



NCCIC ADVISORY

National Cybersecurity & Communications Integration Center

28 APRIL 2011 – 1600 – SONY PLAYSTATION NETWORK COMPROMISE

EXECUTIVE SUMMARY

On Tuesday 19 April, Sony learned its PlayStation Network and Qriocity Networks had been compromised by unidentified actors. Sony closed down the two networks on 21 April and publicly announced the compromise the following day. On April 26, the company disclosed that personal information had been stolen. The information included names and addresses of users, their birth dates, e-mail addresses and possibly other information including credit card numbers.

SPECIFICS

On Tuesday 19 April, Sony learned its PlayStation Network and Qriocity networks had been compromised by unidentified actors. Sony took its first public step by closing down the two networks on 21 April and announced it as an external compromise the following day. On 22 April, Sony released the following statement, "An external intrusion on our system has affected our PlayStation Network and Qriocity services. In order to conduct a thorough investigation and to verify the smooth and secure operation of our network services going forward, we turned off PlayStation Network & Qriocity services."

In a statement issued on April 26 from the company's U.S. subsidiary, it was subsequently confirmed that personal information was stolen. The information included names and addresses for registered PlayStation Network and Qriocity users, along with their birth dates, e-mail addresses and other personal information. Sony warned that other confidential information, including credit card numbers, could have been compromised, warning customers through a statement to "remain vigilant" by monitoring identity theft or other financial loss.

PREVENTATIVE STRATEGIES

The following mitigation strategies are intended to help the public proactively look for possible intrusions as part of a larger cyber security strategy:

- Be aware of unsuccessful (or even successful) email log-in attempts, especially regarding accounts associated with PlayStation and Qriocity. This is probably the first sign you may be targeted or already compromised.
- As credit card information may potentially be compromised, review credit card billing statements and credit reports regularly. The possibility of identity theft rises significantly whenever PII and other personal data is compromised.
- Immediately change passwords of any accounts associated with PlayStation and Qriocity networks.

The National Cybersecurity and Communications Integration Center (NCCIC) encourages the public to use safe, common sense cyber practices, such as not opening emails from unknown individuals or organizations, using spam filters and firewalls, running anti-virus and anti-spyware software and keeping them updated regularly.



NCCIC ADVISORY

National Cybersecurity & Communications Integration Center

For more information regarding computer security, visit the United States Secret Service (USSS), the United States Computer Emergency Readiness Team (US-CERT) or the Federal Bureau of Investigation's (FBI) 'Be Crime Smart' websites at:

www.secretservice.gov/fraud_email_advisory.shtml

http://www.us-cert.gov/reading_room/emailscams_0905.pdf

<http://www.fbi.gov/scams-safety/>

POINTS OF CONTACT

Please direct questions concurrently to the NCCIC and/or its appropriate component listed below:

NCCIC

NCCIC@HQ.dhs.gov
(703) 235-8831

US-CERT

SWO@US-CERT.gov
(703) 235-8832/8833

NCS/NCC

NCS@HQ.dhs.gov
(703) 235-5080

ICS-CERT

ICS-CERT-SOC@dhs.gov
(877) 776-7585