Texas Department of Information Resources
CYBER SECURITY TIPS
Monthly Newsletter
Office of the Chief Information Security Officer | January 2009 | Volume 3, Issue 1

Challenge or Secret Questions

WHAT ARE CHALLENGE OR SECRET QUESTIONS?

Knowledge-based authentication, or the use of *Challenge or Secret Questions*, helps computer users access their accounts when they forget their password. The questions are often designed as simple, easy-to-remember prompts that only the authorized user should be able to answer. They are in effect a backup to your password.

While some systems allow users to create their own challenge or secret questions, most systems have pre-populated questions such as "What is your mother's maiden name? What is the name of your first pet or car? What is your favorite color?" While these systems are a great convenience for the end user (since they are not likely to forget the responses) and are efficient from the administrator's perspective (low overhead), they are very weak from a security perspective.

WHAT ARE THE SECURITY CONCERNS WITH USING CHALLENGE OR SECRET QUESTIONS?

There is a limited pool of secret questions that most Knowledge-Based Authentication systems use, and many of the questions have a limited amount of potential responses, such as "What street do you live on?" If someone researches you and discovers the answers for your questions, they could gain unauthorized access to your account.

In some cases, these answers are easy to guess. A secret question such as "What is your favorite color?" is usually answered with common color names such as *red*, *green*, *blue*, or *orange*. This type of question should be avoided. Other questions with easily guessable answers (i.e., "Which month were you born?" "How many children/grandchildren do you have?" "What year were you born in?") should also be avoided.

The ability for someone to guess the response to a user's secret question has greatly increased due to the large volume of information available on the Internet. This was demonstrated during the recent presidential campaign, when one candidate's email account was hacked into. The attacker was able to do so by conducting a minimal amount of research about the candidate using information found on the Internet to answer the secret questions and get the password for the email account.

Users need to be aware that there is a tremendous amount of information available about them, not only through Internet search engines, but also social networking profiles and other sources.

WHAT CAN BE DONE TO MAKE CHALLENGE OR SECRET QUESTIONS MORE SECURE?

As with the design of a regular password, the responses to secret questions should be difficult to guess but easy to remember. Users are encouraged not to provide the technically correct response to the question. Similar to developing a strong password, the response to a secret question is in effect a password and thus should have the same protections. Using a combination of upper and lower case letters, special characters, and numbers is recommended. There are many ways to obfuscate your response. The key is to develop a methodology that is easy for you to remember but difficult for someone else, even someone you know, to guess. Examples include:

1. Begin and/or end each response with a number, capitalize a letter, and use a special character. For example, the response to your mother's maiden name of *Smith* would be *44SmitH!* You can also insert a number and special character in the middle of the word. In this example, the answer to your mother's maiden name of *Smith* would be *Smi44!th*.

2. Provide answers that do not correspond to the question, thus making it difficult for an attacker to correctly guess. For example, use the name of a city as the response for *mother's maiden name*.
3. Use the question itself to create an easy-to-remember passphrase. By combining the main part of the question with one of your favorite catchwords, you can create a passphrase you can remember. If the question is asking for your favorite sports team, you can, for example, combine *Dallas Cowboys* from the question and combine it with a phrase from your favorite show, such as *CSI*. Your answer would be *Dallas Cowboys CSI*.
4. Follow best practices for strong passwords when developing your responses, such as making them at least eight characters long and using numbers, upper and lower case letters, and special characters. The answers can be different on different websites, even if the same secret question is used. Thus, a hacker won't potentially have access to other accounts if one is compromised.
5. As with passwords, do not share the responses to your Challenge or Secret Questions or your methodology for developing them with anyone.

You should also periodically search your name in an Internet search engine to stay aware of what information about you is freely accessible on the Internet.

ADDITIONAL RESOURCES

For additional information on Challenge or Secret Questions, please visit:

- Choosing and Protecting Passwords: **www.us-cert.gov/cas/tips/ST04-002.html**
- Supplementing Passwords: **www.us-cert.gov/cas/tips/ST05-012.html**
- Using Secret Questions: **www.owasp.org/index.php/Using_Secret_Questions**

For previous issues of the Monthly Cyber Security Tips Newsletter, please visit **www.dir.state.tx.us/security/reading**.

For more information on Internet security, please visit the SecureTexas website – **www.dir.state.tx.us/securetexas**. SecureTexas provides up-to-date technology security information as well as tips to help you strengthen your part of Texas' technology infrastructure. Report serious information security incidents as quickly as possible to your agency's Information Security Officer and to DIR's 24/7 Computer Security Incident Notification hotline: (512) 350-3282.

Brought to you by: MS-ISAC
www.msisac.org

Powered by: US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM
www.us-cert.gov

Distributed by: DIR Secure Texas
www.dir.state.tx.us/securetexas