CareerSource SOUTH FLORIDA

Monthly Security Tips Newsletter

AUGUST 2017

Gaming Online Safely & Securely

VOLUME 1, ISSUE 8

Online gaming is a great way to have fun; however, it comes with its own set of unique risks. In this newsletter, we cover what you and your family can do to protect yourselves when gaming online.

Securing Yourself

What makes online gaming so fun is that you can play and communicate with people from anywhere in the world. Quite often, you may not even know the other players. While the vast majority of online gamers have good intentions, some users want to cause harm. Here are some steps you should take to stay secure:

- Be cautious of any messages that ask you to take an action, such as clicking on a link or downloading a file. Just like email phishing attacks, criminals in online games will attempt to fool you into taking actions that can infect your computer or steal your identity. If a message seems odd, urgent or too good to be true, be suspicious that it may be an attack.
- Many online games have their own financial markets where you can trade, barter or buy virtual goods Just like in the real word, there are fraudsters on these systems who will attempt to trick you and steal your money or any virtual currency you have accumulated. Deal only with trusted people who have established reputations.
- Use a strong passphrase for any gaming accounts. This way, attackers cannot simply guess your passwords and take over your accounts. If your game offers two-step verification, use it. In addition, create different passwords for all of your online accounts. This ensures that your other accounts are safe even if one game becomes compromised. Are you worried you won't be able to remember all your passwords? Consider using a password manager.

Securing Your System

Bad guys may attempt to hack into or take over your gaming computer. Take the following steps to protect it:

- Secure your computer by always running the latest version of the operating system and gaming software Old and outdated software has known vulnerabilities that attackers can exploit to hack into your computer. Keeping your computer and gaming applications updated is essential to eliminating most of those known vulnerabilities.
- Use updated anti-virus software that checks any files you run in real time.
- Only download gaming software from trusted websites. Quite often, cyber attackers will create a fake, infected version of a game and distribute it from their own server.

Gaming Online Safely & Securely

VOLUME 1, ISSUE 8

Securing Your System (continued)

- Gaming add-on packs add new features to games and are often developed by the gaming communities' users. It is important to download the add-ons from trusted locations because attackers can infect these gaming packs with malware. If an add-on requires you to disable your anti-virus software or make changes to your security settings, do not use it.
- Never install or access any type of cheating software or website. Besides being unethical, many cheating programs are actually malware that will infect your computer.
- Check the website of whatever online gaming software you are using. Many gaming sites include a section on how to secure your system.
- Finally, be just as careful playing games on your mobile devices as you would be on your computer. Cyber attackers are beginning to target mobile devices.

For Parents or Guardians

Children require extra protection when gaming online. Having an open dialogue and educating your kids are two of the most effective steps you can take to protect them. One of our favorite tricks to get kids talking is to ask them how their games work; have them walk you through their online world and show you a typical game. Perhaps you can even play the game with them. Additionally, have them describe the different people they meet online. By talking to them, you can spot a problem and protect them far more effectively than any technology could. Some additional steps include:

- Know what games your children are playing and make sure you feel the games are age-appropriate.
- Limit the amount of information your kids share online. For example, they should never share their password, age, phone number or home address.
- Consider having their gaming computer in an open area where you can keep an eye on them. Younger children should not game in their rooms or late at night.
- Bullying, foul language or other antisocial behaviors can be a problem. Keep an eye on your kids. If they seem upset after playing a game, they could have been bullied online. If this is the case, have them stop playing the game and play in more kid-friendly environments, or have them play online games only with trusted friends.
- Learn if your children's games support in-app purchases and if the games offer any parental overrides.

Information provided by:

DEO Florida Department of Economic Opportunity

SANS Securing The Human

MS-ISAC Multi-State Information Sharing & Analysis Center

STOP | THINK | CONNECT

Center for Internet Security

KnowBe4 Human error. Conquered.