Publicado en Madrid el 26/09/2022

S2 Grupo advierte de posibles ciberataques en los eSports

El auge de los eSports y los videojuegos online pone de manifiesto que las familias deben ciberproteger al máximo la actividad para evitar caer en las redes de la ciberdelincuencia. Algunos de los ciberdelitos más comunes en estos entornos son el robo de nombres y direcciones, de tarjetas de crédito, de dinero, ciberacoso, cyberbullying, grooming o envío de malware, entre otros muchos

Por este motivo, el equipo de expertos de S2 Grupo ha elaborado un decálogo para participar en forma cibersegura en los eSports.

Crear correos exclusivamente para los videojuegos online: para jugar online hay que crearse una cuenta. Algunos videojuegos permiten acceder en base a un registro previo en redes sociales. S2 Grupo desaconseja esta práctica porque "las aplicaciones o juegos podrán acceder a mucha información personal". La compañía recomienda crear un email nuevo, exclusivamente para el registro en los videojuegos online y no incluir ningún dato personal como nombre, apellido, fecha de nacimiento, sexo o ciudad.

Crear una contraseña nueva y segura para este email y para los videojuegos online, totalmente diferente a cualquier otra que se use en otros entornos.

No enlazar tarjetas de crédito o débito a los juegos online. Ya sea para pagos frecuentes, como en una suscripción, como recurrentes a la hora del momento del pago de un determinado videojuego o de una serie de ítems durante las partidas, los videojuegos online generan una gran cantidad de dinero. Desde S2 Grupo se aconseja "no asociar ninguna tarjeta bancaria sino usar un monedero virtual como el de PayPal, con una cuenta exclusiva para esto en la que tampoco se almacenará dinero. Otra opción segura y fácil es comprar tarjetas con dinero para gastar en ecosistemas concretos de videojuegos (se pueden encontrar en supermercados). Son tarjetas con un dinero limitado y bastará solo con introducir el código para poder comprar".

No manipular las consolas. Al hacerlo, se pierde la garantía del dispositivo y la seguridad aplicada desde el diseño.

Conectarse sólo a redes conocidas y fiables. Cuando se juega desde el móvil hay una tendencia a conectarse a wifis públicas cuando es posible, como en restaurantes o aeropuertos, y esto pone en riesgo la privacidad del usuario.

Cerrar siempre la sesión: Si se juega en dispositivos ajenos o en una lan-party, debe recordarse cerrar la sesión de la cuenta desde la que se ha entrado y eliminar archivos temporales, historial de navegación o cookies.

Descargar los videojuegos de tiendas oficiales. "Cuando algo es gratis, el producto somos nosotros. Descargar los videojuegos de webs desconocidas puede acarrear infectarnos con malware y poner en riesgo nuestra información privada", afirma S2 Grupo en un comunicado.

Limitar el uso de chats y participación en comunidades online. En los juegos online se puede estar en contacto con el resto de jugadores mediante chats, audio, vídeo, perteneciendo a comunidades de juegos específicos, etc. Esto puede provocar casos de grooming, cyberbullyng o ciberacoso. Hay que concienciar a los jóvenes sobre la importancia de que no se extralimiten en las conversaciones con desconocidos a través de los videojuegos online y sus riesgos.

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 haya la más mínima duda de su origen o fiabilidad, no se debe acceder a éstos porque pueden infectar el dispositivo.

Usar app de control parental. En el caso de los niños, "es necesario el uso de una app de control parental para conocer la forma de jugar de nuestros hijos", aseguran desde S2 Grupo. Algunos videojuegos ya lo incorporan por defecto.

Desactivar el GPS y utilizar cubre cámaras.- Otro riesgo importante de los videojuegos online es el ciberespionaje. Muchos requieren el acceso a la ubicación en tiempo real y activación del GPS al igual que a la cámara del dispositivo. Esto puede suponer información muy valiosa para el ciberdelincuente. Por esto, debe usarse un cubre cámaras para el móvil así como desactivar el GPS cuando no necesite estar activado para el juego online.

Junto a estas recomendaciones, desde S2 Grupo se ha incidido en que para reforzar la seguridad a la hora de participar en videojuegos online o eSports es necesario mantener los dispositivos actualizados y tener instalados en ellos un antivirus. Además, en el caso de los niños, se aconseja a los padres que tomen las riendas sobre este asunto concienciándoles sobre los riesgos en estos entornos, teniendo confianza para que les comenten cualquier anomalía que detecten y fomentando el uso de videojuegos adaptados a sus edades.

"Los videojuegos online y los eSports ya no atienden a cuestiones de edad. Son millones los jugadores que participan en ellos, la cantidad de dinero que mueven en todo el mundo es cada vez mayor y eso ha hecho que haya un aumento de la ciberdelincuencia en ellos y que los ciberataques a través de esta vía sean cada vez más sofisticados", ha explicado José Rosell, socio-director de S2 Grupo.

"Hoy en día, cada vez son mayores los potenciales ciberriesgos que existen para los jugadores online. Muchos de ellos se deben directamente a la alta conectividad que ofrecen los videojuegos entre los propios jugadores. Esto no supone dejar de aprovechar las ventajas que confiere, simplemente es señal de la importancia de conocer los riesgos, ponerles nombre y saber cómo usarlos sin ponernos en peligro", ha comentado Miguel A. Juan, socio-director de S2 Grupo.

Datos de contacto:
Luis Núñez
667574131

Nota de prensa publicada en: Madrid

Categorías: Juegos E-Commerce Ciberseguridad Gaming