

# ¿Cómo hacerte millonario con el “Hacking de sombrero blanco”?



*Bug Bounter: la nueva “profesión” consistente en descubrir vulnerabilidades en Apps y websites de importantes compañías multinacionales*

Roy Castillo, Santiago López, Bitquark, Emily Stark, o el sorprendente caso de Grant Thompson, de tan sólo 14 años de edad. Son algunos de los nombres de las personas que, desde hace años, trabajan a tiempo parcial encontrando errores en la seguridad informática de famosas empresas como Nintendo, Google, WhatsApp, Microsoft, Twitter, entre otras.

El caso quizá más sorprendente es el de Grant Thompson, un adolescente de 14 años de edad que en enero de 2019 descubrió una vulnerabilidad en la aplicación de videollamadas de Apple, Facetime, que permitía espiar a los miembros de una llamada grupal en dicha aplicación.

Curiosamente, Grant encontró la falla mientras usaba Facetime para hablar con sus colegas sobre estrategias para el famoso juego Fortnite. Si bien Apple no ha revelado la cuantía de la recompensa a Grant, actualmente la política de Apple es entregar recompensas de hasta US\$200.000 por las fallas más graves.

Otro caso reciente es el de Santiago López. Este argentino de 19 años de edad, ha logrado US\$1,000,000 descubriendo fallos en ciberseguridad. Aproximadamente, trabajando 20 horas a la semana, gana US\$100.000 anuales. Afirma sentirse bien sabiendo que está mejorando Internet. “Con cada bug, haces Internet más segura. Es impresionante”.

Santiago ha encontrado más de 1.600 vulnerabilidades informáticas y ha alcanzado semejante cifra de ingresos gracias a la mayor plataforma de hacking ético del mundo: HackerOne. Los “bug bounters” (cazarrecompensas de Internet) suelen recibir entre US\$50 y US\$500.000 por unas horas de su tiempo.

En definitiva, surgen diversas incógnitas en relación a esta novedosa ocupación. ¿Es una “profesión” ética? ¿Es necesaria? ¿Es un nuevo nicho de mercado para empresas dedicadas a la ciberseguridad, como Dolbuck?

¿Hasta qué punto se necesitan programas de recompensas para hackers, si hay empresas dedicadas a las auditorías y al Hacking Ético? No hay agujero a salvo de los piratas informáticos. Se hace necesaria mayor inversión en formación relacionada a ciberseguridad y peritaje informático.

***Artículo realizado por la empresa experta en seguridad Dolbuck S.L.***