OUCH! June 2022

The Monthly Security Awareness Newsletter for You

Securely Gaming Online

What makes online gaming so fun is that you can play and interact with others from anywhere in the world, often you don't even know the people you are playing with. While the vast majority of people online are out to have fun just like you, there are those who want to cause harm.

Securing Yourself

The greatest risk to online gaming is not the technology itself but the interactions you have with strangers.

- Be cautious of any messages that ask you to take an action, such as clicking on a link or downloading a file. Attackers will use in-game messaging or phishing emails in an attempt to fool you into taking actions that can infect your computer, steal your identity, or your gaming accounts. 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 world, there are fraudsters who will attempt to trick you and steal your money or any virtual currency you have. Deal only with people that have established, trusted reputations.
- Use a strong, unique passphrase for any gaming accounts. This way attackers cannot simply guess your passwords and take over your accounts. If your game/platform offers two-step verification, use it. Can't remember all your passwords? Use a password manager.

Securing Your System

Attackers may attempt to hack into or take over the computer or device you are gaming on, you need to take steps to protect it.

- Secure your devices by always running the latest version of the operating system and the gaming software or mobile app. Outdated software has known vulnerabilities that attackers can exploit and use to hack into your device. Enable automatic updating when possible. By keeping your devices and gaming applications updated, you eliminate most of those known vulnerabilities.
- Download gaming software and game add-on packs from trusted websites only. Attackers will often create fake or infected versions, then distribute it from their own server. In addition, if any game or add-on requires you to disable any security tools or settings, do not use it.
- Underground markets have sprung up to support cheating activity. Besides being unethical, many cheating programs are themselves malware that will infect your device. Never install or use any type of cheating software or websites.

- Check the website of whatever online gaming software you are using. Many gaming sites have a section on how to secure yourself and your system.

For Parents or Guardians

Education and an open dialogue with your kids is the most effective step you can take to protect children. One approach is to ask them to show you how their games work, have them show you what a typical game looks like. Perhaps even play the game with them. In addition, have them describe the different people they meet online. Quite often online gaming can be a big part of your child's social life. By talking to them (and them talking to you) you can spot a problem and protect them far more effectively than any technology. Some additional steps include:

- Know what games they are playing and make sure you feel the games are age appropriate for your child.
- 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 device in an open area where you can keep an eye on them. In addition, 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 they are bullied online, report it to the game site and have them play online games with trusted friends only.
- Learn if your child's games support in-app purchases and what sorts of parental overrides they provide.

Guest Editor

Charlie Goldner is the founder of CyberNV and a SANS instructor. He is active on LinkedIn and works supporting government agencies. He has spent many hours gaming on PC and consoles over the years.

Resources

Social Engineering: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Multi-factor Authentication: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/
Password Managers: https://www.sans.org/newsletters/ouch/password-managers/
Online Security for Kids: https://www.sans.org/newsletters/ouch/online-security-kids/