Game Over: Poor Password Protection Leaves Online Gamers Exposed to Hack Attacks

Online gaming has quickly become a hugely lucrative industry, with more people than ever owning gaming accounts. According to research from Kaspersky Lab, over half (53%) of people regularly game online, a figure which rises to 64% for 25-34 year olds and 67% for those aged 16-24. It's also potentially lucrative for cybercriminals, as hacked gaming accounts can be sold on the black market. Despite the threats, gamers are frequently leaving their online accounts vulnerable to hacking attempts, putting their valuable progress, personal data – and potentially their income – at risk.

The global games audience – led by online platforms such as Steam, PlayStation Network and Xbox Live – is now estimated to be between 2.2 billion and 2.6 billion and is still continuing to grow. This makes the industry a clear target for cybercriminals who are looking to disrupt online operations and gain access to data such as passwords and bank card information, clearly shown by recent attacks on both the Xbox and PlayStation platforms.

With more than half of people now regularly gaming online, cybercriminals have an enormous pool of potential targets to choose from. Furthermore, gaming has become a major part of many people's lives, with users turning to games when they're bored or lonely and to socialise with friends. Successful attacks can therefore be hugely upsetting for those affected. As well as having their data stolen, victims who have their gaming account broken into can also be emotionally affected, losing access to their favourite games (either temporarily or permanently), the many hours they may have spent building up their profile and any money they might have put into it.
Of those people who have experienced a successful or attempted attack on one of their online accounts, 16% identified their gaming accounts as being a target, a figure which rises to 21% for men. And, as 55% of people can't quickly restore their gaming account details if lost, the distress that accompanies such attacks is significantly amplified.

And these accounts are clearly extremely important to their owners. Rather than being an activity reserved for the home, gaming has become entwined into many people's everyday lives, as illustrated by the fact that almost one-in-three (27%) people regularly use either a smartphone for online gaming. Although devices aren't inherently secure, nearly a quarter (23%) of people use public Wi-Fi to log into gaming accounts and 56% say they don't take any additional security precautions when using public networks, which presents obvious security risks. This danger is further enhanced by the fact that just 5% of people selected their gaming account as being one of three that require the strongest passwords.

Furthermore, as many online profiles today are connected, victims can easily end up losing access to several accounts – such as email and social media accounts – that are important to them in many different ways. While this can be emotionally damaging for leisurely users, professional gamers can be even more seriously impacted, potentially losing out on valuable income.
"With a treasure trove of personal information now available online, cybercriminals have more opportunities than ever to get their hands on user's private data, which they can then sell on the digital black market," commented Andrei Mochola, Head of Consumer Business at Kaspersky Lab. "Online gamers – both amateur and professional – are understandably concerned about having their accounts hacked, or being locked out of their accounts by forgetting their passwords. This is a

dilemma that users face every day, with many choosing the less secure option of using either the same password for all their accounts, or simple passwords that are easy for hackers to guess. However, only by taking appropriate precautions and using strong, unique passwords will users be confident that their valuable accounts are protected and that all their efforts have not gone to waste."

To help protect gamers' online accounts, several of Kaspersky Lab's products include a password manager to help users keep their details safe, such as the Kaspersky Password Manager in Kaspersky Total Security. This feature stores all user passwords in a secure digital vault and provides easy access from PCs, Macs and smartphones. An automatic password generator does the hard work for users by creating strong and resilient passwords, while users only have to remember one master password to access all of their online accounts which is much easier to remember then several.

For further information on the biggest cyber threats facing consumers, read the full report 'Consumer Security Risks Survey 2017: Not logging on, but living on' here.