After PlayStation and Epsilon hacks, take precautions to keep your digital data safe

May 13 2011, By Bridget Carey

Emails, home addresses, passwords, birthdates and bank account numbers. More than 100 million PlayStation Network users entrusted Sony with their data, which is now in the hands of hackers.

Experts say last month's Sony security breach may be the most expensive in history, and it comes on the heels of the largest email heist, as the addresses of millions were exposed in an Epsilon security breach.

I was hit by both, and last week I was on the receiving end of a robo-call phishing attack on my personal cellphone. Hoping I would panic and release my bank info, the scammers claimed my debit card had been canceled.

As many of us have learned recently, there will always be a risk of having your data stolen even if you give it to "trusted" companies. But without going completely off the grid, there are things you can do to better shield your personal information:

- Don't use a debit card online. Credit card companies typically protect users against fraudulent charges if reported, but things get more complicated with a debit card. If cash is taken out of a checking account, replacing that money doesn't always happen quickly.

Chester Wisniewski, a senior security advisor at security software firm Sophos, says victims need to watch credit card statements closely for a long time, since hackers could use the stolen data when guards are down.

If you gave Sony your debit card information, Wisniewski says, take no chances: "I would be canceling it without question."

For victims of the PlayStation Network hack, Sony is offering to cover the costs of credit insurance to pay for identity-repair costs, legal defense expenses or lost money from fraud.

- Change your passwords. Since hackers obtained PlayStation logon passwords and user emails, it doesn't bode well for people who use the same password for everything. If your PlayStation Network password is the same as your email password, change your email immediately.

Access to an email account is a hacker jackpot. They can find out what other online accounts and communities you belong, use your email to fill out those "I forgot my password" forms and change your passwords.

- Expect more spam and scams. If you were hit, expect an increase of email spam and information phishing attacks. Don't click links inside emails, and realize that no respectable company will ask for sensitive information via email Â- not even a phone number to verify your account.

As a backup, be sure to have security software that can watch your back if a link takes you to a malicious website.

- Use an alias when signing up for email lists. For most free email services, like Gmail and Hotmail, you can add a plus sign and a descriptive word after the username. (Instead of JoeSmith@gmail.com, for example, you can give Best Buy JoeSmith+bestbuy@gmail.com .)

It's a neat way to not only have mail from them filtered to a folder but to reveal if a company leaked Â- or sold Â- your email address. If you start getting non-Best Buy emails from that example account, it's time to

automatically forward all email to that address into the trash.

Obviously it's easy to decipher what a real email is when given something like JoeSmith+storename@gmail.com. Some services, like Hotmail, offer a way to create a more unusual alias email address.

- Stop clicking on Facebook junk. Malicious links have been on the rise in Facebook since Osama bin Laden's death, with people tempted to click on bogus "banned" videos and images. Facebook scams prey on your curiosity and vanity: Who is looking at your profile? Look at this banned video! Who thinks you're hot? The intent is to access your profile and collect information before spamming all your friends. Wisniewski said his team hears of 30 to 40 new Facebook scams a day.

- Don't let your guard down. There are those who believe that since no major identify-theft attacks have yet resulted from the Playstation theft, everything will be all right. But think about this: Would a hacker use the information when everyone is on guard and the crime is still in the media limelight? Hackers could wait months before they sell it or use it maliciously.