Recomendaciones sobre la política

Fraude tecnológico y abuso en línea

La oportunidad

La computación en la nube está revolucionando cómo las personas trabajan, aprende, interactúan y juegan. La educación es sólo un ejemplo de cómo una nueva generación de servicios basados en la nube conecta a los estudiantes a todo un mundo de información y recursos, al tiempo que proporciona a los profesores nuevas formas de enseñar.

Las redes sociales son otro ejemplo, ya que la gente de todas las edades utilizan una amplia gama de servicios en línea para formar comunidades y conectarse con amigos y colegas. Además, los servicios en la nube se han convertido en importantes vehículos a través de los cuales las personas y los gobiernos progresan en los valores fundamentales, incluyendo la libertad de expresión, el compromiso civil, la privacidad y el acceso libre a la información.

El desafío

Al mismo tiempo, los servicios en línea han dado lugar a nuevos riesgos y un nuevo potencial de daños, especialmente para las poblaciones vulnerables, como los niños y los ancianos. Los depredadores utilizan los servicios basados en la nube para crear y distribuir imágenes de abuso sexual infantil y para solicitar menores de edad con fines de explotación sexual.

Los estafadores engañan a las personas haciéndoles creer que tienen malware o virus inexistentes en su ordenador, haciéndoles pagar por servicios de asistencia técnica innecesarios. Por desgracia, los métodos que implementan los delincuentes son cada vez más sofisticados y difíciles de detectar.

Recomendaciones sobre la política

Los desafíos únicos para proteger a los niños, los ancianos y a otros ciudadanos vulnerables requieren una respuesta coordinada

e integral. En muchos casos, las leyes existentes necesitan actualizarse para dar respuesta a las tecnologías y amenazas actuales, deben estar equilibradas contra la necesidad de proteger la libertad de expresión incluyendo la privacidad individual, y deben ser innovadoras. Estos marcos legales actualizados deben promover las mejores prácticas de la industria y el desarrollo de herramientas tecnológicas que los consumidores pueden utilizar para ayudar a protegerse. Algunas de estas áreas incluyen:

Fortalecer y hacer cumplir las leyes para impedir la creación de abuso y fraude en línea. Muchas leyes existentes que están destinadas a luchar contra el fraude y la explotación de menores no se redactaron para dar respuesta a los delitos en línea y, como resultado, no se aplican rotundamente. Según el Centro Internacional de Niños Desaparecidos y Explotados, 35 países aún no cuentan con una legislación que trate específicamente con las imágenes de abuso sexual infantil. De los 79 países que sí las tienen, 26 no se ocupan de los delitos informáticos de este tipo. Además, muchas de las leyes que penalizan la creación y distribución de imágenes de abuso sexual infantil no cubren el mundo en línea y están mal adaptadas a las nuevas tácticas de los depredadores de niños, conocedores de la tecnología. A medida que los gobiernos actualizan sus leyes para hacer frente a estas nuevas amenazas, deberían trabajar estrechamente con grupos de derechos, defensa y soporte a la infancia, además de con proveedores de tecnología, todos los cuales juegan un papel en la protección de los niños y las familias en la era digital.

Apoyar las asociaciones público-privadas. Las asociaciones públicas-privadas son esenciales para dar respuesta a la variedad, cada vez mayor, y la complejidad de las amenazas en línea. Los gobiernos, las empresas de tecnología y los proveedores de servicios en línea deberían trabajar juntos para desarrollar y compartir herramientas tecnológicas y experiencia, realizar campañas de concienciación y educar al público sobre los riesgos del ciberespacio. Para dar respuesta

a la protección infantil, los gobiernos deberían considerar asociarse con la Alianza Global para Erradicar el Abuso Sexual Infantil en Internet WePROTECT, una coalición que incluye a 70 países junto con empresas de tecnología y organizaciones civiles dedicada a erradicar la explotación y abuso sexual infantil en Internet.

Promover la cooperación internacional. Cada vez más, los delitos en línea implican a infractores en un país y a víctimas en otro, lo que puede dificultar un enjuiciamiento efectivo. Se necesitan nuevos acuerdos internacionales y de asistencia mutua legal modernizados para reforzar la cooperación entre fronteras, el intercambio de información y la aplicación de las leyes.

La promoción de la educación del consumidor. Muchos crímenes en línea pueden evitarse si las personas están mejor informadas acerca de cómo identificar las amenazas y protegerse a sí mismas. De acuerdo con una encuesta realizada por Microsoft, uno de cada cinco clientes ha sufrido una interacción fraudulenta en línea. Los "mileniales" son particularmente vulnerables a los correos electrónicos fraudulentos y a los anuncios emergentes intrusivos. Los gobiernos deberían centrarse en la educación de los consumidores sobre la seguridad en línea para ayudar a las personas a identificar las amenazas y protegerse a sí mismos, con un énfasis especial en las escuelas, para que los jóvenes aprendan a defenderse de los depredadores en línea y llegar a la edad adulta con fuertes hábitos de seguridad en línea. Los gobiernos también deberían considerar la posibilidad de unirse a, y promover, campañas de sensibilización como "STOP. THINK. CONNECT", una asociación global pública-privada que ofrece directrices básicas a los ciudadanos sobre los hábitos y prácticas seguros en Internet.

Dar soporte a la autorregulación del sector. A pesar de que los gobiernos trabajan para hacer frente a los riesgos asociados con los servicios en línea, pueden promover un entorno de innovación tecnológica y autorregulación del sector que proporciona la

flexibilidad necesaria para responder a la naturaleza cambiante de las amenazas en línea, que puede ser difícil de lograr únicamente a través de la legislación. Los gobiernos y la industria deben trabajar juntos para establecer los principios de seguridad y a los proveedores de servicios se les debe dar la oportunidad y la responsabilidad de determinar los medios de implementación.