OUCH! | July, 2017

The Monthly Security Awareness Newsletter for Everyone

OUCH!

IN THIS ISSUE...

- Securing Yourself
- Securing Your System
- For Parents or Guardians

Gaming Online Safely & Securely

Overview

Online gaming is a great way to have fun; however, it also 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.

Guest Editor

Steve Armstrong is the founder of Logically Secure, a certified SANS instructor, and the architect of CyberCPR, an Incident Management Platform. He is active on Twitter as **@Nebulator** and works with many big gaming companies around the world, fulfilling his childhood and professional dreams.

Securing Yourself

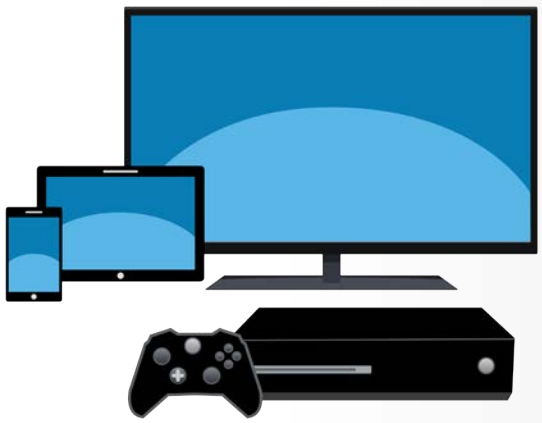
What makes online gaming so fun is that you can play and communicate with others from anywhere in the world. Quite often, you may not even know the people you are playing with. While the vast majority of people online are out to have fun just like you, there are those who want to cause harm. Here are 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, bad guys will attempt to fool or trick you in online games 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 even 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 people that have established, trusted 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, make all of your online accounts have a different password. That way, if one game is compromised, your other accounts are safe. Can't remember all your passwords? Consider a password manager.

Securing Your System

Bad guys may attempt to hack into or take over the computer you are gaming on. You need to take steps to protect it:

Gaming Online Safely & Securely



The key to securely gaming online is to use strong passwords, secure your computer, and use common sense when you receive odd messages or requests.

- Secure your computer by always running the latest version of the operating system and the gaming software. Old and outdated software has known vulnerabilities that attackers can exploit and use to hack into your computer. By keeping your computer and gaming applications updated, you eliminate most of those known vulnerabilities.
- Use anti-virus software. Ensure that it is updated and checking any files you run in real time.
- Download gaming software from only trusted websites. Quite often, cyber attackers will create a fake or infected version of a game, then distribute it from their own server.
- Gaming add-on packs, often developed by the community, are frequently used to add new features. Attackers sometimes infect these gaming packs with malware. Just like when you download games, make sure you download the add-ons from trusted locations. In addition, if any add-on requires you to disable your anti-virus or make changes to your security 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 computer. 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.
- Finally, always be just as careful playing games on your mobile devices as you would your computer. Cyber attackers are beginning to target mobile devices.

For Parents or Guardians

Children require extra protection and education when gaming online. Education and an open dialogue with 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 to show you how their games work; have them walk you through their online world and show you what a typical game looks like. Perhaps you can 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

Gaming Online Safely & Securely

having 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 computer 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, have them stop playing the game and play in more kid-friendly environments, or have them play online games with only trusted friends.
- Learn if your child's games support in-app purchases and what sorts of parental overrides they provide.

2017 Security Awareness Report

It's here! Get your copy of the 2017 SANS Security Awareness report, *It's Time to Communicate*. It's jam-packed with data on security awareness, giving you tips and tricks to keep you safe. Download your free copy: https://securingthehuman.sans.org/resources/security-awareness-report-2017.

Resources

Securing Your Home Network:	https://securingthehuman.sans.org/ouch/2016#february2016
Social Engineering:	https://securingthehuman.sans.org/ouch/2017#january2017
Passphrases:	https://securingthehuman.sans.org/ouch/2017#april2017
Password Manager:	https://securingthehuman.sans.org/ouch/2015#october2015
Two-step Verification:	https://securingthehuman.sans.org/ouch/2015#september2015

License