50 posibles víctimas. Hay que saber que la denuncia tiene el beneficio del anonimato. Phising: es una forma de estafa por medio de la cual se obtienen usuarios y contraseñas a través de medios tecnológicos que procuran que les demos información. El objetivo principal de esta modalidad es económico. Hay otras variantes de estafa como el Vishing: aquí se usan medios telefónicos o mensajes de voz que utiliza ingeniería social. Aquí se alude a un tema que nos provocará alarma o que resulte de nuestro gran interés. El impostor pasa por ser integrante de una empresa u organismo reconocido de prestigio o simular ser páginas oficiales. También el Smishing: aquí se basan también en la actualidad, en una situación que afecte a la población en general o que es de público conocimiento. La oportunidad de estos delitos, parte de que, él **ahora es inminente.** En el caso de los bancos: la clave de acceso a Home Banking. Y en el de plataformas de videos Streaming: Netflix, HBO, y respecto a las tarjetas de crédito es el URL (dominio). También esta técnica en correo electrónico referidos a entidades oficiales (hay que tener en cuenta la observación del sistema cuando figura la mención de que el sitio invocado **“no es seguro”** cuando se consigna lo que pretende ser un mensaje del GCBA., Bs.As. Ciudad, Metrogas, de los que surgen logos y llamados que nos dirigen; hay que mirar el n°5050147 que es de la Ciudad. Estos mensajes falsos pueden surgir a partir de la venta de basas de datos o bien por la existencia de un empleado infiel, por ej. en llamadas, etc. Skimming: es una técnica delictiva utilizada en cajeros automáticos- Hay un gráfico consignando: Tarjeta- apertura- 1er. consejo de seguridad. No hay que usar la tarjeta de débito para operar sino cualquier tarjeta que tenga banda magnética o tarjeta azul. Hay que estar alerta al aspecto referido a elementos no visibles que los delincuentes colocan en el cajero, por ej. adosar un teclado falso al del cajero o cualquier otro aditamento que usen para obtener nuestros datos operativos; se ha conocido que el delincuente puede adosar y esperar a que varios clientes operen sin ser afectados ya que así pueden colectar mayor cantidad de datos de los futuros afectados por la maniobra. Se recomienda que el usuario que advierta algo extraño, no habitual en el cajero o algún elemento desconocido, no opere y se comunique rápidamente con el 911. Hay un aparato- contac less (NFC) que clona hasta 20 tarjetas- pesa menos de 15 gramos y dura 3 horas, capta y copia n° de tarjeta, su titular y datos de operaciones, cuesta 85 u$s -; hay un objeto que puede neutralizar las ondas magnéticas con aluminio para neutralizar el papel. En el mundo que nos toca vivir hoy tenemos que manejarnos con sumo cuidado; prueba de ello es que los Bancos retiraron sus informaciones en Internet. Otro aspecto importante son las consultas sobre cómo responder a llamadas de dudosa procedencia, y de las que a modo de ej. Se consignan:

Preguntas del extorsionador:	**Respuesta a dar:**
Con quien hablo?	A quién necesita?
De donde me contestan?	A quien llamó?
Yo sé que Ud. tiene o Ud. es?	Creo que Ud. está mal informado
Lo tenemos vigilado	Que traigo puesto?
Papá, estoy secuestrado	Cuál es el nombre de los abuelos
Hola tío/a	Cuál es el nombre de su tío/a
Ídem: primo	Con qué primo quiere hablar?

Lo llamo de.... para actualizar sus datos

Ud. es el feliz ganador de....	Ud. está equivocado

TOP FIVE PARA UNA INTERNET SEGURA:

1) Tener antivirus actualizado (anti malware) ícono del candado de seguridad

2) Sitios seguros/ aplicaciones seguras/ Nunca acceder a links de un e-mail no conocido/ activar el doble factor de seguridad icono del candado httpsh (lugar seguro)

3) Contraseñas fuertes; cambiarlas regularmente; no usar la misma para todo; desechar las fácilmente deducibles; por ej. armar con distintos signos- 1b@Rr4.03 candado de seguridad.

4) No revelar información sensible - ojo con los posteos.

5) Políticas de privacidad: Controlar periódicamente mis amistades en redes sociales y que hacemos con ellos. Ante solicitudes extrañas consultar periódicamente. Lo importante es la denuncia!!! porque sin ellas no se puede hacer nada. Se aclara que las infografías ilustrativas del aspecto abordados son: mundial: 1)Wi art. y la 2) nacionales. Reiteran no hacer click en el link que no conocemos y no abrirlo. Informan los expositores que la charla no se graba; si los invitan ellos dan las charlas.

Varios participantes expresan su complacencia y agradecimiento por el carácter de dialogo ameno utilizado por los funcionarios expositores que le dió un carácter dinámico a la reunión.

INFORME POR ALBERTO SILBER (COMISION DE SEGURIDAD)

CONSEJO CONSULTIVO COMUNA 7