It's All Fun And Games Until Someone Loses A Credit Card: Safety In Online Games

Before the cellphone era, gaming was a pretty secure business. You went to the store, bought a disk, a cartridge or deck of cards, and played it many times over until you grew bored of it. On the surface, today's gaming seems like an improvement. The majority of gaming apps are free and they're always available to play regardless of time and place. This convenience, though, does come with costs.

Obviously, the news surrounding the robbery of "Pokemon Go" players in O'Fallon, Missouri is one type of threat that mobile apps can pose. Be aware of apps that others can use to predict your location, and always keep an eye on your surroundings. That will keep you safe from the most obvious threats, but not from all of them.

It is incredibly convenient to have all your games on a single device you can keep in your pocket and have with you at all times. The downside is that everything else – your phone number, your email address, even your financial information – may all be on that device, too. With everything on one device, it's become easier for online scammers to take what they want. Fortunately, there are some steps you can take to protect yourself. Be on the lookout for these three ways mobile games take your money, and know what you can do about them.

1.) In-app purchases

In-app purchases are deceptively simple. You "buy" a free game in the app store, thinking you got a bargain. You play the game for a few minutes, enjoying yourself as you assemble an army or destroy your friends at trivia or pop some bubbles. After a little while, though, you hit a snag – you've maxed out the number of games you can play in one day, and you'll have to wait 24 hours to play again. You're frustrated and upset. You're willing to do anything you can to keep playing. And, lo and behold, the game offers you a solution. You can pay a small fee of $0.99 to continue playing – and paying.

Unfortunately, there's no simple solution to this one: Either you cough up the $0.99 or you don't. In cases like this, sometimes the best move is just not to play that game. The golden rule of the internet works here, too: If you're not paying for something, you're not the customer. You're the product. Don't support business models that work on addiction and deception. Find a different game. Sometimes it's even better to find a game you have to buy once to feel a little more secure in knowing you won't have to keep buying up to keep playing.

2.) Phishing scams

This scam, too, starts with the purchase of an innocent-looking app. In order to use it, the app claims, you need to set up an account with the app manufacturer's website. Citing security reasons, it says the account will ensure mysterious strangers cannot come in and mess up your process playing tic-tac-toe and hangman. All it needs is your email account, and then for you to create a username and password. You input your email account, you come up with a username, and then you use the password that you use for everything. Just like that, you've given a company you know nothing about access to all the details of your online life. Any other system you use that password for can now be compromised.

Another version of the scam is the fake game login screen. An email looking like it's from the game company will soon arrive. It will tell you to login through a link in the email to receive a fabulous in-game prize. Of course, there is no prize, and the email was a tool for scammers to collect your login information.

The best way to prevent this is through research. A quick search for the app you're considering and the word safe is all you need. Look at the top three results. You can then make the smart decision about whether or not to give that app your email address.

3.) "Bonus credit"

This one begins in the same way an in-app purchases scam does. You buy the app, you play the app for a while, and it suddenly says you can't play anymore today. In this case, though, it's not that you've run out of time, it's that you've run out of credits, coins, or some other form of in-app currency that lets you play the game. Once you've paid all your coins for the day, there's nothing for you to do but wait. All you have to do to get more is watch an advertisement or take an IQ quiz. The advertisements are, surprisingly, almost always legit, but the "IQ quiz" will include an agreement to pay $10 a month on a phone bill!

This scam is especially sneaky because crooks don't need access to a credit card number or a login. All that's necessary is for one user on a family plan, even a child, to click through a service agreement without reading it carefully. Then, the whole family's on the hook. If you don't go through your bill carefully every month, these charges can add up, and fast.

For this one, awareness and common sense are the keys. Once you know that the quiz is a scam, simply avoid taking the quiz – at least the quiz that asks for your phone number. Avoid apps that ask you for purchases to play the game. Research apps before you give them any personal information.

The gaming industry has long passed the simplicity of Pong and Pac-Man, but as long as you keep your personal security your number one priority, they can still be just as fun.