Mobile App Games Like Pokémon Go Present Potential Physical And Cyber Security Threats

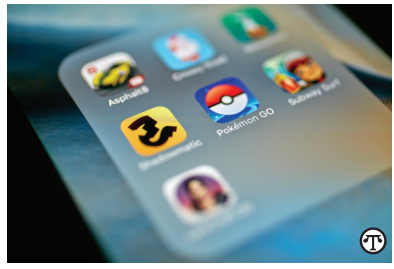
(NAPSA)—Software developer Niantic's new mobile app Pokémon GO has made history as the most played mobile game in the United States to date, according to TechCrunch. SurveyMonkey found that the app boasts more than 21 million actively daily users, who log nearly 35 minutes a day catching augmented reality monsters by visiting real-world location. Nearly all users want to become Pokémon masters, often overlooking the dangers of "catching 'em all" during the process.

With the game's popularity, similar games are expected to be developed in the future. Unfortunately it isn't all fun and games, as there are potential dangers of engaging with others online through these types of games and applications. From muggings to cyberhacking, this augmented reality game poses real-life threats.

As the game loads, players see a warning screen from Niantic, advising them to be aware of their surroundings. Reports of players walking into objects or even traffic have flooded news stations across the country, like Newsweek and Fox, since the launch of the game. There have also been reports of more serious crimes, like muggings and armed robbery. Many of these threats can be avoided by playing with a friend, not venturing out after dark or sticking to familiar places. Most important, players should remain aware of their surroundings while playing.

The potentially most dangerous, and seemingly unknown threat to players may be in the cyber realm, warns Dan Konzen of University of Phoenix. Most players log into the game through Google accounts instead of creating new accounts. This may be more convenient, but can increase the risk for cyberhacks on personal information. With the success of Pokémon GO, similar games are sure to follow. Being aware of physical and cyber threats to personal information will reduce these risks.

Konzen, Phoenix campus college chair, routinely performs live hacks of colleagues' social media accounts to demonstrate how easy it is for hackers to access personal information like locations visited or photos that are blocked by security settings. Hackers often use this info to send phishing emails or hack bank accounts. The same hacking principles apply to Pokémon GO.



Geocaching games can be fun but players need to be careful of their online security.

By signing up through one's Google account, Konzen says players are giving Niantic access to modify emails, calendar or Google Docs, and opening doors for hackers to access other accounts.

"People who are determined to play Pokémon GO and any similar future games should be cautious of using passwords they use for emails or social media sites when signing in," Konzen said. "If hackers are able to learn and access one site from a password, they can access multiple sites if the same password is used."

Additionally, players should be aware that anything posted online can be accessed by hackers, even if protected by security settings. If you plan to risk cyber breaches by playing online games, be aware that information can be accessed. This applies to Pokémon GO or any other mobile games.

"Players should recognize the potential physical and cyber dangers associated with geocaching games," he said. "Be conscientious of your surrounds. If an area or the people around you do not seem safe, don't continue."

University of Phoenix College of Information Systems & Technology prepares cyber professionals to combat increasing cybercrimes. The University offers associates, bachelors and master's degrees that teach the risk management and information assurance skills vital to an organization's success. For more information about each of these programs, including on-time completion rates, the median debt incurred by students who completed the program and other important information, please visit www.phoenix.edu/programs/gainful-employment.