TIPS FOR USING PASSWORDS TO KEEP YOUR INFORMATION SAFE

TIP: Make your password easy for you to remember, but hard for others to guess.
We've increased the minimum length of the eID password to 15 characters, to make it harder to choose a very bad password like **P@ssw0rd**. We've also removed the necessity to use numerals and special characters (though you can still use those if you desire). Length is much more important than complexity in choosing a good password, so choose something that you'll remember and that's easy to type. Even so, try to choose passwords that can't be easily guessed by anyone who finds your profile on the CSU network or a social media site; **mydogsnameisfido** is a really bad password if many people know that you have a dog named Fido. But, if your first dog was named Fido and he really liked salmon-flavored treats, you might find it very easy to remember the password **fidosalmontreats**.

TIP: Never share your password with anyone - not even your loved ones or co-workers.
While you may trust these people, you shouldn't trust that they know how to keep passwords secure. Never, never respond to a request from any organization (particularly a financial institution) that requires you to submit your login and password by email, since it's probably a hoax.

TIP: Never leave your password written down where someone could find it.
Anyone wandering by your desk and seeing a password on a sticky note could log on to your computer as you, and commit crimes in your name - including copyright violations, child pornography, threats, and fraud. If these are done with your logon, especially from your computer, it becomes difficult to prove it wasn't you!

TIP: Don't use your important passwords in more than one place.
One of the major security problems on the internet today is password re-use. If your password is compromised on one system, then any other system you access with that same password could be compromised. So, if you use your banking password for a YouTube account, it's like an open invitation to have your bank account emptied. Fixing this means keeping track of more passwords, but there are tools to make it easier. For Windows, Mac, and Linux, one of the best is the Open Source tool **PasswordSafe**. There's also a version for iOS (iPhone, iPad).

TIP: Use two-factor authentication if it's offered.
Many financial and email sites are beginning to offer stronger authentication options. PayPal offers a one-time password generator for use with eBay and PayPal. Gmail offers a way to use your smart phone to generate a one-time token. The one-time password approach protects against many password attacks. Every time you log in to your account, the service provides a different string of numbers that you append to your password. So, even if your logon is intercepted on its way across the Internet, it won't do anyone any good because your password will be different the very next time.