Password Security Best Practices

Creating a strong password and changing it frequently is one of the smartest things a user can do to protect themselves when working online.

University System of Maryland

Password Security Best Practices

For many institutions, usernames and domains are generated based on a common formula: for the University System of Maryland Office, first initial and last name, with the domain @usmd.edu.

Because of this, it's really not enough to rely fully on the security systems of the places that you use your password on. Often times, the least important passwords becomes the most important because hackers target those first. Sure, your bank is pretty secure. But if you use the same password in multiple locations, or iterations of the same password, it doesn't matter how secure your bank's security system is. Hackers start with the stupid websites that require a username and password to process web payments, or logins to read the news or comment on forums, or whatever. If the password you used to order a pizza last weekend is the same as the one you use to access your student loans…well, no amount of security is going to stop someone when they know your password already.

University System of Maryland

Bad Password Combinations

Here are some of the most common passwords or password configurations people use, brought to you by LifeHacker.com. If this is you – it's time to change!

- Your partner, child, or pet's name, possibly followed by a 0 or 1 (because they're always making you use a number, aren't they?)
- The last 4 digits of your social security number.
- 123 or 1234 or 123456.
- "password"
- Your city, or college, football team name.
- Date of birth – yours, your partner's or your child's.
- "god"
- "letmein"
- "money"
- "love"

University System of Maryland

Password Encrypted Storage Locker

It is highly recommended that you use a password encryption storage locker similar to LastPass, Keeper or KeePass to help securely generate passwords and store them. Programs like these are great for storing a wide variety of passwords

For more information on LastPass, click here.
For more information on Keeper, click here.
For more information on KeePass, click here.
For more information on 1Password, click here.

Please note: these programs are not supported by University System of Maryland Office or the USM IT and support will only be provided on a best effort basis.

University System of Maryland

Tips for a Strong Password

- **Length.** As computers that process Brute Force attacks (just running different combinations of passwords and usernames repeatedly until they get a result) become more intelligent, length becomes the defining variable in passwords that will take longer to process.
- In conjunction with length, choose a **pass phrase** that means something to you instead of a word, a name, or a title. Turn a phrase into a string of characters that look completely unrelated, but in reality, is easy to remember. For example, "all creatures great and small" would become "acg8@s" or something similar.
- Although it's not the 'rule' for unbreakable passwords anymore, **randomizing your capitalization** and using special characters are still useful and effective in making your password harder to crack.
- **Don't use words that can be found in a dictionary or someone's name**. Password generators can crack these in no time. At the very least, use something slightly off the beaten path.
- Have problems remembering lots of different passwords? Try using an encrypted password utility like LastPass, Keeper and KeePass, or 1Password for Mac OS X and iOS.
- Changing your password often is important too, but not terribly effective if all you do is change the number at the end of a word. Using passphrases instead of passwords means you have to change them less often and are more likely to remember them when you do.
- **Make a note.** Don't write your password down, but if you know you have trouble remembering, slip a piece of paper in your wallet with a clue that's significant only to you.

Want to check the status of your current passwords? Microsoft has a nifty strength-checker here, as well as more articles on how to protect yourself online.

If you have any further questions, concerns or more tips on Password Best Practices, please contact the USM-IT Dept. at geeks@usmd.edu