



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 (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 is your favorite color?” If someone researches you and discovers the answers for your questions, they could gain unauthorized access to your account.

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 of the candidate’s email accounts 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 something that is hard to guess, but easy to remember. Users are encouraged to not 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. The use of 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.

Remember: Do not share your methodology with anyone.



Answering Challenge Or Secret Questions:

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 "44SmithH!" OR Insert a number and special character in the middle of the word. In this example the response 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, a user may 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 combine "Sports Team" from the question and combine it with a phrase from your favorite show, such as "CSI." Their answer is, "Sports Team CSI."
4. Follow best practices for strong passwords when developing your responses, such as making it at least 8 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.

As with passwords, do not share the responses to your Challenge or Secret Questions, or your methodology. It is also advised to periodically search your name in an Internet search engine so you are aware of what information about you is freely accessible on the Internet.

Last Words—Cyber Security Trends 2009



The volume and complexity of cyber threats continue to increase. More of our activities—whether at home, school or work involve computers and the Internet. In fact, in the not-too-distant future, your household appliances may be computerized and controlled remotely from your PDAs. Simultaneously, the knowledge required to launch a successful attack continues to decrease. As we develop more defenses, the cyber criminals and hackers come up with new ways to attack our computers. These factors create an environment in which vigilance on a daily basis is required to help mitigate the risks. Threats such as identity theft, worms and viruses, loss of sensitive information and other malicious activity are part of an ever-evolving cyber security threat landscape.

Some of the key challenges we are facing in 2009 focus on application security. Application security is a crucial layer in a multi-tiered cyber security strategy. Building security in at the beginning of development is an important factor in minimizing potential vulnerabilities. We've seen the results when vulnerabilities in web applications are exploited, leading to SQL injection attacks, cross-site scripting and other malicious activity.

Cyber criminals take advantage of web sites that have poor security to add code to the web site without the knowledge of the web hosting company. That code may silently re-direct the user's computer to another site which will download malware to the user's computer, without the user's knowledge. The attackers may also add a script to the site that will automatically execute on the user's computer.

Another alarming trend continues to be the evolution of cyber crime, which has morphed from fairly innocuous web-site hacking and "graffiti" attacks to organized crime syndicates seeking profit. Cybercrime is now big business. The economic recession is another factor that may impact cyber security challenges. The risks due to insider threats are another major concern, and are expected to increase due to the economic downturn. Additionally, phishing scams and other social engineering attacks will increase, as attackers try to take advantage of bank closings, claims for "easy credit" or other online scams. Be vigilant.

Powered by:

Brought to you by:



US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM



MS-ISAC