BACSIRT
Vamos Buenos Aires | Centro de Ciberseguridad
LA AGENCIA DE SISTEMAS
www.ba-csirt.gob.ar
BOLETÍN N°26
FECHA DE PUBLICACIÓN
02 11 17

CIBERCRIMEN: QUÉ ES Y CÓMO PREVENIRSE

Es nuestra responsabilidad hacer que Internet sea un ámbito útil, seguro y confiable que favorezca la conexión, interacción e intercambio positivo entre las personas y no un espacio "anónimo" e "inteligible" aprovechado para delinquir y favorecer el avance de los aspectos más bajos de la humanidad.

Tal como lo conocemos hoy en día, Internet siempre se ha regido por los principios libertad, autorregulación y autogobierno. Justamente esas bases son las que hacen de la inmensa red de redes que constituye Internet, un espacio tan novedoso e interesante de explorar. Ahora bien, como toda nueva creación, además de aportar herramientas y recursos inéditos, trae consigo también nuevos desafíos y problemas a resolver. En ese plano se ubican **las cuestiones relacionadas a los conflictos y delitos que se desarrollan gracias y a través de medios digitales** los cuales, en su conjunto y llevados a la práctica, **conforman lo que se conoce como "la industria del cibercrimen"**.

A simple vista y sin entrar en demasiados detalles, podría parecer exagerado vincular las ideas de "actos ilícitos" o "delitos" y "mundo virtual". Ello se debe, muy probablemente, a que en general todo lo virtual se considera menos real que aquellos objetos físicos que podemos ver y tocar. No obstante, dicha ilusión o paradoja del pensamiento no es más que eso: otra idea, un prejuicio que es necesario desarticular y erradicar del imaginario colectivo.

Ahora bien, ¿por qué afirmamos esto con tanta seguridad?

Esta pregunta tiene múltiples respuestas o, mejor dicho, implica varios argumentos que apoyan dicha convicción. Y tales argumentos tienen, a su vez, casos concretos que los respaldan. A modo de ejemplo, podríamos recordar el caso de Antonella, la chica que a principios de este año fue víctima de ciberbulliyng y acoso a través de las redes y diferentes sitios de Internet como consecuencia de haber subido un video a Facebook Live. También podríamos tomar el caso de los mega-ataques que se dieron a

nivel mundial con los ransomware "WannaCry" y "Petya" los cuales ocasionaron daños millonarios, algunos de ellos irreversibles, para un millar de usuarios; tanto privados como públicos. Un tercer ejemplo lo constituye el caso de Micaela Ortega, la niña de 12 años que fue asesinada en Bahía Blanca luego de que el asesino la contactara a través de Facebook (delito que se conoce con el nombre de "grooming"). Y así podríamos continuar recolectando ejemplos a lo largo de cientos y cientos de páginas. Ejemplos que incluyen, desde casos similares a los expuestos hasta ciberterrorismo y ciberguerra. Esto se debe a de que, **a partir de la aparición de Internet, los principios de territorialidad y soberanía de las naciones, en términos individuales, se ven excedidos**. En el contexto interconectado en el que nos estamos manejando, nos vemos ante la imperiosa necesidad de repensar estos temas de forma global, apelando no sólo a los gobiernos estatales aislados sino, además, a los organizamos internacionales -privados y públicos- y a los sectores empresariales, académicos y de la sociedad civil en su conjunto.

Tengamos presente que el hecho de que lo que sucede en Internet parezca poco real debido a su inmaterialidad, tiene consecuencias muy concretas.

A pesar de que no lo parezca y que los ciberdelincuentes muchas veces usen medidas contraforenses para borrar evidencias, toda actividad digital deja huellas.

Como decíamos, los casos que acabamos de citar implican la ejecución de delitos los cuales, por desarrollarse a través de medios digitales, son llamados "delitos informáticos". Dicha figura legal, se incluye en la legislación argentina a partir del año 2008 en que es sancionada **la ley 26.388, conocida como "Ley de delitos informáticos"**, debido a que **incorpora nuevos delitos y, a su vez, adapta los existentes al entorno digital**. La incorporación de esta nueva norma constituye un importante avance en la lucha contra el cibercrimen; avance que es necesario continuar y profundizar dado que, como decíamos anteriormente, con la aparición de Internet no solo se han trasladado los delitos tradicionales al plano virtual, sino que, además, muchos de ellos se han incrementado y agravado: como sucede con los fraudes, la pedofilia y pornografía infantil, la trata de personas y el narcotráfico, entre otros.

En este sentido, es importante entender que en lo que respecta al funcionamiento de Internet y las reglas que lo gobiernan, todos podemos participar; y, de hecho, no solo podemos, sino que debemos hacerlo. Es preciso que cada uno de nosotros, como usuarios de la red y desde el lugar en el que nos encontramos, tomemos la responsabilidad y ejerzamos nuestro derecho de expresar nuestros puntos de vista y necesidades, plantear nuestros límites y no reproducir ni fomentar aquello que consideremos inapropiado o que no nos gustaría experimentar. De modo que Internet sea un ámbito útil, seguro y confiable que favorezca la conexión, interacción e intercambio positivo entre las personas y no un espacio "anónimo" e "inteligible" aprovechado para delinquir y favorecer el avance de los aspectos más bajos de la humanidad.

Más allá de los estereotipos y falsas creencias instaladas por la películas, los ciberdelincuentes están más cerca de lo que creemos y todos somos potenciales víctimas.

Tal como expresa Sebastián Stranieri, CEO de la empresa VU Security, "*en el último tiempo las amenazas han crecido exponencialmente debido a varios factores. Uno de ellos es la existencia de múltiples medios de comunicación digital y diferentes percepciones de la seguridad. Otro factor es la publicación de información relevante, personal y/o privada en las redes sociales que hace que para el atacante sea muy simple correlacionar datos y explotarlos para delinquir. A medida que la sociedad civil siga integrando herramientas digitales a sus negocios y sus vidas, seguirá creciendo el índice de ciberdelitos, por eso es importante trabajar en la prevención y contar con una política de respaldo de la información*". Y, a propósito de ello, nos sugiere los siguientes consejos a tener en cuenta para proteger nuestra información de delitos informáticos:

- Utilizar software original y mantenerlo actualizado con las últimas versiones suministradas por el fabricante.
- Comprar un antivirus confiable y actualizar las últimas versiones y parches de seguridad.
- Informarse a través de medios de comunicación, expertos en ciberseguridad y boletines oficiales.
- Mantener una conversación fluida con su familia y amigos y capacitar sobre qué contenido se abre y se comparte en Internet y las redes sociales.
- Evitar el uso de redes públicas para acceder a información privada.
- Realizar transacciones críticas desde una red certificada como segura.
- Descargar únicamente aplicaciones de tiendas oficiales como Google Play o Apple Store.

Por último, desde **BA-CSIRT**, queremos remarcar **la importancia de denunciar y no permanecer en silencio ante aquellos casos y situaciones que impliquen, en algún sentido, la concreción de un delito informático. Dado que, como ya hemos dicho, en caso de no hacerlo y a pesar de no tener esa intención, se estaría colaborando con el libre desarrollo de la ciberdelincuencia**, debido a que la falta de denuncias y material probatorio de casos reales hace que no se pueda tener un conocimiento completo del estado actual de la situación y, consecuentemente, tomar las acciones necesarias. ▪