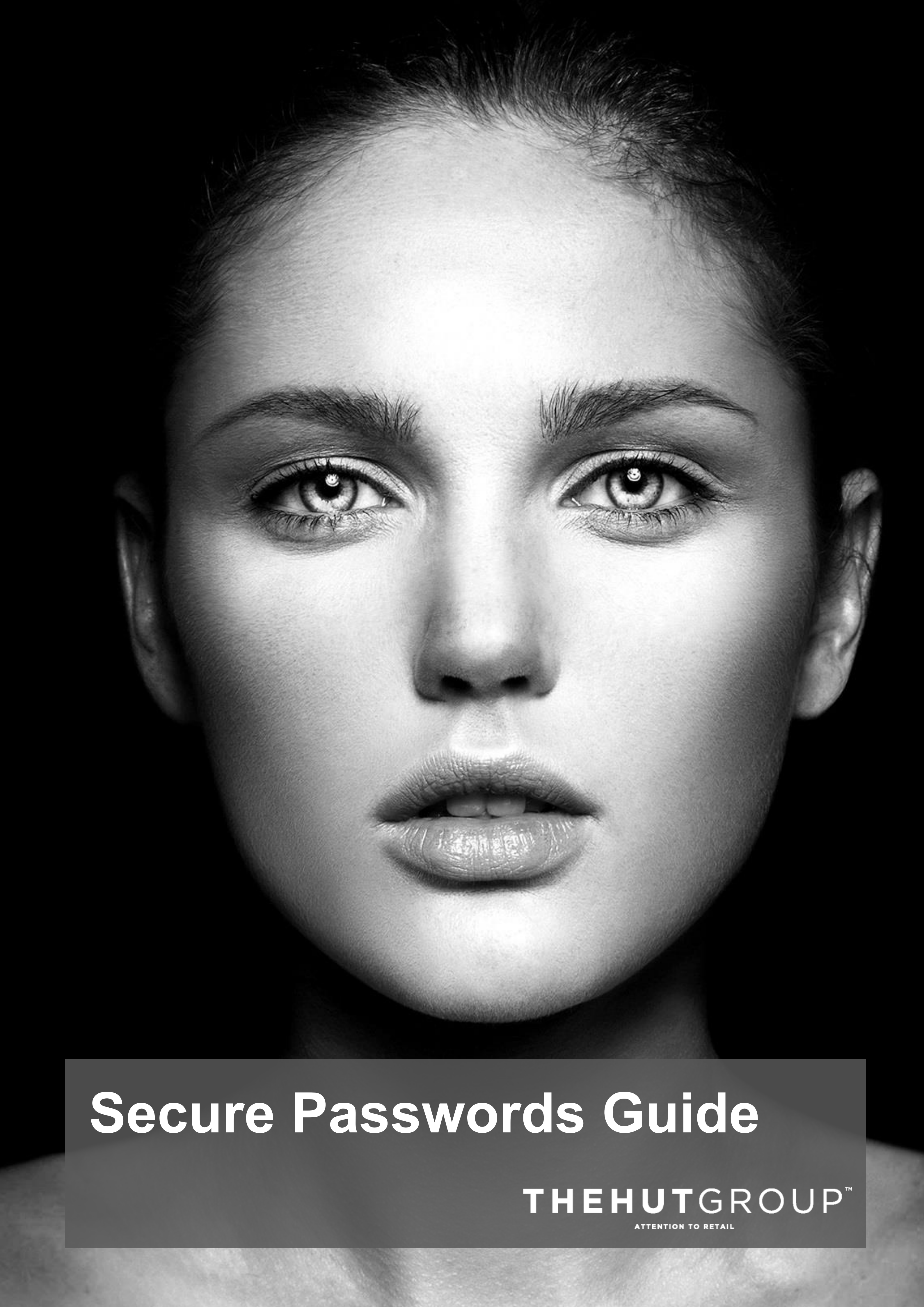


Secure Passwords Guide

THEHUTGROUP™
ATTENTION TO RETAIL

Version: v1.0
Effective: Live
Owner: Graham Thomson, Chief Information Security Officer

Version History:

Version	Author	Description	Reason for Amendment	Date	Next review
1.0	Peter Stanfield	Live	Made live, & referenced on wiki	29/02/2016	01/01/2017

Contents

1. Introduction

This guide will provide you information on why you should have secure passwords, how you can create and use strong passwords, and some advice on how to protect your passwords.

In day to day life we all have a large collection of passwords to remember. We need one for each of our email accounts, banking sites, shopping sites, various social media applications… the list goes on and on. Then you come in to work and we expect you to remember even more!

Well this guide will help you in creating and managing your collection of passwords and try to help you understand a bit more about how strong the ones you choose are.

2. What is a password or passphrase?

A password/passphrase is the thing that proves that you are you and prevents other people impersonating you. The stronger you make your password the less chance a malicious person can guess it, and by changing your password regularly you can keep them guessing for even longer.

3. Why should I use strong passwords?

A very high percentage of security incidents, including those affecting normal people in everyday life, are caused by weak passwords. Why is it so high? This is because a lot of people don't understand how easy it is to guess or hack a password. Hackers use several methods to break in to accounts such as:

Dictionary attack: Using a programme loaded with all the words in a dictionary, this is not limited to the oxford dictionary or similar, it can be a custom made dictionary that contains the worst 100 passwords of 2015, even all the characters & locations from the Star Wars franchise. The hacker will systematically try key words hoping to guess correctly your password.

Brute force attack: This uses a programme to run through a large combination of possibilities starting with something like, a, A, aa, aA, Aa, AA, using a computer program a hacker can test over one million passwords a second. If you have only a small number of characters in your password they will have it guessed before you can blink.

Recon attack: This is more sophisticated and time consuming but you'd be surprised how often it works. This is where a hacker will research its target, checking on social media or via background checks, to find out your family names, mum's maiden name, your birthday, your pets name, favourite tv show, hobby etc. And then uses this information to just guess your password.

To combat these possible attacks remember these six simple things when creating a new password;

- **DO NOT** use a single word easily found in the dictionary
- **DO NOT** use swearing, curse words or common slang
- **DO NOT** use simple combinations like 12345, 12345678, qwerty, abcdefgh, or in fact anything that is in the top 20 common password list (a list produced from hacked password databases) which is shown at Annex A:
- **DO NOT** use names of family members or pets
- **DO NOT** use information personal to you
- **DO NOT** use the previous password but with a new number at the end

4. How do I create a strong password?

Passwords can be made up of any combination of four types of characters and our company policy is that you must choose at least eight characters and use at least three of the four character types:

- lowercase letters,
- CAPITAL letters,
- numerals,
- special characters, this means characters like "%/+$[?£,

If you use a complex password of eight characters long there are over 6.5 quadrillion possible combinations. But the longer the better; in fact a twelve character password (or 'passphrase') is almost impossible to crack, even with sophisticated software.

There are a few clever techniques to creating better passwords, such as using a passphrase. A passphrase is the same as a password but involves using more than just one word to make it ultra-secure, but still easy to remember.

Such as, *Mypasswordislong! or Ilikechicken2much*

The more characters you use in your password the more you increase its security, this is because the possible combinations a hacker would have to go through to find out what you have used is increased and the time it would take to crack your password magnifies.

You could create a sentence such as, *Where is king Arthur?*

This passphrase uses three of the four types of characters. Also remember, that spaces in the passphrase are (in some systems) classed as special characters too. To make things easier to remember you can use a sentence from a book, or a line from a song.

Use a secret combination; *J&Jwuth,2fapow*

Although this passphrase has fewer characters than the previous two, what makes this one strong is that it appears completely random. However, if you know the secret to decoding it, then all becomes clear. (Jack and Jill went up the hill, to fetch a pail of water.) This method is also using all four of character types. Again here you can use the first letters of the words which make up a line from a song, or the first letters from the words in a sentence of a book, etc.

5. What do I do, if I've forgotten my THG log on details?

Forgotten passwords can be reset from the Service Desk or End User Computer teams, the user must be authenticated before the password is changed and the password must never be spoken out loud to the user.

- The Service desk can be reached by phone, email or visiting in person.
- You will be requested to provide your name, and ID for the account needing the password reset.
- The new password will be sent to the mobile number on your Active Directory record. This should match the mobile number you provided as a contact number on joining the company. If you didn't provide one, proceed to HR to add it on your file.
- If you don't have a mobile phone, you can prearrange to use your line managers number.

6. What can I do to keep my password safe?

Some simple things to remember about how to act in keeping your password secure

- Never share your password with anyone, ever

- Never write your password down, unless you use a cryptic code that only you can understand
- Never let people watch you typing in your password, if you think someone watched you, change the password
- If ever in doubt about whether your password has been compromised, change it!

Using password managers

A password manager acts like a digital safe, whether using one online or a local application, which securely stores user accounts, passwords, and other sensitive information or special actions needed to access something.

Using one of these vaults allows you to have hundreds of unique, more complex passwords in random formats without you having to try and remember numerous 20+ digit combinations per account or application. Instead all you need to remember is one strong master password as a key to the safe.

Some additional tips…

1. Use only well-known and trusted password managers. Be wary of products that have not been around for a long time or have little to no community feedback. (Just like fake AV brands, cyber criminals can and have created fake password lockers to steal important information.)
2. Where available you should use two-factor-authentication (2FA) to increase the protection of your vault making it harder to break in and steal your passwords.
3. Ensure that you keep up to date and patch to the latest versions of the software.
4. And lastly avoid any password manager that claims to be able to recover your master password. This means that the support team know your password, or can easily obtain it, which exposes you to risk of tampering or loss.

7. Using two factor authentication (2FA)

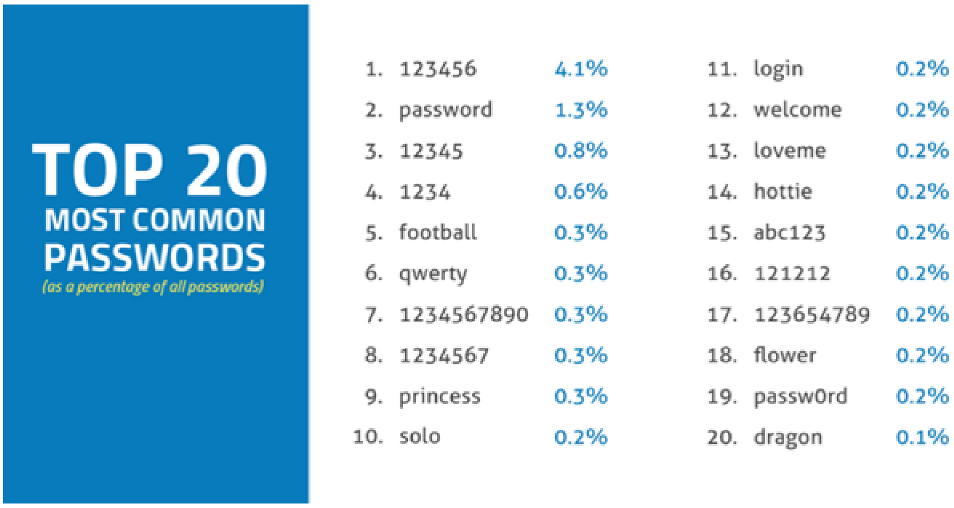
There are three ways in which you can authenticate yourself to a system, something you know, (e.g. password or combination), something you have, (e.g. ID card, token, smart phone, a key) and something you are (e.g. your voice, a fingerprint, or retina of your eye).

A quick example of two factor authentication in real life is your bank card. The card itself is the thing you have, and the pin number you remember and use at each transaction is something you know.

Some systems or websites allow you to use 2FA by taking your mobile number and sending you a text message when you log in to validate it's you and stop hackers gaining advantage of your system. Other websites can use smart phone applications called authenticators, some examples of these applications are *google authenticator, securenvoy, authy, duo mobile,* and there are other ones too. These apps can be sync'd up to your account so that a code or message appears in the application which you will use to log in with alongside your password.

ANNEX A - Top 20 of the most common passwords of 2015

While all these passwords are easy to remember for you, these are so very easy for hackers to guess defeating in essence what a password is for, which is protecting your account from misuse. If you are using any of these listed passwords, go change them now.



TOP 20 MOST COMMON PASSWORDS

(as a percentage of all passwords)

1.	123456	4.1%	11.	login	0.2%
2.	password	1.3%	12.	welcome	0.2%
3.	12345	0.8%	13.	loveme	0.2%
4.	1234	0.6%	14.	hottie	0.2%
5.	football	0.3%	15.	abc123	0.2%
6.	qwerty	0.3%	16.	121212	0.2%
7.	1234567890	0.3%	17.	123654789	0.2%
8.	1234567	0.3%	18.	flower	0.2%
9.	princess	0.3%	19.	passw0rd	0.2%
10.	solo	0.2%	20.	dragon	0.1%

ANNEX B - Blacklisting passwords

The Hut Group will be imposing a blacklist for active directory passwords this is to stop you choosing simple passwords relating to you or the business. The list will be extensive but here are a few examples to help you understand what to avoid;

Corporate - TheHutGroup1, THG01!, 1THG1, The_Hut_Group01, TheHut.com, TheHut01
Your name - BloggsJ1, BloggsJ2, BloggsJ3, BloggsJ01, BloggsJ02, BloggsJ03, JoeBloggs1
Simple - Password, Password01, Pa55w0rd, pa55d, drowssap, 1Password!,
Weak – Qwerty01, Qwert11, Qwer4321, 1234rewQ,
Common – F00tball, Letmein1, Trustno1,