



PASSWORD ETIQUETTE

Below are some guidelines to consider when protecting your data. Make sure to protect your information by creating a secure password that makes sense to you, but not to others. As a rule of thumb remember: Don't use personal information such as your name, age, birth date, child's name, pet's name, or favorite color/song, etc.

How to make your password secure:

1. Be sure no one watches when you enter your password.
2. Always log off if you leave your device and anyone is around—it only takes a moment for someone to steal or change the password.
3. Avoid entering passwords on computers you don't control (like computers at an Internet café or library)—they may have malware that steals your passwords.
4. Avoid entering passwords when using unsecured Wi-Fi connections (like at the airport or coffee shop)—hackers can intercept your passwords and data over this unsecured connection.
5. Don't tell anyone your password. Your trusted friend now might not be your friend in the future. Keep your passwords safe by keeping them to yourself.
6. Depending on the sensitivity of the information being protected, you should change your passwords periodically, and avoid reusing a password for at least one year.
7. Do use at least eight characters of lowercase and uppercase letters, numbers, and symbols in your password. Remember, the more the merrier.
10. Check your password strength. Strong passwords are easy to remember but hard to guess. This has 10 characters and says "I am happy to be 29!".
11. Use the keyboard as a palette to create shapes. Follow that on the keyboard. It's a V. The letter V starting with any of the top keys. To change these periodically, you can slide them across the keyboard. Use W if you are feeling all crazy.

12. Have fun with known short codes or sentences or phrases. This one says “To be or not to be?”

13. It’s okay to write down your passwords, just keep them away from your computer and mixed in with other numbers and letters so it’s not apparent that it’s a password.

14. You can also write a “tip sheet” which will give you a clue to remember your password, but doesn’t actually contain your password on it. For example, in the example above, your “tip sheet” might read “To be, or not to be?”