Turn The Alarm Back On

BY | Sharifah Roziah Binti Mohd Kassim

Introduction

Many Internet users these days will have at least one Internet account, be it email, online banking or a social networking account. One possible reason for this could be the increasing number of people socialising on social networking sites, communicating via email and adopting online banking and e-commerce transactions on the net.

Account compromise refers to the unauthorised act of breaking in another person's account via various available means with malicious intention. This will expose victims to serious confidential data theft in their computers, identity theft, or use of the compromised accounts for spam or scam purposes on the net. Majority of account compromises is carried out for profits-based purposes, such as in spam and phishing activities. Main targets of account compromise are email accounts, social networking accounts and online banking accounts based on the trends we are seeing now on reports received from Internet users.

Statistics

Based on MyCERT's statistics in 2010 and 2011, incidents related to account compromise is growing on a quarterly basis, as shown below. It is predicted that this number will increase with more and more Internet users utilising social networking sites and Internet banking, with lack of awareness on safeguarding their accounts.

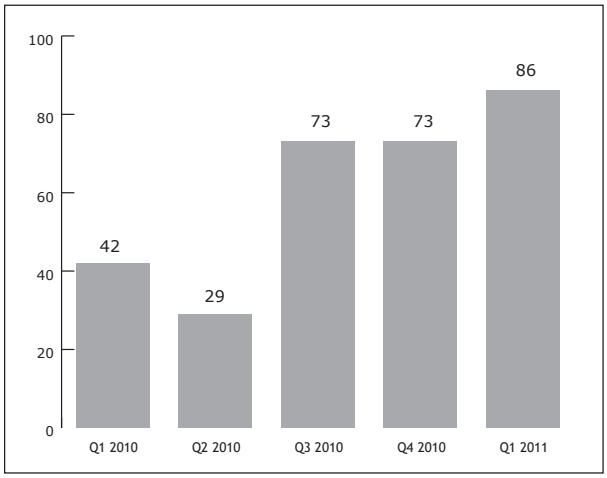

Figure 1: Statistics on Number of Reports Received on Account Compromise: Q12010 - Q1 2011

Indications of Account Compromise

There are many ways one can discover that their account has been compromised. There are several indications that a compromise has occurred and this includes, if it is related to an email account, you may not be able to login to your account or unknown parties like spammers and scammers are also actively using your account. Your friends/relatives may inform you that they receive spam or fraudulent emails from your email address. If it involves a social networking account, you may not be able to log into your account/ profile. Fake profiles impersonating yourself or your personal details and photographs uploaded on the net without your permission. If it involves an Internet banking account, you may notice your account balance decreased or totally wiped out or you may receive a message from your bank that you had transferred a certain amount of money on a particular date. Another sign

of a compromise is when another party is using your confidential data illegally.

How Accounts Are Compromised

There are several ways how accounts can be compromised.

1) Via malware infection in a computer. One of the common ways an account is compromised is through password stealing trojans. Once a computer is infected with a password stealing trojan, it is capable of stealing passwords from an infected computer and will relay the information to the hacker which can be used to break into your account.

2) Sharing passwords. When you share your password with others, you are also sharing your identity because you will be associated with any transactions or activities for that account. Based on MyCERT's experience in incident handling, we found quite a number of account compromise incidents were due to sharing of passwords with third parties such as with friends and colleagues especially concerning social networking account.

3) Using weak passwords. Another common cause of account compromise is due to the use of weak passwords. In a survey of MySpace passwords obtained by phishing, 3.8 percent of those passwords were a single word findable in a dictionary and another 12 percent contained a word plus a final digit; two-thirds of the time that digit was 1. Use of weak passwords makes breaking of passwords easier by humans and by password-cracking tools. Some examples of weak passwords are the ones with names of spouses, pets and birth dates. The simpler the password the more easier it is to break the password within a very short period of time. Unlike, strong passwords, which are difficult to break and takes a longer time.

4) Giving away passwords as victims of social engineering. This is another technique of account compromise in which passwords are obtained via social engineering techniques. This may involve telephone calls to victims purportedly from their banks, or ISPs asking them for their usernames/passwords.

5) Via phishing attacks. Phishers send phishing emails purportedly from the Bank or Service Provider requesting customers to change their passwords by clicking on a link in the email. The username/password typed in the phishing site will then be sent to these hackers and then used to illegally access a victim's account.

What Will Happen When Your Account is Compromised

Many users do not know exactly what happen when their account is compromised. Here are some possible scenarios when your account is compromised. Spammers in spam activities can use compromised accounts and scammers may use your compromised account for Nigerian scam activities. Cyber harassers can harass or threaten victims using details of the compromised account by creating fake profiles. Your compromised account can also be used to steal money if it involves Internet banking. Your system's account can be stolen for unauthorised access to your system, which leads to intrusion, deletion or alteration of files and other confidential data in the system. Your stolen account and password may be sold to an underground economy or posted publicly in online forums which can then be used by third parties for malicious purposes.

Mitigations

It is every account owner's responsibility to safeguard their accounts from being compromised by implementing proper mitigations. Never share your password

with another person to prevent manipulation of your password for malicious activities. Implement strong passwords by using passwords with at least 8 characters, combinations of alphabets, numbers, and characters and change your passwords on a regular basis every six months. Never use the same password for multiple applications and at multiple sites. Install an anti-virus software on your computer and update it daily. Make sure your computer is regularly updated with the latest security patches. Never click on any attachments you receive over the net, either from emails, chat messengers and avoid using public computers while doing online transactions or any activities related to your online accounts. Public computers may contain keyloggers or password-stealing Trojans or may not have anti-virus software in it.

What to Do if Your Account is Compromised

1. Retrieve back the compromised account and change the password immediately. Change all passwords on the system if a privileged password has been compromised. Users may consider changing other passwords as well such as their online banking, email or social networking accounts. Multiple credentials may have been stolen from the same user.
2. Consider closure of the compromised account if you're unable to retrieve back the compromised account to prevent further abuse of your account on the net.
3. Report to your respective bank if your bank account is compromised or if you noticed any decrease or suspicious activity in your account balance.
4. Lodge a police report at a nearby police station if your compromised account is used for malicious or criminal activities on the net such as in scam activities, cyber harassments or in impersonations.
5. Report to Cyber999 for assistance on account compromise incidents. They will assist and advise you accordingly on the matter.

Conclusion

In conclusion, account compromise is becoming a serious threat on the net. By looking at the growing number of account compromise incidents and its repercussions, account owners must be precautious and take proper preventive steps to prevent their accounts from being compromised. By being a little precautious and serious about the repercussions of account compromise, many incidents such as identity thefts, cyber harassments, intrusions, loss of money or confidential data can be prevented or minimised to a certain extent and thus keeping the Internet safe for everyone. ■

References

1. *http://www.daniweb.com/news/story277999.html*
2. *http://www.wired.com/threatlevel/2009/01/professed-twitt/*
3. *http://krarun.com/2010/07/19/social-networking-threats/*
4. *http://mashable.com/2009/10/06/gmail-accounts-exposed/*
5. *http://en.wikipedia.org/wiki/Password_cracking*
6. *http://windowslivewire.spaces.live.com/blog/cns!2F7EB29B42641D59!41528.entry?wa=wsignin1.0&sa=363915619*
7. *http://www.computerworld.com/s/article/9138956/Microsoft_confirms_phishers_stole_several_thousand_Hotmail_passwords*
8. *http://en.wikipedia.org/wiki/Social_engineering_%28computer_security%29*
9. *https://www.mycert.org.my*