**WV Executive Branch Privacy Tip**

# Passwords and Your Privacy



Passwords are the first line of defense against the compromise of your digital information. Revealing the data on your phone, your banking information, your email, your medical records, or other personal information could be devastating. Yet many people fail to follow proper practices when selecting the passwords to protect this important information. Here are some password "dos" and "don'ts" that can help you to maintain the security of your personal data.

**Do** use longer passwords. Passwords become harder to crack with each character that you add, so longer passwords are better than shorter ones. A brute-force attack can easily defeat a short password.

**Do** use special characters, such as $, #, and &. Most passwords are case sensitive, so use a mixture of upper case and lower case letters, as well as numbers. An online password checker can help you determine the strength of your password.

**Don't** "recycle" a password. Password-protected sites are often vulnerable because people often use the same passwords on numerous sites. If your password is breached, your other accounts could be put at risk if you use the same passwords.

**Don't** use personal information (your name, birthday, Social Security number, pet's name, etc.), common sequences, such as numbers or letters in sequential order or repetitive numbers or letters, dictionary words, or "popular" passwords.

**Don't** share your passwords with others. One study found that more than one-third (36%) of people who share passwords in the United States have shared the password to their banking account.

**Do** enable two-factor authentication (when available) for your online accounts. Typically, you will enter your password and then a code will be sent to your phone. You will need to enter the code in addition to your password before you can access the account. Twofactorauth.org has an extensive list of sites and information about whether and how they support two-factor authentication.

**Do** be cautious when you choose the site security questions and answers that will be used to authenticate you if you forget your password. Be sure that you don't pick a question which can be answered by others. Many times, answers to these questions (such as a pet's name or where you went to high school) can be ascertained by others through social networking or other simple research tools.

**Don't** write down your passwords or save them in a computer file or email. Consider a password manager program if you can't remember your passwords. Alternatively, keep a list of passwords in a locked and secure location, such as a safe deposit box.

**Do** take steps to learn more about protecting your online privacy and securing your computer. Feel free to contact PRC if you have questions.



**Note:** Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.