

The Week@eSt# Link in the Chain

*How to Avoid Our Biggest Mistakes
When It Comes to Protecting Assets in
Cyberspace*

*Jill Horner, TAACCCT Grant Coordinator - Cybersecurity
Garrett College
jill.horner@garrettcollege.edu*



Despite the increasing media attention that global cyber attacks have been getting lately, it seems that cybersecurity is STILL not the vitally important issue that it should be for internet users. As a group we are preserving old habits that are supporting the ability of cyber criminals to exploit and fuel the malware economy.

- **Malware:** short for “malicious software” is a general term for computer programs designed to infiltrate and damage computers without the user’s consent. It covers all the different types of threats to your computer safety such as viruses, spyware, worms, Trojans, rootkits and the like.

* It is critical to protect your information from contact with malware, but
HOW?



27 Cybersecurity Experts *from organizations such as Symantec, AVG, Bitdefender, ESET, Malwarebytes, Sucuri, Rackspace, Trustee (IBM Security)* and other security organizations and publications were recently polled to find out what they feel are our **MOST PROBLEMATIC BAD HABITS** in cyberspace---

- Virtually (*no pun intended...okay, maybe a little bit intended...*) **every one** of them agreed that all of the worst problems had one **COMMON THEME.....**

**YOUR
PASSWORD
SYSTEM IS A BIG
PROBLEM**



CREATING STRONG P@SSWORDS and keeping them PROTECTED (in a nutshell)



- Make passwords 8-12 characters in length
- Combine lower case, upper case, numbers & special characters
- Avoid words which can be found in a dictionary
- Do not use one of these common passwords or any variation of them: qwerty1, abc123, letmein, password1, iloveyou1, (yourname1), baseball1
- Avoid names and birthdays of loved ones or other easy to guess personal information
- Create a phrase and use parts of it along with numbers and/or special characters.

EX: **My Memory Is Like Swiss Cheese** could be: **M*m=0S-c**

Want To Retire In The South Of France could be: **w2R6i8S_7f**


- If you must write it down, keep it in a safe and secure place
- Don't use the same passwords for different online accounts
- Do **NOT** tell anyone your passwords!
- Store passwords in a safe place. Consider using KeePass Password Safe (<http://keepass.info/>), Keychain (Mac) or an encrypted USB drive to store passwords. Avoid keeping passwords on a Post-it under your keyboard, on your monitor or in a drawer near your computer!

- A. 123456
- B. Asdf
- C. Iloveyou
- D. Monkey

- A. 123456
- B. Asdf
- C. Iloveyou
- D. Monkey

A. 123456



- According to recent analysis **123456 is the most commonly used** password. However, all of the worst password choices appear on Twitter's recent list of 370 banned passwords and should be avoided at all costs!
- Common passwords are amongst the first passwords to be cracked when under attack.
- A **Brute Force Attack** is a trial and error method use by application programs to decode encrypted data such as passwords through exhaustive effort ("brute force") rather than employing intellectual strategies. 

Splash Data's Ten **WORST** Passwords of 2015



2014 Status

1.	123456	unchanged
2.	password	unchanged
3.	12345678	#4
4.	qwerty	#5
5.	12345	#3
6.	123456789	unchanged
7.	football	#10
8.	1234	#7
9.	1234567	#11
10.	baseball	#8



2. Ideally, what **characters** should you use in a password to make it **strong**?

- A. Letters and Numbers only
- B. Mixed Case (Upper and Lower) Characters
- C. Special Characters
- D. All of the above

D. All of the Above

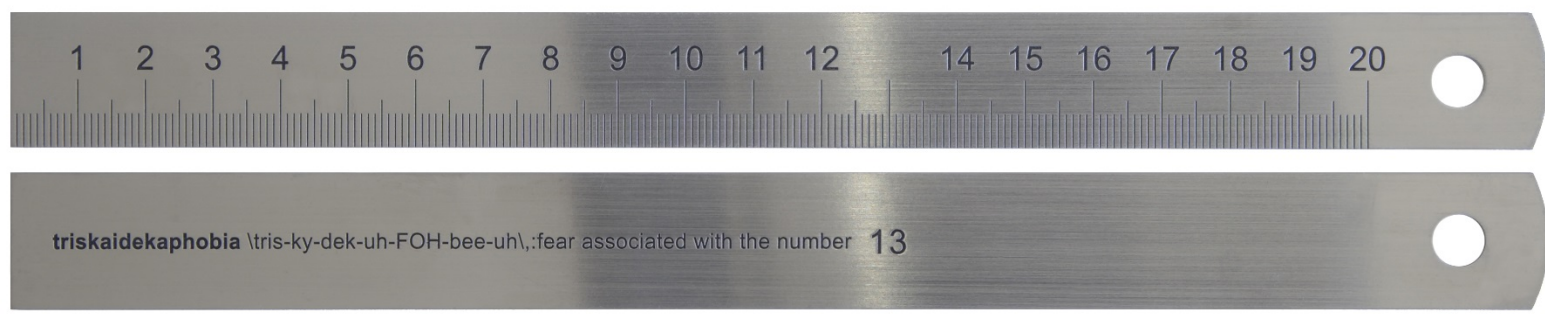


When permitted your password should be made as **complex** as possible without rendering it impossible to memorize.

EX: The easily remembered password *ilovecookies* can be made more secure:

- * by adding **more characters**: *iyumlovemmmmcookiesyum*
- * by changing the **character case**: *iYuMloveMMMMcookiesYuM*
- * by introducing **special characters**: *YuMl()veMM@MMc()()kiesYuM*
- * and **numbers**: *iYuMl(17)veMM@MMc(18)(19)kiesYuM*

Some systems and applications won't let you create passwords over a certain length or accept mixed case or special characters. Familiarize yourself with the applications password policy to enable you to create the strongest possible password, using these techniques.



3. How **long** should a strong password be?

- A. 8 characters
- B. 15 characters
- C. As long as possible
- D. It doesn't matter

C. As long as possible



Contrary to popular belief, a lengthy password can be as secure, if not more, than a complex password.

A **lengthy** password should be used to increase the amount of time it could take to crack; however, **complexity** should also be used so the password is not easily guessed.

i.e. it would be easy to infer the password

*jingle*jingle*jingle*theway* is modified from

jinglebellsjinglebellsjinglealltheway (which may prove easy to

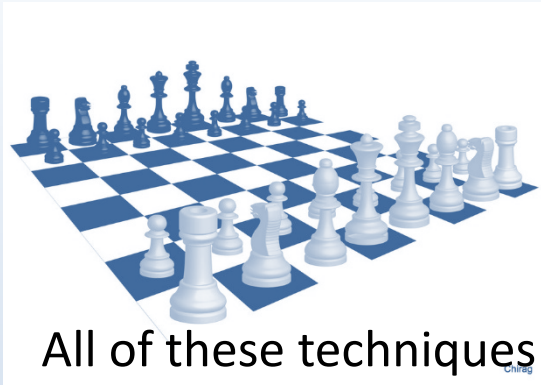
guess), whereas the password *jingle@jingleBeLlSjingleA!!theway*

will prove difficult, if not impossible, to crack using traditional methods.



4. Strong passwords can be difficult to **remember**, what can you do to avoid forgetting them?

- A. Use **mnemonics** (acronyms or phrases that are easy for you to remember), or some other password strategy
- B. Use a **password strategy**
- C. Use **password management software** with encryption
- D. All of the above
- E. Carry a **book** named “Passwords” with you everywhere think you might need to access a secured website.



D. All of the above



All of these techniques can be used to create a strong password.

Mnemonics can be used to make your password easy to remember (e.g. condense a phrase or a joke into a string of letters, add numbers and symbols, etc.)

A **password strategy** can be developed to help you remember your passwords-- i.e. substitute letters for special characters, incorporate elements unique to the system or service into your password, or develop a pattern such as using memorable lyrics from meaningful songs. Ensure your password is complex and to some extent random to avoid them being guessed if your password strategy is found out, or one or more of your passwords created using your strategy is compromised.

Encrypted password management software can be used to manage your passwords if you have a particularly poor memory. However, be aware that these programs are often targeted by intruders. They are also rendered useless if a weak '**master password**' is used to gain access to all other passwords.



5. I have a really ***strong*** password so I should be able to use it for **YEARS**.

True or False?

- A. True
- B. False

B. False



The longer you use a password the longer malicious users have to guess or crack your password.

PERIOD



6. When it's ***TIME TO CHANGE*** your password, what's the best way to choose a new one?

- A. Add a number or special character to the **end** of your old password
- B. Pick something easy to remember such as your favorite football **team** or your **birthday**
- C. Choose something quick and **easy** to type in so nobody can see it
- D. Choose something you can remember, but modify it with a **complex pattern** that only you know

D. Choose something you can remember, but modify it with a complex pattern that only YOU know.



Use a ***password strategy*** to create a memorable, **unique** password.

(Try not to fall asleep, this is sounding a bit repetitive for a good reason)





*I hope they
remember...*



...remember

7. “**Remember Me**” functions in Web browsers or other applications are unsafe and should be avoided. True or False?

- A. True
- B. False

A. True



If you save your password on a **public computer** the next person to use that computer may access your accounts. This might also apply to your home computer or laptop; if curious **fill in the blank** (siblings, parents, children, roommates) have access to your machine they ~~may~~ will be tempted to log into your accounts.

NEVER save username and password details on your smart phone, within messages or your web browser-- if it gets lost or stolen someone could compromise ***all*** of your online accounts.



8. “***Password Reminder***” functions in applications are ***unsafe*** and should be avoided. True or False?

- A. True
- B. False

B. False



Password **hints and reminders** can help to jog your memory and help to avoid creating another password.

If you can create your own **password hint** make sure it only makes sense to you. It should **NEVER** contain your password. 🙄

If you use a service with preset questions i.e. "What was the name of your first pet?" try to make your answers humorous and **abstract**, e.g. use an 'inside joke', or your personal nickname for your little brothers nickname. This will ensure it is both memorable and not easily guessed. **DO NOT USE YOUR MOTHER'S MAIDEN NAME**—do you know how many people are on **ancestry.com**??



9. ***How long*** would it take an attacker to crack a **10-character** password?

- A. Less than an hour
- B. Less than a week
- C. Less than a month
- D. It depends....

D. It depends...



There are **variables other than length** that determine how quickly a password can be cracked. The types of characters used, whether or not the password is based on a common word or phrase, and the ***amount of resources*** available to the attacker drastically affect the time required. That is why it is important to regularly change your passwords in order to minimize the time a cracked password can be used.

For grins and giggles, check out <https://www.grc.com/haystack.htm> -- the interactive Brute Force Password Search Space Calculator



6 characters: 2.25 billion possible combinations

Cracking online using web app hitting a target site with one thousand guesses per second: 3.7 weeks.

Cracking offline using high-powered servers or desktops (one hundred billion guesses/second): 0.0224 seconds

Cracking offline, using massively parallel multiprocessing clusters or grid (one hundred trillion guesses per second: 0.0000224 seconds

10 characters: 3.76 quadrillion possible combinations

Cracking online using web app hitting a target site with one thousand guesses per second: 3.7 weeks.

Cracking offline using high-powered servers or desktops (one hundred billion guesses/second): 10.45 hours

Cracking offline, using massively parallel multiprocessing clusters or grid (one hundred trillion guesses per second: 37.61 seconds.

Add a symbol, make the crack several orders of magnitude more difficult...!

6 characters: 7.6 trillion possible combinations

Cracking online using web app hitting a target site with one thousand guesses per second: 2.4 centuries.

Cracking offline using high-powered servers or desktops (one hundred billion guesses/second): 1.26 minutes

Cracking offline, using massively parallel multiprocessing clusters or grid (one hundred trillion guesses per second: 0.0756 seconds

10 characters: Possible combinations: 171.3 sextillion (171,269,557,687,901,638,419; 1.71×10^{20})

Cracking online using web app hitting a target site with one thousand guesses per second: 54.46 million centuries.

Cracking offline using high-powered servers or desktops (one hundred billion guesses/second) 54.46 years

Cracking offline, using massively parallel multiprocessing clusters or grid (one hundred trillion guesses per second: 2.83 weeks.



10. Now that you are an **expert**, choose the strongest password from this list:

- A. Monkey2
- B. M0nk3y1
- C. ThEM(12)nkEy~Eats@BanEnahs
- D. TH3 m0nk3y 3475 b4n4n4s



C. ThEM(12)nkEy~Eats@BanEnahs



Taking a memorable phrase and using a **mixture of special characters**, **alternate spellings**, and **varying cases** (upper and lower case letters) in a memorable way is an effective way of creating a strong password.

Although it may look complicated, substituting numbers for letters in dictionary words, known as ***L33t Sp34k*** ("***leetspeak***") is one of the first things password crackers look for!

NOTE: Using a capital letter at the beginning of a password and a number at the end is one of the most common patterns used in password creation and it is no match for password cracking software!

Congratulations, you're ready to face the new frontier!



This workforce product was funded by grant #TC-26466-14-60-A-24, awarded by the U.S. Department of Labor's Employment and Training Administration. The product was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The U.S. Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability, or ownership.