online gaming

Let’s talk about online gaming for a while

Online gaming activities are something that is commonplace. Majority of us are addicted to games that we throw security to the wind. In this particular article, I want to tell us what we should know about online gaming activities. You will also understand some of the threat that is related to this activity.

Like I said earlier. online games have become more popular, Most of the time we see users scattered across the globe collaborating together in order to achieve a particular goal. With high-speed internet gaining ground,this trend is now becoming more attractive to new users. Another trend when it comes to an online gaming is Massive Multiplayer Online Role-Playing Game (MMORPG) while is a type of computer role-playing game where a large number of players interact with one another in a virtual playing world.

You should also note that Massive Multiplayer Online Role-Playing Game (MMORPG) is very popular all over the world. It was also discovered that the revenue generated by owners is well over a billion dollar annually.

Large traffics is common with online gaming…

Because of a large amount of traffic involved in online gaming, Massive Multiplayer Online Role Playing Game (MMORPG) has become the primary target of hackers who see it as an opportunity to launch an attack at any given time. They also know that most online gamers always throw caution to the wind.

It has also been discovered that in the world of online games, it is very possible for players to meet and become friends. Some of them also go to the extent of sharing cheats with one another.

I remember those time that I was addicted to Grand Theft Auto!

Online gaming risks

Like I said in my previous article, I have talked about some of the reasons why online games were so popular. It is because people want to enjoy themselves. The negative side of it, however, is that most people are always carried away by online games. This allows their devices to be infiltrated by hackers. In this article, I want to show us some of the online game risks that online game lovers can be exposed to. Follow me as we look at this together in this article.

Let’s talk about online game risks…

Here are the online game risks…

Interaction with fraudsters as part of online game risks

One of the online game’s risks that are very common when you are playing online games is that you might be interacting with fraudsters unknowingly. This can open you to attacks as they have the tendency of stealing your information or tricking you without you knowing.

Interconnectedness as part of online game risks

When you are playing online games, you are also connected to the server where the game is located. This can open up your device to attacks. The other games who have criminal tendencies can use this medium to inflict attacks on your devices. You can also avoid this type of online game risks by installing anti-virus on your device.

Malware transfer as part of online game risks

Another implication of addiction to an online game is malware transfer. When you are connected to online game servers and you have the bad guys or infected systems around, your device can be infected. That is why you should not play online games without a strong and reliable anti-virus.

Online games in Admin mode

Before I start talking about admin modes and the reasons why you should adopt it when playing online games, I want to talk about guest accounts.

First and foremost, in one of my articles, I have talked about some of the reasons why you should never create a guest account. It will really open you up to attacks. The reason being that all guest accounts are not passworded. That makes it easy for hackers to explore this mode to attack your device.

From my previous article, I have focused attention on some of the risks associated with online games but I never discussed playing online games in admin mode. You really have to be very careful when you are playing online games. I will advise that you should never play online games in admin mode. It is very dangerous. It is very essential that you take note of all these warnings if you do not want to infect your devices with malware.

ultima: WE LOVE MAPLESTORY
Sonata: WE LOVE MAPLESTORY
FiAnLaU: WE HATE MAPLESTORY!!

Online games require admin mode…

You need to note that some online games require that they are played in admin mode. That means you will not be granted access if you log in through a user account.

You should be careful when playing games in Admin mode…

You need to be very careful when you are playing such games. If you are forced to play from the administrator mode, make sure you have downloaded the game from the manufacturer server.

You should know that free downloaded games might contain malicious software. This can be hidden in the plugin that is used to run that particular game.

Playing online games in admin mode…

I will say that, instead of playing the game using your admin mode, you should rather play the game directly from their website. You can also play the game using a user account that is not the admin. This will deny attacker accessto your administrator rights. If you have any other idea feel free to use the comment box.

ActiveX risks and online gaming

Understanding ActiveX risks

I have already talked about ActiveX and its usage in my previous articles. I will not do that again in this article. You can click on the link to that article in order to have more understanding of what it is.

My focus for this article is to talk about some of the reasons ActiveX risks should be avoided when you want to play online games. Let's look at the practical steps of avoiding that in this article.

When you are playing this online, some of these games will require the use of ActiveX or Javascript before they can play on your device.

Why you need to take precautions when you are facing ActiveX risks…

When you enable this feature just because you want to play games, it will open up your device to attacks.

Also, I am not saying enable these feature is bad, you can do anything to avoid ActiveX risks but you should be careful that you online enable it for games that you downloaded directly from the Gamers server. The reason being that some of these might have been cooked up by hackers. They might have inserted codes that can do damage to your device.

One of the ways of preventing ActiveX risks is to have some control measures in place. You have to be sure that whatever you are downloading into your system is from a trusted source. You should not believe that everything you got from Google Search Result Pagecan be trusted. It is also very paramount that you have an antivirusthat you actually paid for. That is when you can rest assured that you are safe.

How malicious Malicious game users make their money

Let's talk about how malicious game users make their money

In the recent time, I have discussed some of the ways that you need to prevent yourself from **other game users.**These game users are capable of inflicting your device because you are all connected to the same network. Their focus is to take advantage of your ignorance about security to make money.

That is why you have to be very careful. I also said it in my previous that if you had cause to play or download games, you have to make sure you are downloading from the main game website. I believe anyone that has a website will always want to protect their integrity. I will not want to spread the news that my game site is not secured. I will not want to inflict the system on my audience. That is why I will always work on the health of my game server.

Most of the time, stolen passwordsand another virtual that are stolen from online game users are sold on e-commerce websites such as e-bay or online game forums. These are always sold for real or virtual money on such sites. The malicious game users are making money out of your ignorance. They believe that you did not know anything about security. You felt that you did not have anything that is important to them. The earlier you change that thinking, the better.

Action Point

You need to confirm your subscription by clicking on the link sent to you. You can check the spam folder for it. Add us to your mailing list to receive directly from us.

PS: Click on the link below to sign up for my Online E-Course CRM Training. Make sure you confirm your subscription by clicking on the link sent to you. Thanks

Share on:

WhatsApp

Share on FacebookShare on TwitterShare on LinkedinShare on PinterestShare on Reddit

Sharing is caring.