Tips to help online gamers fight off unwanted villains/cyber crooks

Gamers are used to dodging terrifying villains or having to overcome challenging obstacles of some sort in order to make it to the next level. These days, however, gamers are getting more than they are bargaining for as they are increasingly being targeted by malicious villains. These scoundrels are imposters who don't form any part of the game's plot. They are cyber criminals acting with the intent to cause real harm to the players.

© ra2 studio - Fotolia.com

Online gaming is not just fun and games anymore. Worldwide, it has exploded into a seriously lucrative industry, with billions of dollars at stake. In its latest global games investment review, Digi-Capital - the investment bank for games, apps, digital media/services and tech/telecoms across America, Europe and in some Asian countries - states that online and mobile gaming could have a revenue share of USD48 billion by 2016. A different report, compiled and released by Transparency Market Research and called Gaming Market - Global Industry Analysis - Size, Growth, Share and Forecast 2011 - 2015, places the estimate much higher even sooner, forecasting that the global gaming market will reach USD117.9 billion by 2015.

Fake offers for rare pieces of equipment

"Cyber criminals tend to follow the money makers, so it isn't surprising that they are now honing in on the online gaming industry," said Lutz Blaeser, MD of Intact Security, South African distributor of various IT security software solutions, including G Data. "These perpetrators are using sophisticated methods to lure unwitting gamers into traps with fake offers for rare pieces of equipment and virtual money for digital game characters."

Ralf Benzmüller, head of G Data's Security Labs, says they also resort to more traditional means. "Stealing and trading in user accounts for online games is a very lucrative business for cyber criminals. To do this, the perpetrators develop special computer malware that targets the user accounts of online gamers, or they employ tried and tested phishing methods," he said.

Research reveals that gamers were being targeted by cyber criminals with an attempted 7000 attacks recorded daily last year, with an average of 10 emails containing malicious links and attachments reportedly being sent to gamers' inboxes daily and approximately 5000 new malware programs specifically designed to target online games said to be appearing daily.

G Data has recently highlighted the three most common ways in which online gamers are being targeted. "Apart from the fake offers I've already mentioned, in which the scammers place ads offering rare equipment, virtual currency or high-level game characters on online vending platforms and then steal the buyer's money without ever delivering the goods, there are two other common methods as well," Blaeser said.

The notorious Trojan Horse

"Some malware programs that are used to attack gamers are so-called key-loggers, which are used to spy on keyboard input like user names and passwords. Then there is also the notorious Trojan Horse Trojan.PWS.OnLineGames.NVI, which steals data from the installed browser and can, therefore, steal data from your gaming account too, whatever information is happened to be stored there. Data theft via phishing, which is the second method of attack favoured by hackers, mostly takes place via emails in which the fraudsters pretend that there is some problem with the gamer's user account and then prompts the recipient to enter his user details on a fake website, where it is then stolen."

There are ways in which gamers can protect themselves. "Gamers should use a powerful security solution that remains active during gaming, install all available software updates and only trust official game patches from the manufacturer," advised Benzmüller.

Blaeser offers up additional tips from G Data's guidelines. "You must secure all your accounts with different, strong passwords. To ensure that they are as difficult as possible to crack, each should ideally consist of a random sequence of numbers, special characters and upper and lower case characters. Never have your passwords 'remembered' in the browser. And, lastly, don't reveal too much about yourself online. Rather choose a nickname to use for your gaming accounts and avatars. And make sure your online purchase gaming accessories, virtual cash and other gaming paraphernalia from official online gaming markets, and use a credit card for the payment process as it is more secure," he concluded.