



Password Security

A Simple Way to Create Passwords That You Can Remember

Password Security

If you are using the same identical password for everything, that's not good. **Period.**

We humans, are creatures of habit. When it comes to password security .. that's a bad thing.

How bad can it be?



Password Breaches



- **U.S. Department of Justice** [Feb-2016]: **10,000** Homeland Security employees, followed by **20,000** FBI employees.
- **IRS** [*Revised* May-2015]: 700,000 personal taxpayer information.
- **Premier Healthcare** [Mar-2016]: **200,000** patients; Most victims affected had their names, DOB & basic information stolen. However **1,769** individuals may have had their SSN and/or financial information also stolen.
- **LinkedIn** [*Revised* May-2016]: For those of the **117,000,000** who failed to update their passwords from the 2012 breach, that information was released by hackers in May of 2016.

Password Breaches



- **Dropbox** [*Revised Sep-2016*]: More than originally thought compromised in the 2012 breach, in September of 2016 Dropbox announced that **68,000,000 accounts** had been compromised.
- **Yahoo** [*Revised Sep-2016*]: Hackers had stolen information from a minimum of **500 million** accounts in late 2014, including e-mail addresses, passwords, full user names, dates of birth, telephone numbers, and in some cases, security questions and answers.
- **Yahoo** [*Revised Dec-2016*]: Discovery of another breach in 2013 affecting **1 billion** users.

What Would Happen If?



Someone had your email password?

- Ever use the “Forgot my Password” link on a website? Someone with access to your email account, now can change your password essentially locking you out.

Think about it ...

Worst Passwords of 2015



- 123456
- password
- 12345678
- qwerty
- 12345
- 123456789
- football
- 1234
- 1234567
- baseball
- welcome
- 1234567890
- abc123
- 111111
- 1qaz2wsx
- dragon
- master
- monkey
- letmein
- login
- princess
- qwertyuiop
- solo
- password
- starwars

Password Creation Tips



- Avoid using full words and names. Hackers regularly use “dictionary attacks” to guess passwords.
- Create passwords with 12+ characters using a mix of upper and lowercase, along with numbers and symbols.
- **Use a different password for each website you log into.**

Let's make that easy .. and easy to remember.

Password Creation in 5 Steps



Step One

Pick a two word phrase (no names) and your “lucky number.” Using a phrase you use often, makes it all that much easier.

Example:

Dream Big (and Lucky Number 74)

Password Creation in 5 Steps



Step Two

Create a “street” version combining the two words using capital letters.

- The letter “i” (or “l”) becomes 1 or !
- The letter “s” becomes \$
- The letter “o” becomes 0 (a zero)
- The letter “e” becomes 3, and so on.

Example:

Dr3amB1g

Password Creation in 5 Steps



Step Three

- Add in your lucky number with a pair of symbols around it.

Example:

Dr3amB1g<74>

Password Creation in 5 Steps



Step Four

- Add in 2 (or more) characters from the site you are creating this password for.
- **Ex #1:** For sites where the site name is two or more words, like Facebook, LinkedIn, FoxNews, etc. then those 2 characters are both caps.

Example:

Dr3amB1g<74>LI

Password Creation in 5 Steps



Step Four

- Add in 2 (or more) characters from the site you are creating this password for.
 - **Ex #2:** If the site is one name, like **T**witter, then use one cap, one lowercase.

Example:

Dr3amB1g<74>Tw

Password Creation in 5 Steps



Step Four

- Add in 2 (or more) characters from the site you are creating this password for.
 - **Ex #3:** For sites with common initials (ex. **F**acebook and **F**resh**B**ooks), or if the site has a short name (ex. Asana), then spell out the site name.

Example:

Dr3amB1g<74>Amazon

Dr3amB1g<74>B3\$+Buy

Password Creation in 5 Steps



Step Four and a Half

- Some sites don't allow special characters, so **have a backup plan!**
- Some sites limit the password length .. again, have a backup plan.

Example:

Dr3amB1g74Expedia

Dr3amB1g74Amz

Password Creation in 5 Steps



Step Five

- Mix it up! Place your lucky number wherever you'd like. There's no real reason to follow a [phrase][symbol][lucky number][symbol][2 characters] pattern. Some examples would be:
 - Dr3am<74>B1gFB
 - FB<21>Dr3amB1g
- **Tip:** Most sites will **not** allow a special character to be the 1st character in your password.

Password updates



When to change your password?

- Don't wait until you receive a “we've been hacked” email from a website. Be pro-active!
- Change your passwords **every 6 months**, especially your email accounts, any financial sites (online banking), and any site where you make online payments (credit cards, utilities, etc.).
 - **Tip:** If you are having a hard time updating passwords, then add the year and month:
 - Dr3amB1g<74>B3\$tBuy_2017Jan
 - Dr3amB1g<74>B3\$tBuy_20170101

Add an Additional Layer of Protection



If you are using multiple devices (computer, mobile phone, tablet, etc.), you may want to consider Two-factor authentication (2FA) or Multi-factor authentication (MFA).

A good example from everyday life is the withdrawing of money from a cash machine; only the correct combination of a bank card (something that the user possesses) and a PIN (personal identification number, something that the user knows) allows the transaction to be carried out.

Many sites and SaaS products offer 2FA .. so consider it.

Get a Password Manager



Finally, consider a password manager such as [LastPass](#) or Intel's [True Key](#).

- LastPass allows users to share passwords, without the recipient being able to actually “see” the password.
- True Key allows login via fingerprint, facial recognition, or a traditional password.

Contact Details

Out of the Office Virtual Assistance

Denise Dukette

96 S. Water Street, Vergennes, VT 05491

o: 800 667 1690 x201 | m: 802 870 0829

denise@oofva.com | www.oofva.com

