Coping with a Compromised E-mail Account

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University, Northfield VT

From: Colleague
To: Mich Kabay
RE: Compromised e-mail account

Dear Mich,

Someone has stolen one of my e-mails (not NU), and is using it to ask for money by sending messages to my entire contact list. What can be done apart from changing my password?

* * *

Dear Colleague,

I discussed your situation with a colleague who has more experience responding to cybercrimes. The criminals *may* be

- using your e-mail account OR
- using one with a similar e-mail identification OR
- forging the e-mail headers to make it look as if they have control of your account.

Without access to the actual messages your friends received (including the usually hidden header fields), we cannot tell which technique(s) the criminals are using. If they are using a different account or forging the headers, they presumably have your distribution list to be able to reach your correspondents.

Our recommendations are as follows:

1) Change the password on your e-mail immediately to a difficult-to-guess form; e.g., uja*RODIN_39. Using random syllables (consonant-vowel) helps you remember the password. Record it in a safe place so you can get the remaining e-mails you will need.

2) Establish a new e-mail account with a name noticeably different from the one you have used in the compromised account; e.g., if you were, say, < colleague@gmail.com >, perhaps the new account would be < nucolleague@gmail.com >. If there are security questions beyond the password, choose questions you have not used before; e.g., if your old e-mail account had a question about your city of birth, don’t use that particular question for the new account.

3) Be sure that you can transfer your contact list to the new e-mail account; if there is no provision from the e-mail supplier, then be sure that you have an independent backup of the list such as a file. Normally, you can store all your addresses in your OUTLOOK contact list that is part of the University’s standard software on our laptop computers.

4) Using the *old* (possibly compromised) account, immediately send an e-mail message to everyone on your contact list telling them that

   a) you are OK and they should ignore messages claiming that you are in trouble and need money;

   b) you are shutting down your current e-mail account because it is no longer trustworthy;

   c) you will be using the new account called < ______ > (fill in new address);

   d) if they can, they should add the old address to their JUNK filter.

   Put some details into your signature block so people can have confidence that it's really you sending the message; e.g., include info such as your professorial title or your phone number.

5) Contact or log on to the account-management pages for every mailing-list you subscribe to or association you belong to and change your e-mail address to the new one using their change-of-address procedures. Occasionally, you may need to do this using your *old* (compromised) account because some mailing lists send confirmation of a proposed e-mail change to the *original* (old) e-mail address for verification. That approach interferes with the ability of criminals to redirect your correspondence without your permission.

6) *Shut down the compromised account.* Use the procedures available from your e-mail supplier – generally available through their HELP feature.

7) More generally, be absolutely sure that you never use a password for more than one account. If there are *any* accounts which use the same password as the compromised account, you *must* change their passwords at once.

8) You may store your passwords securely in OUTLOOK on your computer by creating a new contact card and checking the "Private" button (looks like a padlock) in the CONTACT sheet. You should create a separate contact card for each Website or other password-protected function.

9) Do not use the Internet Explorer "remember password" function. There is no security to prevent someone who has access to your computer from logging in to password-protected. Modern browsers offer a "password safe" feature that will remember the password for each Website but impose a master password. If you use Internet Explorer as your browser, download and install Bruce Schneier's "Password Safe" software which is safe, secure and free: < http://passwordsafe.sourceforge.net/ >. It will impose a master password on the "safe" so that only you will be able to use your other passwords on Websites. Effectively, you will have only one password to remember even though you may have hundreds of different, complicated ones. My passwords (but not the master password) look like this: 8*4Jur_hvn(_gaM. Because the computer password safe remembers them, they are all very difficult for a criminal to guess ("break").

Good luck!

For further reading on this subject with additional practical suggestions, see the following articles.

- Boatman, K. (2007). “How to Recover When Your Email Account Is Hacked.” *Earthlink Security Center* < http://www.earthlinksecurity.com/articles/email_hacked/index.html >.

- Chase, J. (2011). “Hacked and Hijacked: What to Do if Your E-mail Account Gets Compromised.” *Switched* < http://www.switched.com/2011/02/24/what-to-do-email-account-hacked/ > (2011-02-24).

- “Security, Doctor” (2011). “What to Do When Your Email Account Has Been Compromised.” Zone-Alarm by Check Point < http://blog.zonealarm.com/2010/06/what-to-do-when-your-email-account-has-been-compromised.html > (2011-06-10).

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >