INFOARMOR®

DETECTION IS THE NEW PREVENTION

Passwords are digital currency, yet most of us put little thought into creating them. A case in point: the most common passwords of 2015 are “123456” and “password.”

Although there is no sure-fire way to prevent identity fraud, you turn your password from hackable to uncrackable by following these 10 top tips:

1. **Gimme 10.** Create passwords that are at least 10 characters, so they are difficult to break.

2. **Mix it up.** Use numbers, symbols and letters – capital and lowercase – as well as variations on punctuation, spelling and capitalization.

3. **One-of-a-kind.** Designate a unique password for each website.

4. **(Bo_H@s2STNKIEt0e$!)** Make sure passwords do not contain common dictionary words or phrases. Instead, create a random sentence and build a unique password from the initials with a mix of symbols and numbers.

5. **Not so personal.** Never create a password that contains your birthdate, anniversary date, graduation date and other personal dates that may appear on public websites or in social media**.**

6. **Remember the two-step** … as in two-factor authentication to ensure a secure login process. It’s like when you make a transaction at a bank that requires your bankcard and a PIN number. Set up your online passwords in the same way.

7. **Know the code.** Protect mobile phones, iPads and other hand-held devices with passwords.

8. **Free Wi-Fi…or not.** That’s because it could be a gateway to stealing your personal information. Access sensitive accounts using a secure and private Internet connection.

9. **Log off.** Identity thieves may be lurking in public places to steal your password, so be sure to log off of any accounts when using public computers or devices.

10. **Don’t write it down.** A password, that is.