OUCH! | March, 2015

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- Securing Yourself
- Securing Your System/Accounts
- For Parents

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 can do to protect yourself and your family when gaming online.

Guest Editor

Jake Williams is the founder and principal consultant at Rendition Infosec, a certified SANS instructor and co-author of several SANS courses. He is active on Twitter as **@MalwareJake** and blogs regularly at **malwarejake.blogspot.com**.

Securing Yourself

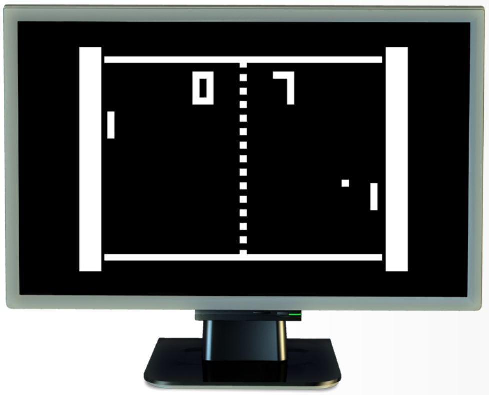
What makes online gaming so engaging is that you can play and communicate with others from anywhere in the world. Quite often, you may not even know the people you are playing with. While the vast majority of people online are out to have fun just like you, there are those who want to cause harm. Here are some things you should do 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 phishing attacks, bad guys will attempt to fool or trick you into taking actions that will infect your computer. 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 out of your money or attempt to steal it outright.
- Be careful performing transactions where real money is used to purchase in-game goods and vice versa. Only perform these actions in marketplaces with a known good reputation.
- Limit the amount of information you or your children share online. Never share detailed personal information, such as your password or home address.
- Many websites, such as online banking, use security questions to help confirm your identity. Attackers have been known to obtain the answers to these security questions by befriending victims in online games. Remember that you are under no obligation to answer questions people ask you when gaming.

Gaming Online Safely & Securely

Securing Your System/Accounts

The next step is to secure the computer you are using. Bad guys will attempt to take over your computer or your gaming accounts. You need to protect them:



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

- Use strong passwords for your computer and 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 sure each of your gaming accounts has a different password. That way, if one game is compromised, your other accounts are safe.
- Secure your computer by always running the latest version of the operating system and the gaming software. Just like your operating system and web browsers, old and outdated gaming software often 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.
- Run anti-virus; ensure that it is updated and checking any files you run in real time.
- Download gaming software from only trusted websites. If you are installing software to play a game, make sure you download it from the vendor's website or some other well-known, trusted location. Quite often, cyber attackers will create a fake or infected version of a game, then distribute it from their own server. If you install one of these, bad guys will have complete control of your computer.
- Gaming add-on packs, often developed by the community, are frequently used to add new features. Attackers sometimes infect these gaming packs with malware that can be very difficult for anti-virus to detect. Just like when you download games, make sure you only 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 firewall, do not use it.
- Underground markets have sprung up to support cheating activity. Besides being unethical, many cheating programs are themselves rootkits, which are arguably the most dangerous type of malware. Never install or use any type of cheating software.

- 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; be sure to follow any advice they have.
- 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

If you are a parent, be sure your kids follow the steps outlined above. (For younger children, you may have to perform these steps for them.) In addition, communicate with your children about the risks. Education and an open dialogue with your kids are some 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 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 having them talking to you), you can spot a problem and protect them far more effectively than any technology.

Video of the Month

Be sure to check out our free resources including the Video of the Month. This month we're covering The Payment Card Industry Data Security Standard (PCI DSS). You can always view the latest video at http://www.securingthehuman.org/info/174967.

Resources

Social Engineering:	http://www.securingthehuman.org/ouch/2014#november2014
Phishing Attacks:	http://www.securingthehuman.org/ouch/2013#february2013
Passwords:	http://www.securingthehuman.org/ouch/2013#may2013
What is Anti-Virus?:	http://www.securingthehuman.org/ouch/2014#december2014
Stay Safe Online:	http://www.staysafeonline.org/stay-safe-online/for-parents/gaming-tips

License

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus