

# THINK PRIVACY

## Monthly Privacy Advice from the NYS Consumer Protection Board

Passwords are the first line of defense in protecting personal information on our computers. However, their value is often misunderstood and underestimated. According to studies, passwords are all too easy to steal. Thus, it is important to follow best practices in the creation of passwords to help safeguard your personal data. Here are ten suggestions to help you create stronger passwords.

1. Do not pick passwords that others can easily guess. Pet names, child's names, birthdays and parts of Social Security numbers are the most common type of passwords used and are the easiest to figure out. As a result, steer clear from the familiar.
2. Be creative. Pick random or strange words or phrases that would be hard for an intruder to guess and easy for you to remember. For example, kids love Elmo. This can be: **KidsLElmo**
3. Use a combination of letters and numbers. For example, Elmo loves my 2 kids. This could be: **ElmoLmy2kids.**
4. Change your password frequently. A good bet is to revise your password every three months.
5. Do not write down your password near your data. Too often passwords are found on a Post-it, on a top of computer screen or inside a desk top drawer.
6. Do not share your password with anyone. It is for your use only.
7. Try to memorize your password. Avoid writing it down and risking it to unwanted exposure.
8. Try to use different passwords for different computing environments. This will help protect you from an intrusion into all of your personal data.
9. Do not let your computer auto-fill or save your passwords. This reduces the chance that your data will be easily compromised in the event of a stolen computer.
10. Use a password protected screensaver. This will reduce the chance that intruders will be able to access your data.

The stronger your passwords, the safer your data will be from intruders, hackers or criminals. The time you spend today in creating solid passwords might indeed save you considerable expense and effort later, if your personal information is compromised.