December 26, 2012

Important Notice: Gmail, iCloud and Twitter Account Hacking!

Kiyoshi Otani
Chief Information Security Officer
Executive Vice President for Finance and Public Relations

Recently, incidents of receiving spoofed e-mails from hacked Gmail accounts are on the rise at the Institute. These attacks for hacking are becoming more and more sophisticated and do more than simply breaking into an email account with a vulnerable password. For example, recent trends show that hackers are capable of integrating and analyzing personal information pertaining to multiple network services and/or combining linkages of email accounts with fraudulent techniques. Please be aware of vulnerabilities that lie in linkages of network services that you subscribe to, and please review them in the light of needs, taking appropriate measures against these attacks.

Example of recent attacks:

1. Apply for a password reset in a service that the hacker intends to break into.
   → Information needed to reset the password is sent to another email account
2. Discover that email address (which received the information above) from open information and postings on Twitter and/or other network services.
3. Apply for a password reset to the company that provides the email account. For example, an easy target would be a company that accepts an application by phone by requiring only open information, credit card information (which the hacker has newly registered beforehand), and date of birth for client identification verification.
   → An email service provided by a company with a weak client identification verification system is taken over.
4. Break into a targeted email account using emails that the previously hacked email service received.

Example of actual damages:

1. Once iCloud is taken over, an iPhone is remotely operable using the “Find my iPhone” function.
2. Once a Gmail account is taken over, the hacker not only steals important information from the email account but also gain access to almost all services offered by Google, which are then used for the secondary attack.

Measures required for prevention:

As described above, one company with a weak client identification verification system can compromise the safety of all other network services that one may use. Information available from each service may vary, however users must be aware that the hacker is capable of analyzing information gathered from different services and use it to abuse them. While it is essential to properly manage a password, we strongly suggest all network users to take the following measures to avert these willful attacks.

- Reevaluate services that you subscribe to: Do not sign up with new services unless necessary, and unsubscribe to the ones that are no longer used

- Keep your personal information disclosure to a minimum
- Do not share the same set of ID and password with multiple services
- Be careful of fishing and skimming tactics
- If you notice a password change that you were not aware of, immediately stop using all the services that are dependent on the same security system.