THE NATION'S NEWSPAPER

Special Reprint Edition

USA TODAY

A GANNETT COMPANY

As seen in USA TODAY Money

April 27, 2011

PlayStation hackers may have gotten personal info

Intruders may have had access to credit card data

By Mike Snider
USA TODAY

Hackers who broke into Sony's PlayStation Network online service might have stolen members' credit card information, Sony said Tuesday.

The intrusion, which happened between April 17 and 19, has resulted in a week-long system outage that could last as long as another week. As many as 75 million users globally use the network to play online games together and download movies, TV episodes and game demos.

Sony says it will send an e-mail to all account holders advising those who gave their credit card information to either PSN or Sony's new Qriocity music system that hackers may have gotten their credit card number and expiration date but not the card's security code. "While there is no evidence at this time that credit card data was taken, we cannot rule out the possibility," Patrick Seybold, senior director of corporate communications and social media, said in a statement on Sony's official PlayStation blog.

"An unauthorized person" did get users' personal information including birth date and e-mail addresses, he said. In the wake of the security breach, PSN members should be alert for e-mail, telephone and postal mail scams that ask for personal or sensitive information, Seybold said.

Users should change the passwords on other services and accounts that might use the same user name or password as their PSN account. "We encourage you to remain vigilant, to review your account statements and to monitor your credit reports," he said.

Consumers should heed Sony's advice, says Tim Rohrbaugh, vice president of information security for Intersections, an ID theft protection and risk management firm in Chantilly, Va. "On something like a PlayStation or (Internet-connected) TV, you can't use the same password that you use on your bank account or the accounts where a lot of damage can happen," he says.

Some users criticized Sony on social networks and forums for not coming forward with information about the breach sooner. But Rohrbaugh applauded Sony for a quick response. "The average amount of time it takes for a company to find an unauthorized access is six months-plus," he says.

The Sony breach and another earlier this month at Epsilon, which provides e-mail marketing for 2,500 companies, is "a wake-up call" to pay attention to what is going on with your data, he says.

The outage comes at a bad time for Sony. Hot titles such as Valve Software's Portal 2, Warner Bros. brawler Mortal Kombat and PlayStation 3 exclusive Socom 4 all hit stores last week.

PlayStation hackers may have gotten personal info

Objectives

- ► Read the article "PlayStation hackers may have gotten personal info"
- ► Discuss the differences between the real world and the online world
- ► Define "disinhibition"
- ► With three peers, create an online code of conduct

Time Requirement

55 minutes

Materials

You will need:

- A copy of the article "PlayStation hackers may have gotten personal info"
- A writing utensil
- A copy of the Online Code of Conduct activity

Read and Respond

As a class, read the article and answer the following discussion questions.

1. How could hackers get personal information when people were only playing PlayStation?
2. Why should you use a different password for your online game, social network and email accounts than you do for an online bank account?
3. What other security risks, besides hacking, are there when you have an online presence?
4. What safeguards should you put in place when you are online?
5. List all the ways/devices you use to connect to the Internet.

Code of Conduct

Companies, like Sony, have an obligation to protect your personal data, but you are just as responsible for protecting your privacy. Because the information on the web can stay there in perpetuity, it's a wise idea to think before you send or post. Get in a group with three other students. Use the following discussion questions to generate ideas for what you think should be included in your own personal online code of conduct.

1. How is the online world different from the real world? List at least four ways.
2. Are there guidelines, like The Golden Rule (treat others as you want to be treated), that you try to abide by in the real world? List them.
3. Do those guidelines tend to shift when you're in the online world? If so, how? And why?
4. What do you think "disinhibition" might mean? Can you give a specific example you have seen of someone exhibiting disinhibition online?
5. Considering the list you created in question 5 above, are there Internet-ready devices that you are more security-conscious about? Less conscious about? Why the difference?
6. Have any of your accounts ever gotten hacked? How do you think the "unauthorized person" got your password? What did you do to fix the security breach?

With the answers to these questions in mind, create a list of guidelines that you would be willing to follow that help keep you, your data, your property and your community safe online. You can find a sample one here: http://bit.ly/safeteens11. Use the outline on the following page to direct your thoughts. You do not have to use every number in each section.

PlayStation hackers may have gotten personal info

Online Code of Conduct

I hereby pledge to do my best to adhere to the following for the safety and well-being of myself, those I come in contact with, and my online community.

Physical Safety	1. 2. 3. 4.
Psychological Safety	1. 2. 3. 4.
Reputational and Legal Safety	1. 2. 3. 4.
Identity, Property and Community Safety	1. 2. 3. 4.

PlayStation hackers may have gotten personal info

Apply

After you've completed your code of conduct, share one guideline from each of the four sections with your classmates. Then, as a class, discuss:

1. How does the fact that you created these guidelines increase or decrease your willingness to follow them?
2. How can following these guidelines help protect you and your data from hackers?
3. What other situations do you think may be minimized by following these guide lines?
4. Was there an area you think should be covered by the code of conduct that was not? If so, what was it?