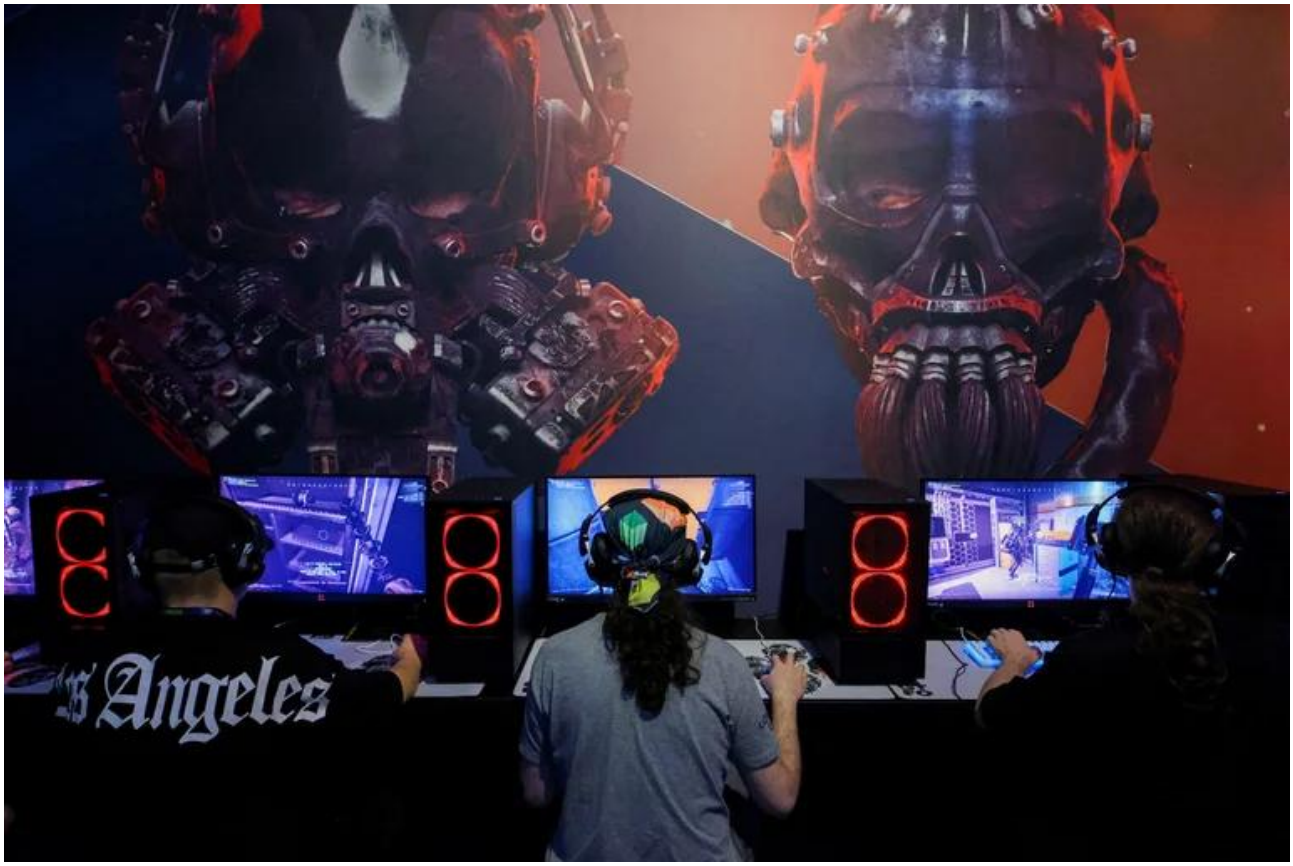
Tres cosas que no debe hacer un gamer para evitar ser víctima de ataques cibernéticos



Con el crecimiento de la industria de los **videojuegos**, las comunidades de jugadores que giran alrededor de títulos como FIFA, Call of Duty o Fortnite, aumentan constantemente para convertirse en un ecosistema que, pese a centrarse en la diversión y el ocio, también puede ser la ventana para que **cibercriminales** actúen.

La empresa de ciberseguridad Check Point Software, advierte que incluso los videojuegos pueden ser objetivos de ciberdelincuentes debido a la **información sensible** que tienen sobre los jugadores, como datos de cuentas bancarias y transacciones, incluso sus bienes virtuales.

Los ciberdelincuentes vulneran las **cuentas de los jugadores** para robar sus bienes virtuales y venderlos por dinero real a otros usuarios interesados en adquirirlos. El robo de los **inventarios** de los jugadores no lo único que buscan, sino que también es posible que la cuenta vulnerada sea vendida en su totalidad a otras personas.

Mientras más datos se hayan acumulado en la cuenta y los bienes sean exclusivos o raros, más dinero puede obtener el criminal.

El robo de los inventarios de los jugadores no lo único que buscan, sino que también es posible que la cuenta vulnerada sea vendida en su totalidad a otras personas. (Photo by Sean Gallup/Getty Images)

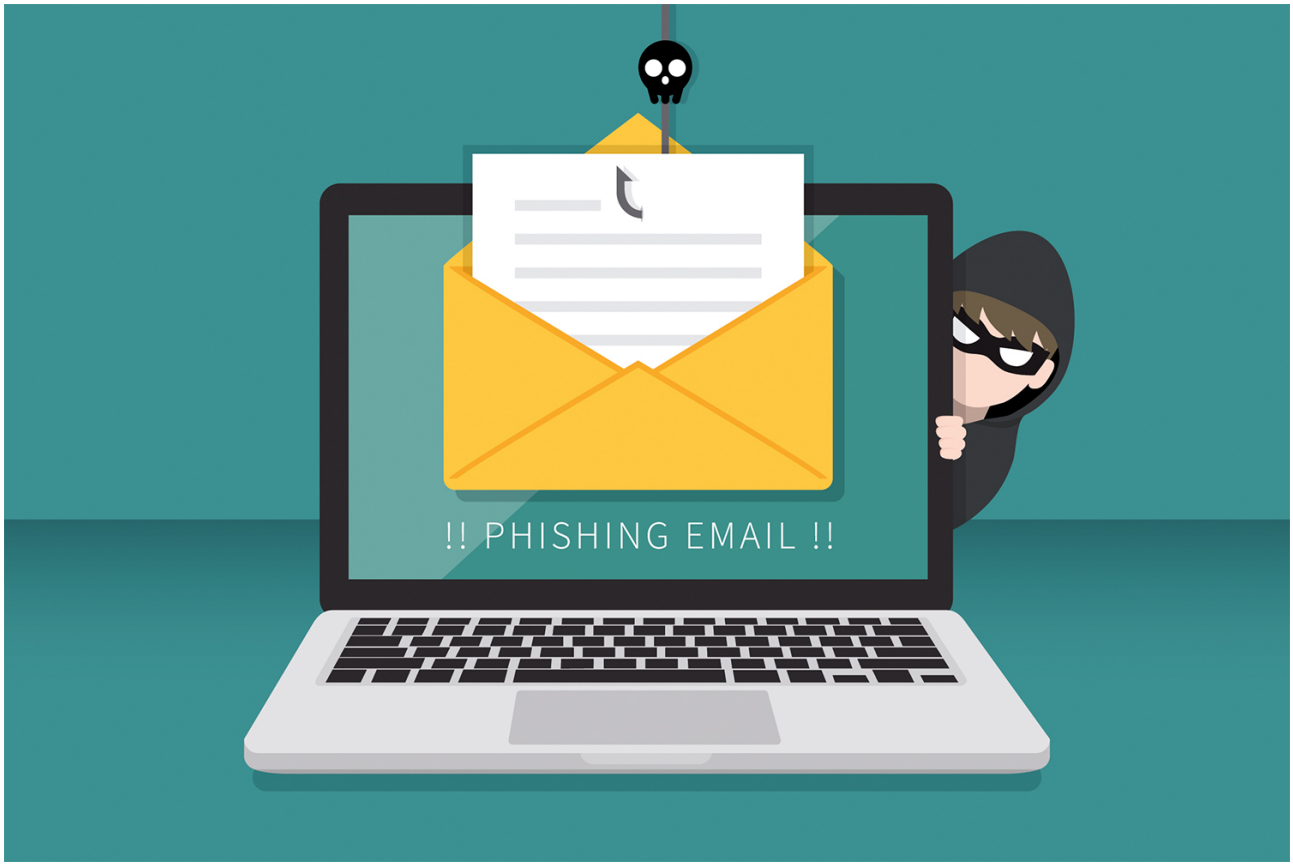
Estos casos de vulneración de la **seguridad** de los usuarios no solo se producen en juegos de consola, sino también con dispositivos móviles como tablets o **smartphones**. Los cibercriminales pueden incluso rastrear información tan íntima como la ubicación o incluso escuchar las llamadas telefónicas.

Qué no hacer para evitar ser una víctima

La posibilidad de sufrir un **ataque cibernético** que vulnere las cuentas de los usuarios en videojuegos siempre está presente, por lo que depende de cada persona tomar medidas preventivas y actitudes vigilantes antes cualquier eventualidad.

En primer lugar, **no se debe crear usuarios con contraseñas débiles o reutilizadas.** Este es un problema común pues una nueva cuenta implica la gestión de una nueva contraseña y, en caso de que ya se tengan múltiples plataformas de acceso a videojuegos, recordar esa información es cada vez más complicado.

Optar por la misma contraseña, aunque sea segura, también representa un **riesgo de seguridad** pues, una vez que sea vulnerada para un perfil, todos los que tengan la misma clave de acceso caerán. Contar con un **gestor de contraseñas** puede ayudar a solucionar ese inconveniente. Aumentará la seguridad de las distintas cuentas y disminuirá notablemente el riesgo de sufrir un ciberataque.



Las campañas de phishing no solo se pueden difundir por medio de correos electrónicos, sino también por páginas de inicio fraudulentas diseñadas para que los usuarios entreguen sus contraseñas de forma voluntaria. (Segurilatam)

Atención a posibles casos de **phishing** que son dirigidos a los usuarios de videojuegos populares. Las campañas de estafas con esta modalidad no solo se pueden difundir por medio de correos electrónicos, pues otra forma usada por los ciberdelincuentes es la

creación de páginas de inicio fraudulentas para que los usuarios entreguen sus contraseñas de forma voluntaria.

En otros casos, por más que un ataque de phishing no tenga acceso por completo a la cuenta de sus víctimas, sí es posible que extraiga parte de un inventario o bienes virtuales del jugador.

Finalmente, los jugadores deben evitar cualquier **propagación de malware** que pueda afectar alguno de sus dispositivos o consolas. Usualmente estos casos se presentan junto con las estafas de **phishing** por medio de **aplicaciones** o códigos que prometen hacks o formas de sacar ventaja dentro del juego para poder avanzar más rápido.

Cualquier descarga desde sitios no seguros puede ser una puerta abierta para distintos tipos de virus que incluso pueden difundirse por medio de **mensajes de spam** a otros jugadores, por lo que hay que prestar atención a las aplicaciones o ventanas de chat abiertas.

Fuente: Infobae