Publicado en Madrid el 29/06/2020

15 consejos en eSports para evitar ser víctima de los ciberdelincuentes

La compañía de ciberseguridad S2 Grupo asegura que el incremento del volumen de negocio de los videojuegos online y los eSports ha incrementado los ciberataques en este sector. Por ello su equipo de expertos ha elaborado un listado de recomendaciones para jugar de forma segura, entre los que se incluyen la importancia de crear un correo electrónico exclusivo para esto, no enlazar tarjetas bancarias ni manipular las consolas, entre otras

Según los expertos de S2 Grupo es fundamental que los jugadores, adultos o jóvenes, conozcan las claves para disfrutar con ellos sin correr riesgos de seguridad que puedan poner en peligro la cuenta bancaria o la intimidad de las familias, entre otros aspectos.

"Los videojuegos ya no atienden a cuestiones de edad, son millones los jugadores, mucho el dinero que se genera diariamente, muchos los ciberdelincuentes, variados los ciberataques y también las consecuencias. Ahora existen estrellas de los eSports y sus campeonatos son televisados. Y esto hemos visto cómo todavía ha crecido más durante la crisis del Covid-19 y la cuarentena", ha afirmado José Rosell, socio-director de S2 Grupo.

"Los entornos de juego online han cambiado, su impacto económico también y, por tanto, hay que conocer las nuevas reglas del sector para evitar riesgos innecesarios. En S2 Grupo hemos realizado un informe de la situación del sector para detectar las vulnerabilidades más frecuentes que acometemos en relación al juego online y así establecer un decálogo con claves para su uso ciberserguro", ha declarado Miguel A. Juan.

Consejos de ciberseguridad de S2 Grupo en videojuegos online y eSports

Tras el estudio del estado de la ciberseguridad del sector, los expertos de la compañía han dtallado estas 15 recomendaciones:

1.- Crear un correo electrónico exclusivo para los videojuegos online.- Es importante tener una cuenta de correo para cada ecosistema de juego (Sony, Nintendo, etc.) y no vincular el acceso a los juegos a través de redes sociales porque tendrán disponible mucha información personal. En estos emails nuevos no debe darse ningún dato privado.

2.- Utilizar contraseñas nuevas y robustas.- Ésta debe tener al menos 12 caracteres que incluya mayúsculas y minúsculas así como caracteres especiales como el "%" y un mix entre números y letras.

3.- No enlazar tarjetas de crédito o débito a los videojuegos online.- Se aconseja no asociar ninguna tarjeta bancaria, sino usar un monedero virtual. Lo ideal para las compras en los videojuegos online, es

crear una cuenta de PayPal exclusiva para esto

4.- No manipular las consolas.- Al manipular, alterar o se pierde por un lado la garantía del dispositivo y, por otro lado, la seguridad aplicada desde el diseño.

5.- Descargar los videojuegos de tiendas oficiales.- Descargar los videojuegos de páginas webs desconocidas, puede llevar a infectar los dispositivos y comprometer la información privada.

6.- Conectarse a redes conocidas y fiables .- Cuando se juega a los videojuegos online sobre todo en dispositivos móviles, se suele tender a conectarse a redes públicas como la de un restaurante o un aeropuerto. Éstas son redes abiertas, vulnerables y poco fiables. Se aconseja usar los datos móviles, preferiblemente.

7.- Cerrar siempre la sesión de la cuenta.- Si se juega en dispositivos de terceros o ajenos o en una lan-party, no se debe olvidar cerrar la sesión de la cuenta así como eliminar archivos temporales, historial de navegación o cookies.

8.- Mantener los dispositivos siempre actualizados.

9.- Instalar un antivirus.- En todos los dispositivos es básico tener un antivirus de confianza (preferiblemente de pago) instalado que añada una capa de seguridad extra a los dispositivos a través de los cuales se juega online.

10. Limitar el uso de chats y participación en comunidades online.- Muchas veces pueden provocar casos de grooming, cyberbullyng o ciberacoso.

11.- No acceder a enlaces o extensiones desconocidas.- En muchos foros, comunidades de videojuegos o chats con jugadores desconocidos, es frecuente que se publiquen o se envíen diferentes enlaces o extensiones. Cuando se tenga la más mínima duda de su origen o fiabilidad, no se debe de acceder ya que puede llevar a infectar el dispositivo de juego.

12.- Usar app de control parental.- Es necesario el uso de una app de control parental que permita llevar un control sobre la forma de jugar de los hijos. También hay que tener en cuenta que algunos videojuegos traen por defecto su propio control parental.

13.- Fomentar proactivamente el uso de videojuegos adaptados a cada edad.

14.- Desactivar el GPS y usar cubre cámaras.- Otro riesgo importante de los videojuegos online es el ciberespionaje. El acceso a la ubicación en tiempo real y activación del GPS o a la cámara del

dispositivo puede suponer información muy valiosa para los ciberdelincuentes. Es por ello que se aconseja usar un cubre cámaras para móvil y desactivar el GPS cuando no haya que tenerlo necesariamente activado para el juego online.

15. Crear una atmósfera de confianza y concienciar.- Hay que advertir a los más jóvenes de los diferentes riesgos a los que están expuestos así como sus consecuencias.

Datos de contacto:
Luis Núñez
667574131

Nota de prensa publicada en: Madrid

Categorías: Juegos Entretenimiento Ciberseguridad Ocio para niños Gaming