ADOBE STOCK

Que el videojuego de tu hijo no te robe la cartera

Captan a los críos con **ofertas falsas de monedas virtuales** para vaciarte la cuenta corriente... sin que te des cuenta

JOSÉ CARLOS CASTILLO

Del mismo modo que los pescadores acuden al lago o río con más peces, los ciberdelincuentes encuentran su particular filón en aquellas aplicaciones y plataformas digitales con mayor número de usuarios. Una de ellas son los videojuegos por internet, que en los últimos años se han convertido en el anzuelo perfecto para dejarnos sin blanca. Los expertos en ciberseguridad ponen el foco en los menores, más propensos a caer en la trampa. No solo pasan una gran cantidad de horas frente al móvil o el ordenador, sino que están habituados a interactuar con desconocidos en el marco de las partidas, sin desconfiar de sus intenciones.

El 'modus operandi' está muy claro. «Los malhechores digitales abordan a niños y adolescentes previo seguimiento de sus perfiles en redes sociales o herramientas como Discord, donde acostumbran a compartir imágenes y hacer comentarios», explica Joan Arnedo, investigador y experto en ciberseguridad por la Universitat Oberta de Catalunya (UOC). Les envían mensajes de carácter emocional y, sobre todo, por los apartados de chat de sus videojuegos favoritos, a los que suelen contestar rápido. En ellos, los estafadores se hacen pasar por usuarios de su misma edad (utilizando un vocabulario similar) y les hacen ofertas. «La mayoría se basan en presentar, a través de webs externas al juego, supuestos mecanismos para obtener monedas virtuales gratuitas o más baratas que usar en el juego. Para ello se envían mensajes como 'introduce tus datos aquí para conseguir...', 'instálate esto en el ordenador para conseguir...', 'pincha en este enlace...'», desgrana Arnedo.

Y los críos pican: compran esas supuestas monedas con dinero real, utilizando las tarjetas bancarias de sus padres o los métodos de pago previamente habilitados en sus teléfonos móviles, para conseguir contenido extra en sus juegos. Lo habitual en estos casos es que el ciberdelincuente se embolse una importante suma sin que el menor reciba lo prometido. Aunque el último disgusto se lo llevan los padres, que ven cómo la cuenta bancaria termina en números rojos.

Ojo con las tiendas virtuales

Aunque el experto de la UOC alude a Fortnite o Roblox como los juegos más peligrosos en cuanto a estafas –registran millones de transacciones diarias en torno a sus respectivas monedas virtuales, PaVos y Robux–, también pide atender a las grandes tiendas digitales de videojuegos. «El nivel de fraude es estratosférico en torno a plataformas como Steam, ya que los usuarios pueden comprar créditos o ciertos tipos de bienes digitales en el mercado gris». Por no hablar del robo de perfiles a través de correos electrónicos fraudulentos, lo que permite a terceros acceder a los datos de pago guardados en dichas tiendas.

Como queda patente, los peligros no dependen tanto de los videojuegos en sí como de las vías de comunicación que propician. Unos riesgos a los que también se exponen los adultos y que en muchos casos obedecen a descuidos (o desconocimiento) en materia de ciberseguridad. «Por ejemplo, usar en un videojuego la misma contraseña que empleamos en el resto de servicios (como el correo electrónico) empeora la situación en caso de que caigamos en la trampa. Algunos niños ni siquiera son conscientes de que han sido estafados y, viendo que no han obtenido la recompensa prometida, vuelven a pinchar en el enlace de marras presos de la frustración», prosigue Arnedo.

El papel de los padres

En lo que a los padres respecta, el experto recomienda activar las opciones de control parental y autenticación en dos pasos siempre que estén disponibles; además de supervisar las partidas para detectar cualquier mensaje extraño. «Si es demasiado bueno para ser cierto, es que hay truco. También hay que estar alerta frente a aquellos jugadores que insistan en entablar conversación fuera de la plataforma oficial del juego».

Si, pese a todo, el menor fuese víctima de estafa, el primer paso por parte de los adultos será cambiar la contraseña de la cuenta de juego afectada y notificar la situación a la plataforma correspondiente: «En aquellos juegos donde tengan 'amigos', vale la pena hacer una criba y mantener únicamente a los conocidos en persona. Igualmente, anularemos la tarjeta de crédito asociada y los procesos automáticos de pago e introducción de datos personales».

En último término, el docente de la UOC apuesta por una educación digital básica para todo crío que juegue habitualmente por internet. «Deben entender que nada es gratis en la red y que las monedas virtuales tienen un valor real que pagan los padres. También que los datos personales son sagrados y que siempre podrán contarnos cualquier error que hayan cometido sin miedo a ser castigados. Ellos son las víctimas, no los culpables, como quiere hacerles creer el estafador», concluye.

Descargas desde foros... mejor no

La empresa de ciberseguridad Kaspersky alertó hace unos meses sobre los más de 19 millones de intentos de ciberataque camuflados –solo durante el último año– en videojuegos de éxito como 'GTA', 'Minecraft' o 'Call of Duty'. Concretamente, con la difusión de supuestos archivos de instalación que contienen programas maliciosos, capaces de tomar el control de ordenadores y 'smartphones' sin que el menor sea consciente. Ante esta amenaza, la mejor medida preventiva es descargar dichos títulos únicamente a través de sitios oficiales, desconfiando de aquellos archivos «provenientes de foros, redes sociales o enlaces desconocidos».