Metro.net (web)

Resources

- Safety
- Pressroom (web)
- Ask the CEO
- CEO Forum
- Employee Recognition
- Employee Activities
- Metro Projects
- Facts at a Glance (web)
- Archives
- Events Calendar
- Research Center/ Library
- Metro Classifieds
- Bazaar

Metro Info

- 30/10 Initiative
- Policies
- Training
- Help Desk
- Intranet Policy

Need e-Help?

Call the Help Desk at 2-4357

Contact myMetro.net

Password Protected

Metro's new log-in procedure wants security-strength passwords that refresh every 60 days.

By Elizabeth Bennett
ITS Chief Information Officer

ITS Software Engineer Vath Nguon and Systems Project Manager Richard Bezjian at ITS Data Center. Nguon will supply the code to implement the new password security procedure.

(August 25, 2009) Information Technology Services (ITS) is launching a new password procedure designed to strengthen security measures that protect Metro's network against unauthorized access.

Last week, many U.S. news services reported a 28-year-old hacker has been charged in what federal prosecutors are calling the largest case of identity theft ever seen. The hacker and two others were arrested for stealing 130 million credit card numbers from several retail vendor networks.

Incidents like this highlight the ever-present threat of cyber attacks and network security breaches.

To keep Metro's network and systems secure, ITS utilizes a variety of security methods, one of which is the use of log-in passwords to validate an employee's identity.

The new password log-in procedure, which begins Thursday, August 27, will require employees to enter a "strong" password when their current password expires. The new password will be valid for 60 days. Previously, passwords had a 30-day time limit. As before, invalid password attempts are limited to three.

Be strong! When you enter a 'weak' password ...	the directions get specific.
	"The password supplied does not meet the minimum complexity requirements. Please select another password that meets all of the following criteria: (The password) is at least 8 characters, has not been used in the previous 12 passwords, must not have been changed within the last 8 days, does not contain your account or full name, contains at least three of the following four character groups: English uppercase characters (A through Z) English

lowercase characters (a through z) Numerals (0 through 9) Non-alphabetic characters (such as !, $, #, %). Type a password which meets these requirements in both text boxes."

Roll your mouse over image to see message box that comes with an invalid password.

What is a strong password?

Strong passwords use length and a mix of uppercase and lowercase letters, numbers and special characters to create complexity in the structure of the password and are considerably harder for an attacker to "crack" and have these traits:

Length: Passwords must contain a minimum of 8 characters and a maximum of 14 characters.

Use the entire keyboard: Create your password by selecting from three, or all, of the following four groups:

- Upper case letters – A to Z
- Lower case letters – a to z
- Numerals – 0,1,2,3,4,5,6,7,8,9
- Special Character - symbols found on the keyboard that are not characters or numerals, such as # @ & *

Tips for creating a strong password:

Create a strong password by thinking of a short phrase you can remember and condense it by removing vowels and substituting numerals and special characters for some of the letters. For example: "C$200wpGO" would represent the phrase "Collect $200 when passing go"; or, "Spd>$100Tx" would represent the phrase "Speeding costs more than a $100 Ticket."

Think out of the box: Put a little *Piz@zZ! in your password, says Vath Nguon.

Do not use your user name, real name, or company name, do not use words that are found in a dictionary in any language and avoid using sequences or repeated characters or numerals, such as qqqq, 1234, or abcd.

Password change

To keep your password secure, it will expire every 60 days. When you create your new password, it will be validated for the traits of a strong password. Your password will not be accepted if it fails the validation.

Forgot your password?

If you forget your password, enter “password” for your ID and “password” for the password and a temporary password will be generated for you to log-in. After you log on, you will be asked to create a new, personal password.

Reminder: After three invalid password attempts, your account will be locked out. To unlock your account, please contact the Help Desk at 922.4357(2HELP).
