Managing Lost Passwords:
How Not to Do It

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Dear Bob,

I am writing to you formally in your capacity as CEO of the Metaphoronic Corporation, makers of the bioport<http://www.imdb.com/title/tt0120907/> that I had installed in my lower spinal column last year for direct neural connectivity<http://brainwaves.corante.com/archives/2008/07/02/webcast_of_entire_neural_interface_conference_in_june.php> to my Windows 2010<http://blogs.zdnet.com/microsoft/?p=592> operating environment. It’s been great, by the way: I love the way I can simply _think_ what I want to make the system perform properly. The only problem I’ve had is what happens when I daydream, but let’s not go there.

Today I could not sign into the Web page for the SpinalTap<http://www.imdb.com/title/tt0088258/> application that makes adjustments to the interface and could not find instructions on getting the password e-mailed to my e-mail account or on how to reset it to a temporary password and get _that_ by e-mail, so I called your HelpDesk to find out what to do.

The very nice agent cheerfully demonstrated that your HelpDesk has no clue how to deal with lost passwords for SpinalTap: she

1) Asked me for my user ID: unacceptable because it began a phone-based process for resetting a password;

2) Asked me one of my verification questions (“What was the last name of the girl who arranged for me to step on her foot on a ski trip in 1963?”): UNACCEPTABLE because it means the authentication data are not one-way encrypted;

3) Read me my old password: UNACCEPTABLE because it means the password file is not one-way encrypted!

Normally, passwords and other authentication data are one-way encrypted: the responses to questions are encrypted and the ciphertext of the response is compared to the stored ciphertext of the correct answer; however, it is difficult (expensive, slow) in practice to regenerate the original cleartext data unambiguously from the stored ciphertext. (See my lecture on cryptography fundamentals if you like<http://www.mekabay.com/courses/academic/norwich/is340/20_Cryptography_1.ppt>.)

Access to the authentication questions, to their answers, and to the passwords implies that the HelpDesk agent(s) can impersonate customers at any time by logging into SpinalTap using their purloined IDs. The damage caused to your Company's reputation if one of your employees were to sabotage a customer’s settings and cause serious damage – psychotic breakdown, for example,
due to the impression that two-headed lizards were chewing on his left hallux – could be disastrous.

To put the problem in perspective, it would be the same kind of problem of impersonation as if a member of your staff were falsely accused of damaging Company records, sending inappropriate e-mail within the Company or to external recipients or posting inappropriate materials on a Company Web page. Not only would the victim of the impersonation suffer – so would the Company.

Although I realize you probably know this perfectly well, for the record, I will assert that

1) The problem is not the individual HelpDesk agent's: she was courteous and professional and doing her job as she was instructed to do it. She deserves no blame.

2) IMNHO,* The SpinalTap system, not the HelpDesk, should have a mechanism for resetting the password by ASKING THE USER the authentication questions on screen before e-mailing a one-time password to the officially registered e-mail account for recovery.

3) The idea that a phone call supposedly from a user (but potentially from a social engineer) is an acceptable basis for resetting has been discounted decades ago. In the absence of automated password resets, the only acceptable mechanism for secure re-authentication of an employee is to have the user physically come to the HelpDesk or to a proxy for recognition or for documentary identification and authentication using a Company-issued photo ID. Possibly you can get around this requirement in a distributed environment by using Webcams, but there are security issues there too because of the uncertain integrity of digital imagery. However, for an external customer who cannot reasonably show up at your offices, you _must_ develop a social-engineering-resistant methodology like the simple approach using pre-established e-mail addresses which is already implemented by uncounted numbers of Web sites.

I recommend that the written procedures for coping with loss of a password on the SpinalTap system be analyzed by the Company HelpDesk managers and corrected. If there are no written procedures, I will help write some for you that conform to industry best practices at my usual consulting rates.

Best wishes,

Mich

=>o ASCII ribbon campaign against HTML e-mail o<=

* IMNHO = in my never-humble opinion <g>

***

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of
Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2008 M. E. Kabay. All rights reserved.

Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.