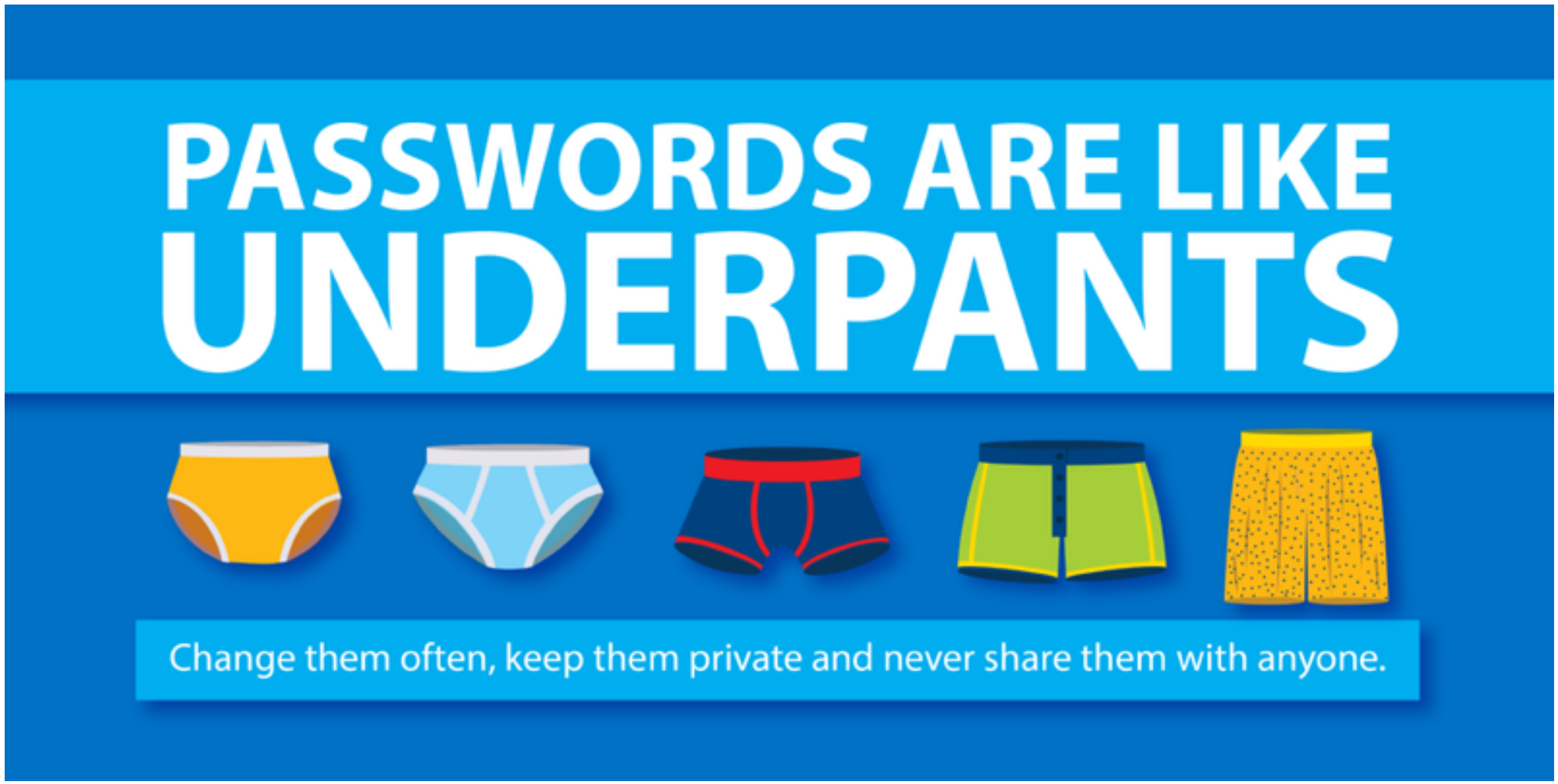
Passwords

12-19-2017



Passwords

- From what you've seen what are the properties of the Vigenere Cipher that make it harder to crack?
- In other words, if you had to crack a Vigenere cipher what would you do?
- Vigenere is strong because looking at the cipher text there are no discernible patterns assuming a good key was chosen.
- Because the ciphertext is resistant to analysis it leaves us simply having to guess what the key is.
- Even if we know the length of the key we might still have to try every possible letter combination which is a prohibitively large number of possibilities.

Passwords

- For a long time, the Vigenère cipher was considered to be an unbreakable cipher and was used by governments to send important messages.

- But in the 1800s Vigenere was discovered to be susceptible to a modified form of frequency analysis. After that point it was considered insecure.

- Still the properties of Vigenere that we've found are desirable.

How good is your password?

- We know that a good encryption algorithm reduces the problem of cracking it to simply guessing the key.

- We want the key to be Computationally Hard to guess - in other words, hard for a computer to guess.

- Computationally Hard typically means that arriving at the solution would take a computer a prohibitively long time - as in: centuries or eons.

- In terms of cracking encryption that means that the number of possible keys must be so large, that even a computer trying billions of possible keys per second is unlikely to arrive at the correct key in a reasonable amount of time.

- Nowadays when you use a password for a website or device, your password is used as a cryptographic key.

- So, choosing a good password is meaningful because we want the key to be hard for a computer to guess. How good is your password?...

howsecureismypassword.net

Take a few moments to check out some of your commonly used passwords

Try typing common words from the dictionary or well-known names like “Apple” or “Chicago”

Try typing something that’s over 16 characters

Try a string of 4 random words together, like AppleChicagoBalletTree

Type a 0. Then keep typing 0s and watch what happens to the statistics. (Actually, you might want to just hold 0 down for a while.)

HOMEWORK

The AP CS Principles framework contains the following statement: Implementing cybersecurity has software, hardware, and human components. Based on what you've learned so far, describe at least one way that cybersecurity involves "human components."

Please send me your response with *p8 in the subject line