Get Authentic Advice
Before Giving Advice on Authentication

by M. E. Kabay, PhD, CISSP

I recently visited a site where the signup procedure included a request for a secret authentication question. Here's an edited version of what I wrote to the folks running the site after I signed up.

# # #

Dear Folks:

On the HELP page where you discuss good secret questions, you have written:

> When you create a new <certificate>, we ask you to choose a secret question and type the corresponding answer. If you forget your password, we'll ask you for the answer to your secret question and the name of the country and region in which you live. We'll use your answers to these questions to verify your identity before we allow you to choose a new password.

For your security and convenience, make sure that the answer to your secret question is:

(1) Something only you know.

(2) Not related to your password or sign-in name in any way.

(3) Unlikely to change over time.

(4) Extremely difficult for others to guess, even if they see your secret question.

Some examples of good secret questions are:

(a) What are the last five digits of my Visa card?

(b) What are the last five digits of my social security number?

(c) What is my mother's maiden name? <

[I have labeled the items for purposes of clarity.]

Your criteria are good.

Your examples are bad.

Question (a), the credit-card number, fails criteria 1 and 3: lots of people can know the user's credit-card number and people have to get new cards all the time. In addition, the answer is not unique because many people have several credit-cards. Depending on what your staff do when an answer is wrong, there could be repercussions such as being permanently barred from reactivating the certificate.
Question (b), SSN, fails criteria 1 because abuse of the social security number has resulted in widespread availability of this information, especially to criminal hackers. Some states even use the SSN as the driver's license number — and sell CDs with those data to anyone willing to pay.

Question (c), mother's maiden name, fails criteria 1 because that information is a matter of public record and can even be obtained online in some states. In addition, many family members know the answer and, with the widespread occurrence of unmarried mothers, there are now many people whose name is the same as their mother's family name.

Please feel free to use the examples and analysis above (verbatim, if you like -- no attribution required) to show your users how easy it is to choose bad questions.

To get the concept across to inexperienced users, I recommend plentiful, personally memorable and preferably amusing examples. Consider

* What was your first boy/girlfriend's favorite movie/book/?

* What was the nickname of your favorite teacher in grade six?

* What made you get really sick when you were 4 years old?

* Whom did your best friend imitate at the famous Halloween party in where three of your schoolmates were arrested?

* What award are you proudest of?

* How long and where was your sister away the year your dog ate the hamster?

#

I suspect that somebody without adequate training in INFOSEC principles was responsible for providing their examples.

Recommendations:

* Before giving advice to the public on legal matters, consult an attorney with suitable expertise for advice.

* Before giving advice to the public on information security matters, consult an information security specialist with suitable expertise for advice.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

Copyright © 2000 M. E. Kabay. All rights reserved.

The above version includes corrections of errors in the original article:

I gave bad examples of personal questions.