Expert gives tips on safeguarding against data theft

April 11 2011, By David Terraso

Nick Feamster, assistant professor at Georgia Tech's College of Computing and researcher at the Georgia Tech Information Security Center offers his expertise on the Epsilon data breach and what users and custodians can do to protect their data.

The Epsilon data leak incident was serious, as it exposed a large number of people to an attack called "spear phishing," whereby an attacker targets specific users or organizations with attempts to steal personal information. However, it is also important to realize that this incident could have been much worse. Many third-party organizations, ranging from identity management companies and large cloud service providers, like Google, have aggregated large amounts of our personal information in one place, making us increasingly vulnerable to the type of attack we saw with Epsilon, whereby a single breach can result in the compromise of a large amount of user data.

There are two big lessons we should take away from this incident. First, we must raise our own awareness about where our data is stored and become more cognizant of how we might be making ourselves vulnerable to these types of incidents by allowing data about us to be aggregated in just a few places. Second, we need better security tools: software will remain vulnerable, and compromise is inevitable.

Although this may be one of the largest data leaks we have seen in U.S. history, this is not the first instance of a very serious data leak. In the past, we have seen data leaks involving the breach of more sensitive

information, including credit card numbers and even Social Security numbers. Facing the stark reality that these compromises are likely to continue and worsen, we must develop better tools for prevention (i.e., making it difficult for attackers to access data once they have compromised a system) and auditing (i.e., figuring out exactly what data has been breached, when, and by whom).

Here are some quick tips on what users can do to minimize the damage that a data breach can have on them.

1. Safeguard passwords for sites that hold a lot of your data. In particular, do not use the same password for a site like Google as you may use for other sites. This may at least reduce the risk that a breach of your password on another site would result in your password on a "higher value" site also being cracked.

2. Try not to store information related to your identity in these services. Specifically, users might want to be particularly careful about documents that contain Social Security numbers, birthdates, credit card numbers, passwords to other accounts (such as bank accounts), and other information.

3. Be aware of phishing attacks, and pay particular attention to any request to "reset" your password on a high-value site. These sites, as a general rule, will never send you a link by email asking you to enter your password. Pay particularly close attention to any message that comes via email asking you to click on a link where you are asked to enter a password.

4. Be on the lookout for suspicious login activity patterns to your account. Sites such as Google provide information about where on the network your account was last accessed from (there is typically a link at the bottom of the website for this). You might want to periodically

check this information, to make sure that you recognize the places where your account has been accessed.

5. Take note of what sensitive data you may have stored in these services. If a data breach occurs, you will want to assess the worst-case scenario and take measures to protect yourself from fraud or identity theft. (For example, if you did have any documents with addresses, birthdates or sensitive information stored in these services, you may be more vulnerable to identity theft.)

In addition to things that users can do, there is also a serious need for more extensive protection against data leaks in the enterprise space. Software will continue to be vulnerable, and there will be users who will inevitably not take these recommendations. We do need better mechanisms to provide safeguards against these types of breaches in the event that a compromise does occur.

This is an active area of research in my group here at the Georgia Tech Information Security Center where we are developing various technologies to combat data leak threats.

Provided by Georgia Institute of Technology