PASSWORD REPORT CARD:

Most people are failing miserably when it comes to password length and complexity. The most common passwords (cleartext, alphanumeric) are all brute forcible in a matter of seconds. This is if they have not already been exposed (unencrypted) in a previous data breach.

So how does your password stand up when it comes to crack-ability?

Check your passwords against this grade sheet, to see whether you would "pass" or "fail" the test.

STOP

- All numbers or lowercase characters (8 or fewer characters)
  - Example: "123456"/ “password"
- Combination of numbers and lowercase characters (8 or fewer characters)
  - Example: "bnn2345"/ "tanner1"
- Combination of numbers, upper and lowercase characters (8 or fewer characters)
  - Example: "doggy!"/ "Washington#1"
- Other considerations:
  - Often harder for an individual to remember.
  - When it comes time to change, most will just iterate; i.e., "Washington#1" becomes "Washington#2"

GO

- Long password phrases
  - Example: "jeansturnipcandytable"
  - Easier to remember and the length of the password makes it harder to crack.
- Long password phrases with a “stop” character, symbol or number
  - Example: "stingycats%makegreatpets"
  - Adequate protection (other than increasing length).
- Password Managers
  - Randomly generated long passwords take the most exploitable element (the human element) out of password creation.

This guide is adapted from articles by ID Agent

DVD NETWORKS

711 Moorefield Park Drive, Suite E, Richmond, Virginia 23236
www.dvdnetworks.com
804.271.6300