

UHI INFORMATION TECHNOLOGY NEWS

February 2007

A publication of the Department of Information Technology

STRONG AND SECURE PASSWORDS

Even though they're often overlooked for more complex and high profile computer defenses like firewalls and anti-spam and anti-spyware software, passwords are an extremely important component of any organization's computer security strategy. In fact, passwords are so important that rule #5 on the Microsoft Security Response Center's top ten list of computing security laws states, "weak passwords trump strong security."

Poorly chosen passwords can result in compromises of individuals' systems, data, or even an organization's network. As the University of Houston's first line of defense against stolen data, passwords play a major role in securing important and sensitive information, helping keep the "bad guys" (hackers, spammers, phishers) out while safeguarding our systems and accounts. Passwords also serve as the primary (and often only) authenticator of users, making them the equivalent of a computer system's ignition key.

In addition, UH passwords provide security for many of the university's broad-based software applications, including the

PeopleSoft, Cougar 1Card, and CougarNet systems, as well as the UH Student System (which includes online enrollment, admissions, and student financial records). These and many other university applications contain confidential data and information on students, faculty, and staff, and are required by law to be adequately protected from hackers.

Security Breaches

As important as passwords are to UH's overall security strategy, many users don't know about-much less follow-basic password guidelines. Instead, they offer up weak passwords that provide little resistance to hackers' efforts.

Recent news stories have chronicled major computer security incidents that have resulted in significant data losses within government agencies, banks, and investment firms. In some instances, security breaches were traced to careless and negligent use of passwords.

While financial and government entities are primary targets of hackers, they aren't the only targets. Although not as well publicized, major security breaches have occurred within U.S. institutions of higher education that have led to compromised personal information and data on hundreds of thousands of people.

Several high-profile incidents took place this past year. In April 2006, the University of Texas computer network was hacked, resulting in an info-breach affecting 197,000 people. In May, Ohio University suffered two separate hacking incidents within a month of each other that compromised the personal information of 360,000 people. Then, in June, Western Illinois University had to notify 180,000 people that their personal data had been compromised. These incidents, which represent just a few of the total number of security breaches that occurred at U.S. colleges and universities in 2006, illustrate the need for securing our important data through strong passwords and other means.

Weak Passwords

Passwords are effective only to the extent that hackers can't figure them out. The use of weak passwords (passwords that can be easily guessed or obtained by a hacker) provides attackers with numerous opportunities to compromise systems and the data contained within them.

Keeping Your Passwords Secure

Control Access to Your Passwords

- DON'T SHARE YOUR PASSWORDS WITH ANYONE.
- Memorize your passwords instead of writing them down.
- If you must write your passwords down, don't store them around your computer or in an obvious place.
- Change your initial password immediately.

Avoid These Password Pitfalls

- Passwords consisting of names, house numbers, social security numbers, birth dates, phone numbers, or any other easily guessed or easily obtainable information.
- Passwords formed from words found in a dictionary (including foreign words.)
- Acronyms, geographical or product names, and technical terms.
- Names from pop culture, e.g., spock, eminem...also slang words.
- Simple strings of letters from the keyboard or keypad, e.g., qwerty.
- Any of the above spelled backwards or pluralized, or with some letters capitalized, appended, or preceded by a single digit or special character.

Strong Passwords

- Contain eight characters or more.
- Include combinations of upper and lower-case letters, numbers, and special characters:
! # % & () * @ ^
- Should be changed at least every 90 days; and passwords protecting privileged or high-level access accounts should be changed more frequently.
- Should not be reused.



Weak passwords trump strong security.

continued on back

Hackers employ a variety of methods to illegally obtain passwords. One of the more popular and frequently applied methods is the use of “cracker” software, which is available to hackers in the form of readily available and relatively effective computer programs that contain entire dictionaries of multiple languages.

A feature of cracker programs is that they can create words from word lists based upon popular (“pop”) culture, such as slang terms and terms from movies, novels, and music. This feature is useful to hackers because these words and phrases are often used in the construction of passwords.

Cracker programs are also responsible for “brute force” attacks against systems. These attacks occur when software is used to compute every possible combination of letters, numbers, and punctuation characters to crack a password. UH protects itself from these attacks through automated lockouts that prevent additional login attempts after a certain number of failed ones. The university also constantly monitors logins, and when a large number of failed attempts are registered, system administrators are notified.

Passwords are effective only to the extent that hackers can't figure them out.

An issue relating to the use of weak passwords is the “single password” factor, referring to the use of a single password to safeguard multiple accounts. Strictly from a security standpoint, it's always safer to use different passwords for each of our accounts. But studies have shown that a majority of users (86%, according to a recent poll of IT administrators) employ just one or two passwords for all of their separate accounts. They do this because it's far easier to keep up with a couple of passwords than with many.

However, if only one or two passwords are used to protect several accounts, best practices dictate that these passwords need to be strong ones, capable of deterring a thief or hacker. This links to the fact that one or two strong passwords are better than several weak, poorly chosen ones...especially when they are changed on a regular basis.

Another issue with weak passwords relates to how we remember them. Often, we compose our passwords using bits of personal information, such as our child's birthdate, our mother's maiden name, a PIN number or a street address. We do this because it's easier

to remember passwords made up from personal information than passwords constructed from random strings of numbers, letters, and special characters. But, by using personal information in our passwords, we create a security problem. Hackers aren't dummies; they know our tendencies and they capitalize on them. They go after our birthdates, maiden names, street addresses, and phone numbers because these items of information are relatively easy for them to uncover. By avoiding the use of personal information in our passwords, we make it much harder on hackers to gain access to our information.

Strong Passwords

Strong passwords, a.k.a. complex passwords, are those that are hard to detect both by humans and by computers. They rely on deterrence as their defense, achieved by being sufficiently complex to deter hackers from spending a lot of time and effort to crack them.

Strong passwords are designed to reduce or eliminate the chances of hackers figuring them out through commonly used methods, and they are effective up to a point. But even the strongest password can be cracked by a knowledgeable, patient, and determined hacker using a sophisticated cracker program running on a very powerful computer.

Increasing a password to eight letters—using upper and lower case letters—jumps the number of possible combinations to 53 trillion.

Strong, complex passwords consist of two main features: a large (preferably eight) number of characters; and a mix of numbers, upper and lower case letters, and special characters. Adopting these features in your passwords provides adequate protection in most cases.

Recommendations

The University of Houston's password security recommendations are commensurate with the importance of the protected information and data. This means that low-risk, less critical UH systems such as IT Training or personal e-mail accounts don't require the same degree of password protection as systems with higher risks associated with them.

Obviously, protecting the university's corporate and financial data within the PeopleSoft system, and protecting students' access

to their grades and personal information requires a much higher level of security.

However, a certain amount of compromise is necessary with the creation and use of strong passwords that are, by design, complex. Strong passwords have to be complex enough to keep the information they protect safe, but not so complex that they're constantly forgotten and have to be reset. Forgotten passwords can lead to major delays and interruptions in services, increased support costs, and a reduction in the efficiency of university processes and operations.

A proven and effective way to achieve easily remembered strong passwords is by associating their characters with a phrase or song title. For example:

Step 1—Choose a phrase: e.g., *Home of the University of Houston Cougars*.

Step 2—Write down the first character of each word: HotUoHC-s (To meet the eight-character minimum, Cougars was hyphenated as C-s.)

Step 3—Substitute special characters and numbers to increase complexity: H0tUo@UU-cl (Choose substitutions that have meaning to you.)

Password Changes Coming!

On Monday, March 19, 2007, UH will begin implementing new password standards for the campus. The IT Strong Passwords project, created to protect the university's systems, data, and network, requires all computer users to begin employing strong and complex passwords. The new standards go into effect starting with the CougarNet system. Other UH systems will be phased in over several months.

As additional UH systems are brought into compliance with the new password standards, IT will keep you informed. For more information on strong passwords, go to www.uh.edu/strongpasswords.

Facts on Strong Passwords

- There are 308 million possible letter combinations for a six-letter password that uses all upper case or lower case letters.
- A hacker with a readily available password “cracker” program can check them all in under three minutes.
- Increasing a password to eight letters—using upper and lower case—jumps the number of possible combinations to 53 trillion.

IT SUPPORT CENTER

PHONE SUPPORT
713.743.1411

24 x 7 (Except university holidays)

WALK-UP SUPPORT

Philip Guthrie Hoffman Hall (PGH) Room 116

8am - 8pm, Mon. - Fri.

(Except university holidays)

E-MAIL SUPPORT
support@uh.edu

Visit Us Online @ www.uh.edu/infotech/help