Publicado en Madrid el 18/12/2020

Las 6 motivaciones de la ciberdelincuencia en los videojuegos online

Con la llegada de la Navidad, las vacaciones y los regalos, se aumenta considerablemente el tiempo en el que niños y adultos dedican a los videojuegos online. Por este motivo, desde S2 Grupo se ha destacado la importancia de acceder a ellos de forma cibersegura y minimizar al máximo la posibilidad de caer en las redes de los ciberdelincuentes

Para concienciar sobre la ciberseguridad en los videojuegos online, S2 Grupo ha elaborado un informe en el que su equipo de expertos ha destacado, por medio de un comunicado, las 6 principales motivaciones de los ciberdelincuentes en este ámbito:

Obtener dinero por vía directa .- Este sector genera mucho millones de euros porque muchos de los videojuegos se compran online y, además, los que son gratuitos requieren pagos para mejorar a los "personajes". Por tanto, el dinero está en todas las fases del videojuego y las tarjetas bancarias estarán en la red.

Obtener dinero por vía indirecta.- Los datos personales son en la actualidad un activo muy importante y su valor cada vez es mayor. Éstos son robados y vendidos por los ciberdelincuentes en la denominada "Dark Web" (web oscura), que conforma el gran conglomerado de páginas webs de Internet y que no son visibles para la mayoría de usuarios que usan buscadores como Google y que normalmente propician negocios ilegales como venta de armas, drogas, trata de personas, pederastia, etc. "Debemos ser conscientes de que si nuestros hijos utilizan videojuegos que tengan acceso a la cámara del móvil o usan alguna fotografía del jugador, el ciberdelincuente podría hackear el dispositivo y acceder a las fotografías, las cuales podrían acaban vendidas en una web de pederastia", ha explicado José Rosell, socio-director de S2 Grupo.

Acosar a un jugador.- Los videojuegos online, permiten conectividad con otros jugadores, se puede hablar en tiempo real con ellos mediante unos auriculares con micrófono a la vez que se juega, por lo que es un canal potencial para llevar a cabo amenazas, extorsión, chantajes, insultos o vejaciones. "En estos casos, suele pasar que cuando uno de los jugadores tiene un "mal perder", comienza el ciberacoso, llegando a robar algún tipo de información del contrincante, si tiene los conocimientos necesarios para ello", ha comentado Miguel A. Juan, socio-director de S2 Grupo.

Grooming.- Se trata de una práctica en la que un adulto, se hace pasar por un menor de edad (perfil falso), en cualquier medio online, para contactar con un niño o adolescente, intentar ganarse su confianza y acercarse a él para obtener información de su vida privada, pudiendo luego redirigir sus conversaciones en otras plataformas como redes sociales. Desde S2 Grupo, se recomienda a los padres que lleven un control moderado sobre la actividad de sus hijos en relación a los videojuegos online. "Más de uno hemos escuchado a nuestros hijos decir: "Espera que estoy jugando una partida online y ahora mismo no puedo parar" Pues en ese preciso momento, si nos acercamos, escucharemos tal vez a nuestros hijos hablando en directo posiblemente con un desconocido", asegura José Rosell.

Mejorar su perfil de jugador.- Otra de las motivaciones frecuentes de los ciberdelincuentes en torno a los videojuegos es mejorar su propia cuenta o perfil. En este caso, se está hablando de que son también jugadores pero en lugar de jugar con su perfil y/o personaje, roban una cuenta de otro jugador mucho más avanzado en el juego. Además, existen otras motivaciones para robar una cuenta como,

por ejemplo, que la cuenta de la víctima sea Premium o para vender dicha cuenta en webs como eBay. Obtener ventajas en el juego.- En este caso, el jugador utiliza sus conocimientos de hacker para modificar el juego y obtener beneficios sobre su cuenta y que le aventajen en el juego. “Esto era mucho más común en las consolas de sobremesa tradicionales y es algo más complejo de llevar a cabo en la actualidad, ya que las plataformas online de juegos permite denunciar estas cuentas y los usuarios son eliminados”, afirma Miguel A. Juan. Desde S2 Grupo se ha destacado que, hasta tal punto son comunes los hackeos en videojuegos y consolas basadas en la motivación del dinero, que muchos ciberdelincuentes se atreven a publicar en webs como “Mil anuncios”, sus servicios para hackear videojuegos y dispositivos.

“Conocer los riesgos y las motivaciones que impulsan a actuar a los ciberdelincuentes es fundamental para que los niños y adolescentes, que son más vulnerables, tomen conciencia de que éste es un tema muy serio y necesitan protegerse igual que lo hacen en la vida off-line. Si tienen claro que no se irían con un desconocido y los peligros que correrían en caso de hacerlo, lo mismo debe suceder con el paralelismo e la vida conectada a la red”, ha afirmado José Rosell, socio-director de S2 Grupo.

“En cuanto los jóvenes conocen las motivaciones de los ciberdelincuentes, conectan directamente con la necesidad de ciberprotección. Esto es clave para que puedan disfrutar de los videojuegos online y de los eSports sin riesgos. Ellos saben que si dejan la puerta de casa abierta, pueden entrar a robar. Pues tienen que saber también, que si no tienen una contraseña segura, por ejemplo, les pueden robar de la misma forma”, ha apostillado Miguel A. Juan.

Datos de contacto:
Luis Núñez
667574131

Nota de prensa publicada en: Madrid

Categorías: Nacional Juegos Entretenimiento E-Commerce Ciberseguridad Ocio para niños Gaming

NotasdePrensa
https://www.notasdeprensa.es