Password / Passphrase Guidance

VERSION CONTROL

Date	Author	Version	Amendments
16/12/2016	Tony Unger	V0.1	Draft
16/12/2016	Tony Unger	V0.2	Updated with bookmarks
20/01/2017	Tony Unger	V0.3	Updated with summary page
22/01/2017	Tony Unger	V0.4	Updated format, page numbers, layout
03/09/2019	Tony Unger	V0.4	Reviewed, no changes
23/11/2020	Tony Unger	V0.5	Reviewed, removed, added and updated content.
03/08/21	Richard Best	V0.6	15 character password change
13/10/22	David Smith	V0.7	Reviewed, no changes

--- IMPORTANT SECTION PLEASE READ ---

Summary

Organisations are increasingly becoming the victims of data hacks and breaches. Since many people use the same credentials for multiple accounts, we want to ensure IET accounts and data are secured with strong passwords and remain protected.

This article provides tips on how to choose good passwords or passphrases in line with the IET policy and keep them safe.

Whilst it is always important to use strong passwords, the best advice is to enable a 2nd authentication mechanism where possible, commonly known as Multi Factor Authentication (MFA). This prevents anyone but you from using your account to log in to websites, even if they know your password or passphrase. Nowadays, passwords alone are not considered an effective solution for securing accounts.

Passwords and passphrases are used to access many online services, such as email, credit card and bank accounts, eCommerce sites like Amazon, and social networking sites like Facebook and Twitter. It is important to choose good passwords or passphrases to make sure no one gets access to your private information. Here are some tips on how to create secure passwords and passphrases and how to keep them secure.

Note that the passphrase is an alternative to the password and functions identically to a password by authenticating you for all the common services you are eligible to use based on your affiliation with The IET.

If you struggle with creating and remembering a complex password, an equally good option is to use a passphrase instead. Passphrases are simple sentences that use length instead of complexity to make them secure. Passphrases at the IET must be at least fifteen (15) characters. For more on passphrases, see the section contained in this article called “Choosing good passphrases”

Passwords and passphrases at the IET must be:

- A minimum length of at least 15 characters
- A mixture of upper and lower case letters, numbers, and punctuation
- Must not have been used previously
- Must not contain your first name, last name, username

Note: IET passwords and passphrases should NEVER be used for any services or applications outside of the IET.

--- IMPORTANT SECTION COMPLETE ---

--- Read on for further information ---

Sections within this document:

Introduction

This article provides tips on how to choose good passwords or passphrases and keep them safe.

Choosing Good Passwords

Secure passwords at the IET must have at least fifteen (15) characters and combine letters, numbers, and symbols. Choose passwords that are memorable, but not easily guessed.

Below are some tips for choosing good passwords.

Do;

- ***Use a long password of at least 15 characters***

  The longer and more complex your password is, the harder it is to crack.

- ***Use multiple character sets***

  Use a mixture of upper and lower case letters, numbers, and punctuation such as !, @, #, etc. Try to use at least three (3) out of the four (4) character sets available on your keyboard (e.g., KK, nn, 123, !@#). However, avoid using characters that don't appear on a standard keyboard, as they may not work correctly in all circumstances.

- ***Select something unique or specific only to you.***

  For example, the passphrase:

  DavidHasselhof@RollingStones!

  Could be a list of posters you have hanging on the walls of your office, home, dorm room, etc. This is a good passphrase because it's easy to remember (memorable to you) because you know what the category is ("posters I have hanging in my office going from left to right), it's long (29 characters), it has unexpected characters (the "@" symbol" and the "!"), and it's unique or specific only to you ("wall posters I have for things I like or am interested in"). To anyone else this list might seem strange and arbitrary, but you are unlikely to forget it (because these are *your* posters in *your* office).

- ***Combine a few pronounceable "nonsense" words with punctuation***

  For example nuit+Pog=tWi. Pronounceable nonsense words are easier to remember than random characters.

- ***Use letters chosen from words in a phrase or song lyric***

  Think up a phrase. For example, "Marx's Communist Manifesto has 8196 words in it!". You can use that as your passphrase, or choose the first letter from each word. "Marx's Communist Manifesto has 8196 words in it!" You'll notice that in this example we've decided to include all the punctuation to improve the quality of the password. So, your password would be M'sCMh8196wii!. It is a nice, long password with a good mixture of character classes.

Don’t;

- ***Don’t use dictionary words or names in any form in passwords***

  Dictionary words are any common words, names, dates, or numbers. Don't assume that this is limited to English dictionaries: if you can find it in the dictionary of any language (even fictional ones, such as Klingon), don't use it! One standard method for cracking passwords is a brute force attack, in which the attacker tries possible passwords over and over again. They try passwords in all sorts of languages using dictionaries of common words and names.

- ***Don't use common misspellings of dictionary words either***

  Many of the dictionaries include both common misspellings and words with letters replaced with similar looking numbers (e.g. replacing “l” with “1”). You should also avoid simply adding a numeral to the beginning or end of a word.

- ***Don't use the name of the computer or your account***

  Since these can be found out, these passwords can be very easy to guess.

- ***Don't use sample passwords***

  Obviously, if the password appears in a document such as this for the whole world to see, don't use it.

Choosing Good Passphrases

Secure passphrases at The IET must be at least fifteen (15) characters in length, and these characters include punctuation and spaces between words or letters. Note that the criteria for what constitutes a good password and what constitutes a good passphrase differ. Unlike a password, for example, passphrases obviously need at least some dictionary words to function as they are intended to.

Below are some tips for choosing good passphrases.

Do;

- ***Select something memorable to you***

  Part of the reason someone might choose to use a passphrase instead of a password is because he or she finds a passphrase to be more memorable. Examples include a favourite childhood memory, favourite foods, places you've visited, experiences you've had, etc., or some combo of these things. For example, "space camp MashedPotatoes4!" (a favourite childhood memory and favourite food) is a particularly strong passphrase. While a hacker may try any of these words individually, only *you* know *all* the words and characters in this specific combination that form your passphrase.

- ***Add unexpected characters***

  Consider adding additional (unexpected) characters that only you know. So, for example "space camp" and "mashed potatoes"--your favourite childhood memory and favourite food--becomes "space camp MashedPotatoes4!"

  Adding other characters such as symbols, numbers, and capital letters increases the complexity of your passphrase and makes it more difficult for hackers to crack.

- ***Use a long passphrase***

  Since passphrases rely on length instead of complexity (like passwords do) for security, the longer your passphrase is, the harder it is to crack. Note that creating a longer passphrase--which includes spaces and punctuation--is easier than you might think. As noted earlier, a passphrase of, "space camp MashedPotatoes4!" is memorable and hard to crack because it's long (29 characters).

Don’t;

- ***Do not choose famous or well-known lyrics/lines/etc.***

  While lines taken from the U.S. National Anthem, for example, might seem like a good passphrase, these lines are widely-recognized and famous, so in practice they make bad passphrases that are easy to crack. If you like the idea of basing your passphrases on a favourite book, song, movie or play, etc. consider taking a passphrase from a book, movie, play, etc. that is meaningful to you and not very well-known. Do not use anything that could be easily found in a book of quotations, an online quotation compiler, or can be found easily by Google.

  If you must choose an (obscure) passphrase from a favourite book, movie, play, etc., you should add unexpected characters like numbers and symbols,

and consider abbreviating it or changing it so only you know the "code". For example, "To be or not to be/that is the question" would become "tB or not TB/titq7!"

A good passphrase will, in general, not be a quote but a seemingly nonsensical list of items (like "space camp MashedPotatoes4!") memorable, meaningful, and unique only to you.

- ***Do not use reuse a word or phrase if your account or passphrase has been compromised***

  For example, if your first passphrase was "spacecamp MashedPotatoes4!" do not reuse any of these words in your next passphrase, and never "create" a new passphrase by re-using an old passphrase but adding in new words or characters: for example, "spacecamp MashedPotatoes Hi5!" Hackers will easily be able to crack this.

Other examples

Below are some other examples of good passphrases and why they are good passphrases:

"Zelda Katamari MGS3#"	These are all video games. Lists of various categories, such as favourite items (food, games, books, etc.) can make good passphrases, so long as that information is *not* easily available online (on your Facebook, in your email, or on other social media accounts) or can be easily guessed by someone (everyone knows you love all the Harry Potter books, and there's a picture of you on Google images at a Harry Potter convention, for example)
"Fido&Mr.Kitty&Bandit"	A list of all your childhood pets' names is very easy to remember (memorable to you), contains unexpected characters ("&"), long (42 characters), and is unique to you; it's something that only you--in this specific order--would know.
"Bullriding at a Taxidermy Convention?!"	Funny and unique, and so easy for you to remember (memorable to you), long, contain uppercase and lowercase letters, and contain an unexpected character "?!"

The point of all these examples is that there is flexibility in choosing a passphrase: not all examples will be equally memorable to you, even if they're information only

you know. For some people, a list of items they love with unexpected characters thrown in will be a perfectly easy passphrase for them to create and remember; other people may need spaces between words or a funny phrase to help them create and remember a passphrase. In other words, you may have trouble remembering "Zelda Katamari MGS3#" but not "Bullriding at a Taxidermy Convention?!" Allowing for the principles listed in this document, what makes a good passphrase depends partly on you.

Smart Computing with Passwords and Passphrases

Don't use the same password or passphrase for all your accounts

Using the same password or passphrase (where applicable) for multiple services is very dangerous because if it is stolen from one service, hackers can use it to access all your other accounts. While having a completely different password/passphrase for each service you use is impractical, you can consider what the password or passphrase is protecting when choosing a password/passphrase. Some services may not require as secure a password or passphrase if they do not contain any private information. If you are unsure, always opt to use a different password or passphrase. Consider using a password or passphrase manager, such as Password Safe or LastPass to help manage multiple passwords/passphrases.

Never share your password or passphrase

Never give out your password or passphrase. Requests for your password or passphrase and other private information are phishing scams. IET administrators or reputable companies, such as your bank or credit card company will *never* request this kind of information through email, fax, or phone.

Don't even share your passwords with friends or family members. Under no circumstance give them your IET password or passphrase to gain access to any IET service.

Your password/passphrase is like your signature; giving it out to others amounts to giving them the authority to sign your name, which makes you responsible for all activities associated with your account.

Use non-secure networks with care

As a convenience, hotels, restaurants, and businesses often offer public internet access. Please use this access with care, and avoid accessing confidential information, such as financial data using these networks. Hackers often target these networks to obtain confidential information for financial gain. Whenever possible, use the IET VPN to carry out work related business, as an added layer of protection.

Don't store your password or passphrase within web browser applications

Many web browsers and email clients offer to store your password or passphrases. This is not good practice and should be avoided. Never store passwords or passphrases associated with important services, such as financial accounts.

Computer viruses and spyware programs can easily retrieve stored passwords or passphrases from these accounts. They may even be able to distribute your passwords or passphrases before you notice that anything is wrong.

Never use information in a password or passphrase which can be found online.

For example, the names of the street you grew up on, your Harry Potter blog, the states you lived in, your obsession with making homemade canned goods on Pinterest, your likes on Facebook, and relatives' names can all be easily found online, and some websites are devoted solely to compiling biographical information about you.

Avoid written copies of your passwords or passphrase safely

If you feel the need to write down your password or passphrase or access it from a written source, in the first instance you probably need to rethink and create a more memorable example.

If however, you absolutely have to write down, consider leaving out some of the easily remembered characters and insert them when typing them in and store securely. Destroy the written format once you have memorized the passwords or passphrases.

Here are some tips for safely storing a hard copy of your password:

- Never write down the name of the service the password is for. E.g., if the password is for an Adobe application, do not write "Adobe: spacecamp MashedPotatoes4!" on a sheet of paper--no matter how safe you think that sheet of paper is.
- Leave some characters out. Instead of writing "spacecamp MashedPotatoes4!" write down an abbreviated form that only you'll understand. E.g., "sc MP4!"
- Store the partial password or hint in your locked mobile phone rather than a piece of paper

Enhanced Password Protection (Multi Factor Authentication)

To strengthen your account security, the IET security team strongly encourages users to consider opting in to Multi Factor Authentication (MFA) wherever possible. Multi Factor Authentication enhances the security of your accounts by using your phone, tablet or other device to verify that you are really you when you attempt to access applications and services. Normally this will be in the form of a unique code sent to your phone or email address which is required to gain access in addition to username & password credentials. This prevents anyone but you from using your account to log in to websites, even if they know your password or passphrase. Many online services such as banks and email providers already offer such schemes as a layer of additional security verification. It is best practice to make use of such security enhancements where available. The IET offers Multi Factor Authentication for several of our online services and will be expanding coverage going forward.

Should you have any queries or feedback regarding the above information, please contact the IET Information Security team.