University of Dayton
eCommons

News Releases | Marketing and Communications

10-9-2008

New Times Call for New Passwords

Follow this and additional works at: https://ecommons.udayton.edu/news_rls

Recommended Citation
"New Times Call for New Passwords" (2008). *News Releases*. 1702.
https://ecommons.udayton.edu/news_rls/1702

This News Article is brought to you for free and open access by the Marketing and Communications at eCommons. It has been accepted for inclusion in News Releases by an authorized administrator of eCommons. For more information, please contact frice1@udayton.edu, mschlangen1@udayton.edu.

University of Dayton, Ohio (url: http://www.udayton.edu/index.php)

New Times Call for New Passwords

10.09.2008 | Campus and Community

This fall, unit by unit and student by student, computer users around campus are putting what information technology risk management officer Dean Halter called "teeth" into their network passwords.

The new policy on "strong passwords" is all in the name of security, Halter said. Strong passwords, which use mixed cases, numbers and seldom-used characters, make it harder for unauthorized users to break into the network and access student, health, personnel, financial and other data.

"A good password policy is just part of a comprehensive program that includes antivirus and antispyware protection, patch management solutions, intrusion prevention systems, firewalls and other security measures," Halter said, asking people to see the inconvenience as a small investment in security. "Every member of the UD community, not just UDit, has to do their part to protect all the sensitive information we maintain and they access every day. A virus on a workstation, a lost flash drive with a spreadsheet, sharing a password to allow someone Internet access — are all enough to undermine the layered security solution we've put in place. Asking users to change their passwords is a very small but important part of it."

For the past several years, UDit assigned strong passwords to new users with their Novell network accounts, but users had the option to change them.

"Now, you'll be able to change it, but you can't just change it to something simple," he said.

Departments have established their own deadlines; the conversion is targeted for completion by the end of the calendar year, Halter said. To provide assistance, UDit has created a Web site (url: http://campus.udayton.edu/%7etss/passwords.php) with password requirements, tips on creating easy-to-memorize passwords, and instructions for changing the password and synchronizing it with Notes and workstations. A user can also use an online "password checker" to make sure it meets all the requirements.

Some password security wisdom from the pros in UDit:

- Keep your password in your head, if at all possible. It's seven characters — just like a phone number and two fewer than your Social Security number.
- Don't panic. It's good for five years — longer than some computers.
- Randomness trumps mnemonics: Hard to believe, but you weren't the first person to think of using your pet's name in your password. This and other easy-to-find bits of personal data — birth dates, nicknames, ZIP codes and so forth — are easy starting points for figuring out a network password.

Poor but nonetheless popular places to store a password:

- Under your keyboard
- On a post-it note affixed to your monitor
- Written in permanent marker on the side of your hard drive
- On a Rolodex card marked "passwords"
- On your bulletin board

Why are strong passwords better?

People are trying to break into the network 24 hours a day, Halter said.

"I was reviewing the system logs on one of our servers the other morning and saw that someone had tried unsuccessfully to brute-force their way into it by guessing different user names and passwords 600-plus times over the course of the previous evening," he said. "A typical week will see UD receiving 40 million emails and dropping 98 percent of them as Spam, many trying to convince recipients to reply with their user names, passwords or Social Security numbers or open an attachment that'll

install a virus."

The detriment of intrusion is much greater than mere inconvenience, he said.

"A Trojan horse can give a bad guy access to all the information you work with in the course of a day — research, intellectual property, education records, credit or debit card information. … It's reported that it takes the bad guys anywhere between 4 minutes and two days to hack an unpatched machine. We're just trying to make sure everyone understands the risks and what we are trying to do."

Call the help desk

For more information about passwords, see the Web site above or contact the help desk at 229-3888.