Technology for Librarians 101

Computer Security - Password Management Best Practices

Passwords are an important aspect of computer security. They are the front line of protection for sensitive data, network access, and email access. Passwords are also used on a lot of websites to merely gain access to news articles and other information.

With the need for more and more passwords, how do you create another good password that you will keep secure by never writing it down? Please follow these practical tips and best practices guidelines.

Create a strong, easy to remember password

- Use a minimum of 12 characters.
- Use a combination of letters (upper and lower case), numbers, and keyboard characters.
- Do NOT use a dictionary word (in any language) or any commonly used word such as:
    - Name of family member, pet, friend, co-worker, fantasy character, etc.
    - Login user name, computer name, command, site, company, hardware, software.
    - Birthday and other personal information such as address and phone number.
    - Word or number pattern like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., fido2, 3secret).

A good way to create a strong password is to take 2 or 3 words or a phrase that is important or memorable to you and turn it into a password that is easy to remember.

Example phrase: There is no place like Nebraska
Example password: tinplike*Ne6r!

NOTE: Do not use this example!

Also, update your passwords on a regular basis, at least annually.

The Microsoft Safety & Security Center offers a password checker tool on its "Create strong passwords" page.

Consider what the password is protecting

- Passwords that protect access to sensitive data, email account(s), or network services at work or home should each be unique and easy to remember.
    - Do NOT use any work-related password for home or personal use.
    - Do NOT use any personal password for work-related resources.
- Passwords used for Web services that only give access to a service, such as reading newspaper articles, may be reused or based on a similar pattern. The University of Chicago IT Services "Good Password Practices" article has an interesting suggestion for creating passwords for these Web service access needs.

> "For less important passwords or passphrases (where applicable), you can use different iterations of the same basic password. For example, the password above, M'sCMh8196wii! could become nM'sCMh8196wii!NYt for a New York Times account "NYt" added after the core and "n" added before for "news". However, the passwords or passphrases protecting your most sensitive information should always be completely different from other passwords or passphrases." (https://itservices.uchicago.edu/services/safecomputing/passwords/; Last Accessed 8/26/14)

Keep your password safe

- For optimum security, do not write down your primary passwords.
- If you must write down passwords, keep them somewhere private such as in a locked drawer. Do not post it on your computer or anywhere around your desk.
- If you store passwords in a file on any device, that file must be encrypted.
- You may also download or purchase special software for password storage. UNL Extension personnel have no recommendation for a specific program; however, individuals have successfully used Password Safe, LastPass, or KeePassX for many years. For information on other software, do a Google search on "password management software."

Protect your password from misuse

You should follow these guidelines to protect your password.

- Do NOT reveal a password to the boss, assistant, or co-worker.
- Do NOT share a password with family members.
- Do NOT talk about a password in front of others.
- Do NOT hint at the format of a password (e.g., "my family name").
- Do NOT reveal a password on questionnaires or security forms.
- Do NOT reveal a password in an unencrypted email message.
- Do NOT use the "autosave" feature in your browser or other software.
- When using public or shared computers, make sure that you do NOT use the "autosave" feature. Also, make sure that you logoff and close the browser.

One source for staying up-to-date on password security issues is the Password Articles page on the Kim Komando site.

If you suspect that an unauthorized person may know one of your passwords protecting sensitive data, change that password immediately!

NOTE: There is no implied or intended endorsement by UNL Extension of any website provided in this list.

Technology for Librarians 101 is offered as part of the Nebraska Broadband Mapping and Planning Initiative, funded through a grant by the U.S. Department of Commerce's National Telecommunications and Information. The Initiative aims to increase broadband adoption and use. For more information, check **http://broadband.nebraska.gov**