RESPUESTA DEL MINISTERIO PÚBLICO FISCAL DE LA CABA ANTE ESTE FENÓMENO

Los ataques contra la integridad de los dispositivos o sistemas informáticos abarcan gran cantidad y diferentes tipos de maniobras, desde un mero acceso ilegítimo al sistema informático de un ciudadano que luego puede derivar en el borrado y/o modificación de sus archivos, hasta ataques distribuidos de denegación de servicios que paralizan diferentes sistemas proveedores de servicios a través de la web, mediante incesantes consultas que colapsan la capacidad de respuesta del sistema informático. Estos ataques, han afectado lo que se denomina infraestructuras críticas, que son aquéllos servicios fundamentales para el desarrollo de la sociedad, como hospitales y aeropuertos -entre otros-.

La UFEDyCI también cuenta con protocolos de intervención inmediata en estos casos, siendo necesario una vez puestos en conocimiento de la Unidad Fiscal los hechos y, de forma inmediata, asegurar la evidencia digital debido a la alta volatilidad que esta presenta y el claro peligro de eliminación de aquélla evidencia que pueda permitir la identificación de los autores de la maniobra. Asimismo, resulta fundamental conocer acabadamente la maniobra, detectando si el ataque se dio a través de un virus informático, malware o código malicioso; analizar los servidores por parte de personal especializado de acuerdo a las buenas prácticas forenses; entre otras medidas según las características propias del caso.

PANORAMA ACTUAL EN ÉPOCA DE COVID-19

Interpol ha publicado un informe el día 26 de marzo de 2020[2] , donde advierte sobre un marcado aumento en incidentes de delitos cibernéticos que se adaptan alrededor de aspectos del coronavirus, y apuntan a organizaciones y víctimas desprevenidas, indicando que se ha verificado un aumento en la cantidad malware que usan la pandemia COVID-19 para infectar los sistemas informáticos de individuos y organizaciones. Asimismo, resalta que se ha verificado también que los hospitales se han convertido en el foco de ciberataques y, por otra parte, que debido a la cantidad de gente que trabaja bajo la modalidad "home office", se presentan riesgos y vulnerabilidades adicionales que los ciberdelincuentes pueden intentar explotar.

Europol, en el informe ya indicado, advierte también sobre un probable aumento de ataques de denegación distribuido de servicios, en virtud del significativo aumento en el número de personas que trabajan de forma remota desde su hogar, lo que ha empujado el ancho de banda al límite.

En este sentido, también se ha verificado un aumento de casos de *"ransomware"*

RANSOMWARE:

Tal como lo define Europol, el ransomware es un tipo de software malicioso que los delincuentes utilizan para capturar archivos de un dispositivo y cifrarlos, denegando el acceso a los mismos por parte de los usuarios legítimos y solicitando un pago para su recuperación. En general, los autores solicitan dicho pago en forma de bitcoin o alguna otra moneda virtual y, en su defecto, proceden la eliminación definitiva de los archivos alojados en dichos sistemas. De ello se desprende que el objetivo principal es la ganancia financiera.

[2] Europol, "Catching the Virus. Cybercrime, desinformation and the COVID-19 pandemic". 3 april 2020.

CONSEJOS ÚTILES

INTERPOL, A TRAVÉS DEL INFORME MENCIONADO, HA BRINDADO UNA SERIE DE DIRECTIVAS ÚTILES A LA HORA DE EVITAR ESTE TIPO DE ATAQUES CONTRA SISTEMAS Y DATOS INFORMÁTICOS

- EVITAR ABRIR CORREOS ELECTRÓNICOS SOSPECHOSOS Y CLICKEAR ENLACES EN CORREOS ELECTRÓNICOS Y ARCHIVOS ADJUNTOS NO RECONOCIDOS;
- HACER COPIAS DE SEGURIDAD DE LOS ARCHIVOS EN LÍNEA Y OFF LINE REGULARMENTE Y CON SEGURIDAD,
- UTILIZAR CONTRASEÑAS SEGURAS;
- MANTENER ACTUALIZADO EL SOFTWARE, INCLUIDO EL ANTIVIRUS;
- ADMINISTRAR LA CONFIGURACIÓN DE LAS REDES SOCIALES Y REVISAR LA CONFIGURACIÓN DE PRIVACIDAD Y SEGURIDAD; FORTALECER LA RED DOMÉSTICA;
- EDUCAR A LA FAMILIA, ESPECIALMENTE A LOS NIÑOS, SOBRE CÓMO MANTENERSE SEGUROS EN LÍNEA;

SUPLANTACIÓN DIGITAL DE IDENTIDAD

Con el auge de las redes sociales en los últimos años, se ha detectado un gran número de casos en los que se utilizan imágenes o datos de una persona para crear un falso perfil en diferentes redes sociales, páginas web, envío de correos - entre muchos otros canales digitales, sin autorización de la persona afectada.

DIFUSIÓN DE IMÁGENES Y GRABACIONES ÍNTIMAS NO AUTORIZADAS

Dentro del universo de conductas que tienen lugar en el ciberespacio, se advierte un notable crecimiento de aquéllas que tienen por fin la publicación y/o difusión de imágenes o videos captados en la intimidad, sin autorización, y que tienen relación con la sexualidad. Muchas veces, estas conductas se dan dentro de supuestos de violencia de género. Varios países han decidido incluir estas conductas como delitos en sus legislaciones internas. Si bien Argentina se encuentra analizando esa posibilidad en el Congreso, la Ciudad Autónoma de Buenos Aires ha previsto ciertos supuestos de difusión de imágenes íntimas no autorizadas en la legislación local, a través del Código Contravencional.

LEGISLACIÓN DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES

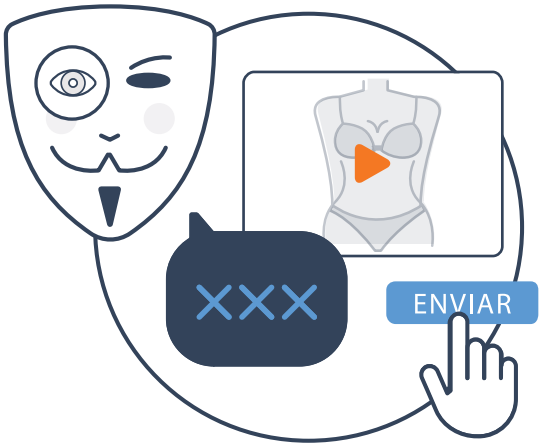
Si bien las conductas de suplantación de identidad y la difusión no autorizada de imágenes íntimas no han sido receptadas aún como figuras penales en la Argentina, la Legislatura de la Ciudad Autónoma de Buenos Aires ha incorporado al Código Contravencional que rige en la CABA y respecto de los cuales la UFEDyCI tiene competencia, los siguientes artículos:

> *"Artículo 71 quinquies: Suplantación Digital de la Identidad. Quien utiliza la imagen y/o datos filiatorios de una persona o crea una identidad falsa con la imagen y/o datos filiatorios de una persona mediante la utilización de cualquier tipo de comunicación electrónica, transmisión de datos, página web y/o cualquier otro medio y se haya realizado sin mediar consentimiento de la víctima, siempre que el hecho no constituya delito es sancionado con una multa…trabajo de utilidad pública… o días de arresto…"*

Las sanciones se elevan al doble en determinados supuestos previstos en la norma, indicándose asimismo que resulta ser una acción dependiente de instancia privada, que el consentimiento de una víctima menor de 18 años de edad no será considerado válido y, por último, la norma prevé que no configura suplantación de identidad el ejercicio del derecho a la libertad de expresión

“Artículo 71 bis- Difusión no autorizada de imágenes o grabaciones íntimas. Quien difunda, publique, distribuya, facilite, ceda y/o entregue a terceros, imágenes, grabaciones y/o filmaciones de carácter íntimo sin el consentimiento de la persona y a través de cualquier tipo de comunicación electrónica, de transmisión de datos, páginas web y/o a través de cualquier otro medio de comunicación, siempre que el hecho no constituya delito, es sancionado con multa… días de trabajo de utilidad pública… arresto…”

La norma aclara que el consentimiento de la víctima para la difusión, siendo menor de 18 años, no será considerado válido. Tampoco podrá alegarse el consentimiento de la víctima en la generación del contenido como defensa a la realización de la presente conducta. Resulta ser un delito dependiente de acción privada, con excepción de los casos en los que la víctima sea menor de 18 años de edad. Aclara la norma que no configura contravención el ejercicio del derecho a la libertad de expresión.



PANORAMA ACTUAL EN ÉPOCA DE COVID-19

La UFEDyCI ha registrado un aumento significativo de denuncias relacionadas a la suplantación de identidad en diferentes redes sociales, muchas veces siendo afectados niños, niñas y adolescentes cuyos datos e imágenes publicados en sus redes sociales, son utilizados para la creación de perfiles falsos y posterior contacto de sus autores con otros menores. Asimismo, y debido al aislamiento obligatorio impuesto, han cobrado relevancia las denuncias de difusión de imágenes íntimas no autorizadas.

Los supuestos y diversidad de los casos son amplios, pero a modo de ejemplo pueden destacarse casos de relaciones sentimentales ya finalizadas, en virtud de las cuales se procedió al envío de imágenes íntimas las que hoy en día son publicadas en distintos sitios o enviadas a contactos de la persona afectada. Se han advertido también la fusión de las dos conductas antes apuntadas, es decir, la creación de un perfil falso en las redes con imágenes y datos de la víctima, en donde se difunden posteriormente videos o fotos íntimas.

ESTRATEGIAS ACTUALES IMPLEMENTADAS POR LA UFEDyCI EN EL MARCO DE LA CUARENTENA DECRETADA

UNA VEZ RECIBIDAS LAS DENUNCIAS, LA UNIDAD REALIZA EN FORMA REMOTA DIFERENTES MEDIDAS

- CONTACTO TELEFÓNICO INMEDIATO CON LAS VÍCTIMAS, A FIN DE INDAGAR SOBRE LOS HECHOS DENUNCIADOS Y ESPECIFICAR CIERTOS ASPECTOS INDICADOS EN LA DENUNCIA.

- VERIFICACIÓN DE LOS PERFILES E IMÁGENES/VIDEOS DIFUNDIDOS A TRAVÉS DEL CUERPO DE INVESTIGACIONES JUDICIALES, CON LA DEBIDA PRESERVACIÓN DE ACUERDO A LAS BUENAS PRÁCTICAS FORENSES PARA, EVENTUALMENTE, UTILIZAR ESA EVIDENCIA EN JUICIO.

- CONSTATACIÓN FEHACIENTE DE LAS REDES SOCIALES Y CORRECTA IDENTIFICACIÓN DEL PERFIL –EJ: ID EN FACEBOOK- PARA REALIZAR POSTERIORES PEDIDOS A LAS EMPRESAS PRESTATARIAS DE SERVICIOS EN INTERNET.

- SOLICITUD DE DATOS INFORMÁTICOS SOBRE LOS PERFILES, SITIOS Y CUENTAS INVESTIGADAS CON EL OBJETO DE CONTAR CON DATOS INFORMÁTICOS QUE NOS PERMITAN IDENTIFICAR A LOS AUTORES DE LOS HECHOS. ELLO, SE REALIZA CON INTERVENCIÓN DEL JUEZ, A TRAVÉS DE LOS SISTEMAS INFORMÁTICOS DEL MINISTERIO PÚBLICO FISCAL Y DEL CONSEJO DE LA MAGISTRATURA, EN FORMA REMOTA. UNA VEZ AUTORIZADO EL PEDIDO DE INFORMACIÓN O CONTANDO CON EL OFICIO DIGITAL DEL JUEZ, SE PROCEDE A ADELANTAR LOS REQUERIMIENTOS A LAS EMPRESAS PRESTATARIAS DE SERVICIOS DE INTERNET, A TRAVÉS DE LOS PORTALES DIGITALES CORRESPONDIENTES.

- EVENTUAL SOLICITUD DE BAJA DE LAS IMÁGENES Y VIDEOS DIFUNDIDOS EN SITIOS WEB, DE ACUERDO AL ANÁLISIS DE CADA CASO.

CONSEJOS ÚTILES

ADEMÁS DE LOS CONSEJOS INDICADOS EN LOS DIFERENTES ATAQUES INFORMÁTICOS, A FIN DE FORTALECER LA SEGURIDAD DE LOS DISPOSITIVOS Y EVITAR EL ROBO DE DATOS, IMÁGENES Y VIDEOS ALOJADOS EN LOS DISPOSITIVOS, SE RECOMIENDA:

- NO BORRAR LAS CONVERSACIONES MANTENIDAS, EN SU CASO, CON LOS AUTORES DE LAS MANIOBRAS.
- REALIZAR EN FORMA INMEDIATA LA DENUNCIA A FIN DE QUE SE PRESERVE CORRECTAMENTE LA EVIDENCIA NECESARIA PARA INICIAR LA INVESTIGACIÓN.
- APORTAR TODOS LOS DATOS DE AQUÉLLAS PERSONAS CON LAS CUALES EL/LOS PERFILES HAYAN MANTENIDO CONTACTO.
- NO COMPARTIR IMÁGENES, VIDEOS ÍNTIMOS NI INFORMACIÓN PERSONAL CON PERSONAS DESCONOCIDAS, O CONOCIDAS SÓLO A TRAVÉS DE REDES SOCIALES.
- RESTRINGIR LA INFORMACIÓN PERSONAL QUE SE PUBLICA A TRAVÉS DE LAS REDES SOCIALES.

OTRAS ACTIVIDADES FOMENTADAS EN TIEMPOS DE CUARENTENA

Desde la UFEDyCi, creemos que una adecuada prestación de justicia, no sólo demanda la eficiente administración e investigación de casos, de acuerdo a las últimas tendencias a nivel mundial para combatir el Cibercrimen.
A diferencia de otras áreas delictivas, las distintas maniobras realizadas por los autores de conductas cometidas en el ciberespacio, van mutando y perfeccionándose día a día, a la par del avance de la tecnología.

Esto demanda una capacitación constante por parte de todas las personas que intervienen en la investigación de este tipo de conductas, debido a que, sólo si entendemos y conocemos las características propias y alcances de las maniobras desplegadas - incluyendo su faz técnica -, podrán ser correctamente analizadas a la luz de la legislación vigente tanto a nivel de fondo como procesal.

Entender acabadamente las implicancias jurídicas que tienen estas conductas cometidas en el ciberespacio, es la única manera de afrontar en forma seria y eficaz la problemática.

Asimismo, los avances tecnológicos y la aparición de nuevas redes sociales y aplicaciones de mensajería instantánea, otorgan nuevos espacios para que los delincuentes desarrollen sus actividades ilícitas, adoptando formas y características disímiles. Por ello, resulta fundamental mantener informada a la sociedad y trabajar sobre el área de prevención.

Esto permite, por un lado, mantener a los ciudadanos informados sobre los nuevos peligros que van surgiendo en relación a su vida e identidad digital, evitando que se conviertan en víctimas de ciberdelitos. Por otro lado, brinda la posibilidad de conocer paso a paso cómo actuar en caso de ser víctima de un delito informático, permitiendo que la Justicia cuente con la información necesaria para iniciar una investigación e identificar a sus autores.

CAPACITACIÓN

De acuerdo a estos pilares que entendemos fundamentales para combatir el Cibercrimen en nuestro país, es que, junto con el Área de Capacitación del Ministerio Público Fiscal y el Centro de Formación Judicial del Tribunal Superior de Justicia, la UFEDyCI organiza diferentes cursos de capacitación, no sólo en la Ciudad de Buenos Aires, sino en todo el país.

La idea es brindar a todos los operadores judiciales y abogados, conocimientos técnicos y jurídicos como así también compartir la experiencia adquirida en el marco de investigaciones de ciberdelitos.

Bajo este panorama, ya se encontraba organizado a través del Área de Capacitación del Ministerio Público Fiscal, un curso que comenzaría durante el mes de marzo de este año, en donde los integrantes de la UFEDyCI abordaríamos los diferentes ciberdelitos, legislación nacional e internacional en la materia, métodos de investigación y desafíos procesales actuales.

Decretada la cuarentena en toda la Argentina, y con la intención de continuar pese a ello con los objetivos trazados por la Unidad Fiscal, junto con el Área de Capacitación del MPF, la UFEDyCI adaptó el curso de capacitación para que sea realizado bajo la modalidad on line, para toda la Ciudad Autónoma de Buenos Aires y diferentes Provincias del país.

En el mismo, se abordaron en profundidad y a través de clases filmadas, cada una de las cuestiones de derecho penal de fondo, procesal, evidencia digital e investigación de delitos informáticos.

CAMPAÑAS DE CONCIENTIZACIÓN Y PREVENCIÓN

En este mismo sentido, desde la UFEDyCI entendimos que en este momento de confinamiento, todas estamos más conectados en la red, ya sea por estudio, trabajo u ocio; lo que da lugar a que haya más escenarios y más tiempo para el ciberacoso a niños/as, jóvenes y mujeres.

El confinamiento y la nueva mécanica interfamiliar debido al cierre de escuelas genera que los niños, niñas y adolescentes pasen más tiempo en casa frente a la pantalla. Si bien esto tiene beneficios, también trae ciertos riesgos: pueden ser víctimas del delito de grooming.

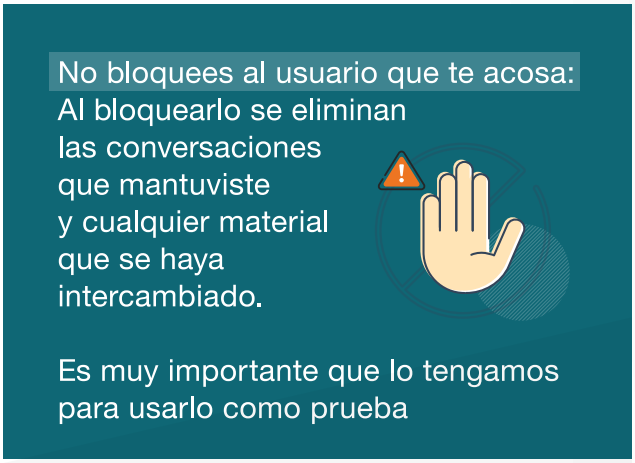
Las mujeres también pueden sufrir ciberacosos, tales como la difusión no consentida de imágenes íntimas a través de Internet, o el hostigamiento con el envío constante de mensajes intimidatorios a través de redes sociales o plataformas de mensajería instantánea. Esto puede suceder en virtud de que los celos traspasan el ámbito de confinamiento que se está viviendo, ya sea de una pareja actual o de ex parejas.

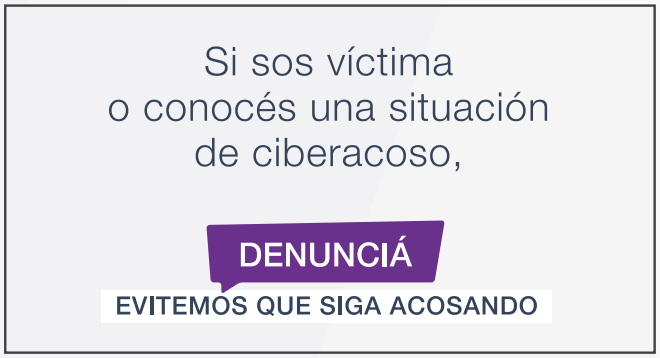
A su vez, la imposibilidad de contacto personal en el mundo físico, genera que las relaciones interpersonales pasen a un escenario virtual. Si bien esto es positivo ya la tecnología nos permite conectarnos con otros, cierto es también que estas nuevas modalidades de relacionarse, tanto en adolescentes como en adultos, generan riesgos y consecuencias no deseadas si no somos conscientes de los recaudos que debemos tener tomar.

Es por ello, que desde la UFEDyCI, junto al Área de Prensa y Comunicación MPF CABA, elaboraron campañas de prevención para enseñar a los ciudadanos cómo evitar ser víctimas de distintos tipos de ciberacosos y cómo actuar en caso de que esto pase.

Éstas campañas consistieron en videos animados y placas con información, las cuales fueron publicadas en redes sociales tales como Instagram y Twitter, como así también en la página del Ministerio Público Fiscal de la Ciudad que cuenta con una sección dedicada a los Delitos Informáticos.

En la primera de estas campañas de prevención, se brindó información acerca de en qué consiste el delito de Grooming, cómo pueden hacer los niños, niñas y adolescentes para evitar ser víctimas de este tipo de conductas y se elaboraron recomendaciones de cómo actuar en caso de que esto suceda. Los consejos estaban dirigidos tanto a los niños, niñas y adolescentes como así también hacia sus padres, ya que estos últimos, frente a este tipo de conductas, suelen tener el instinto de contactarse con el acosador, lo que nunca es recomendable en este tipo de casos, ya que puede frustrar la investigación penal.





La segunda campaña estuvo dirigida a las mujeres, haciendo hincapié en la existencia de figuras penales y contravencionales dentro del ámbito de la Ciudad de Buenos Aires que permiten sancionar conductas como el hostigamiento virtual y la difusión no consentida de sus imágenes íntimas, incentivándolas principalmente a denunciar estas conductas pese al estado de cuarentena.

La tercer campaña de prevención estuvo dirigida a concientizar a adolescentes y adultos acerca del intercambio de mensajes, fotos y videos eróticos y sexuales a través de medios electrónicos, el llamado sexting, informándolos acerca de los efectos nocivos de que sus videos o imágenes íntima estén en manos de todo el mundo. Se hizo hincapié en que, si bien esta práctica no está prohibida, sí lo está la difusión no consentida de estas imágenes, invitándolos a denunciar estos casos ante la UFEDyCI.

PALABRAS FINALES

De esta forma, la UFEDyCI ha logrado sortear muchos de los problemas que hoy en día trae aparejados la cuarentena que se encuentra atravesando la Argentina, permitiendo adoptar decisiones de calidad en la investigación de conductas cometidas en los entornos digitales, sin las dilaciones que ocasionan -a nivel mundial-, las medidas impuestas para evitar el contagio de COVID-19.

Los centros de denuncias en la web, telefónicos y por correo electrónico se encuentran abiertos para que la comunidad denuncie diferentes hechos delictivos cometidos a través de Internet.

Asimismo, con el apoyo del Fiscal General de la Ciudad Autónoma de Buenos Aires, se han arbitrado los medios necesarios para que los investigadores tengan acceso remoto al sistema de gestión de casos, facilitando su ingreso, evaluación e investigación a través de la disposición de medidas on-line y bajo modalidad "home-office", lo que permitirá identificar a los autores que se encuentran detrás de las maniobras delictivas.

Sin dudas, esta pandemia, más allá de traer aparejada una profunda crisis sanitaria, ha tenido como consecuencia el aumento de conductas ilícitas cometidas en el ciberespacio. Los factores son diversos: modalidad de trabajo remoto, bajas medidas de seguridad de los sistemas informáticos, mayor cantidad de tiempo en la web de niños, niñas y adolescentes, diferentes estrategias de los delincuentes en la utilización de la pandemia como pantalla para realizar maniobras de ataques informáticos, entre muchos otros.

Sin dudas esta pandemia ha marcado un antes y un después en las sociedades de todo el mundo, con impactos impensados a nivel social, sanitario y económico. Sin embargo, no debemos dejar que la crisis nos paralice, por eso continuamos enfrentando al Cibercrimen en tiempos de coronavirus.

UFEDyCI

UNIDAD FISCAL ESPECIALIZADA EN DELITOS
Y CONTRAVENCIONES INFORMÁTICAS

@ ufedyci@fiscalias.gob.ar

MPF | MINISTERIO PÚBLICO FISCAL
Ciudad Autónoma de Buenos Aires

@mpfcaba