



April 26, 2011

SONY BREACH

Sony, in a statement on Monday, said engineers and security consultants reviewing company systems discovered that personal information from 24.6 million additional customer accounts may have been stolen. The information included customers' name, addresses, e-mail addresses, birthdates, gender, phone numbers, login names and hashed passwords. Other pilfered information came from a 2007 database that may have included about 12,700 non-U.S. credit or debit card numbers and expiration dates, but not credit card security codes, and about 10,700 direct debit records of certain customers in Austria, Germany, Netherlands and Spain that included bank account numbers, customer names, account names, and customer addresses. Additionally, billing addresses and purchase histories are also suspected to have been gathered by the cyber intruders.

Last week, Sony reported the information of 77 million customer accounts were exposed between April 17 and 19. That means personal information of more than 100 million customer accounts has been exposed. The breach is of users of its PlayStation Network and Qriocity online service.

The Department of Homeland Security said it's working with Sony to gain a better understand of what caused the breach that exposed personally identifiable information including names, addresses, passwords and, possibly, credit card information.

"The Department of Homeland Security is aware of the recent cyber-intrusion to Sony's PlayStation Network and Qriocity music service," DHS spokeswoman Amy Kudwa said. "DHS's United States Computer Emergency Readiness Team is working with law enforcement, internal partners and Sony to assess the situation."

With billing information and other details like purchasing history, fraudsters have plenty of information to launch targeted attacks. Fraudsters have knowledge of these people as being gamers; they have knowledge of their music; they know what kinds of games they bought. It's the perfect way to perpetrate fraud on the internet.

From here, it's easy for cybercriminals to use socially engineered tactics to trick consumers into revealing other personal details, such as Social Security numbers and bank account information. The correlation of this data is very useful. The combining of e-mail addresses with other information, and it's easy for fraudsters to turn that combined information into cash.

Sony's PlayStation Network is offline until more about the breach is uncovered. Sony has not said when it expects to be back online. Sony is sending a system software update to its gamers and asking them to change their passwords once the PlayStation Network is restored.

The investigation could take months and still not pinpoint the source of the compromise.

Spear phishing is a growing threat, and in the case of the Sony breach, it's the primary concern.

Hackers appear to have penetrated a Sony server or file, gaining access to names, mailing addresses, e-mail addresses, birthdates, login and password details for the PlayStation Network and Qriocity, as well as handles [online IDs] used by Sony gamers. Fraudsters now have plenty of information to launch targeted attacks.

In computing, phishing is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by email or instant messaging, and often directs users to enter details at a website, although phone contact has also been used. Phishing is when a fraudster sends you an email or link, claiming to be from a legitimate company. They'll often send you to a fake website they've created, and trick you into entering your password and personal information. You're then an easy target for account/ID Theft.

A phishing email will either entice you with the promise of money or appeal to your desire to protect your personal information by claiming that your account has been compromised. You will be advised to click on a link the email in order to receive money or to provide information in order to secure or re-activate your account.

By taking the bait and clicking on the link in a phishing email, you are exposed to at least two risks:

1. Clicking on any link in a phishing email is that you will be redirected to a web site that will look similar or identical to the web site the cybercriminal is impersonating. Once at the site, you will be directed to provide personal information that will allow the identity thief or cybercriminal to steal that personal information and use it for financial fraud or other crimes.
2. Clicking on any link in a phishing email is that you will be activating the execution and installation of a virus that will be surreptitiously installed on your computer. The virus may steal the personal information stored on your computer by transmitting the personal information to the identity thief or cybercriminal who sent you the phishing email. The virus may also take over your computer and turn it into part of a botnet (malicious software robot network) designed to transmit other virus laden emails to thousands of other computers around the world.

The anti phishing working group maintains a list of phishing scam emails and websites to help people identify and avoid being scammed in the future.

The anti phishing working group will review the message and any websites to which it links, and post it to the Phishing Archive on the anti phishing working group website.

1. Create a new email to [reportphishing@antiphishing.org](mailto:reportphishing@antiphishing.org)
2. Drag and drop the phishing email from your inbox onto this new email message
3. Do not use "forward" if you can help it, as this approach loses information and requires more manual processing.