LAUREA
UNIVERSITY OF APPLIED SCIENCES
Together we are stronger

Evaluating Password Managers for Enterprises

Mika Qvintus

Laurea University of Applied Sciences

Evaluating Password Managers for Enterprises

Bachelor of Business Administration
Bachelor's Thesis
June, 2018

Laurea University of Applied Sciences
Degree Programme in
Business Information Technology
Bachelor's thesis

Abstract

Evaluating Password Managers for Enterprises

2018 Pages 21

Employees within enterprises have hundreds of passwords to remember. This problem is known as password fatigue. The objectives of this thesis were to do research on authentication, passwords, and password managers, to provide a solution for password fatigue, and to find best password manager for Cargotec.

The data of this thesis was collected from an interview with an information security architect, two books: Certified Information Systems Security Professional Study Guide 2012 and The Perfect Password 2005. Benchmarking was used to evaluate password managers.

The results of this thesis confirm that passwords are still the dominant form of authentication. There is no security feature that allows the same cost level, efficiency, and usability. Password managers provide a solution to employees' bad habits of creating weak passwords, and enhance information security within an enterprise. Password managers solve the problem that is known as password fatigue.

Keywords: Password, Password Manager, Password Fatigue, Enterprise

Table of Contents

1 Introduction

I work in an international company called Cargotec. I have focused my studies into information security. I inquired from the information security team within Cargotec, what I could do for my thesis. Together with the team we came into a conclusion that I would evaluate password management tool for Cargotec.

Employees within Cargotec have excessive amount of passwords to remember. This problem is known as password fatigue. Password fatigue is a feeling, where employees constantly have to remember hundreds of passwords. Password fatigue causes employees to use weak passwords, which weakens information security within Cargotec.

Thesis was started by doing investigation on authentication methods and passwords. Password's threats were evaluated. Passwords were confirmed to be dominant form of authentication within enterprises.

Password managers were evaluated separately for enterprises. These evaluations were done by benchmarking. Key factors in this evaluation were cost, manageability, and security. Security was the primary factor to consider within this evaluation.

Goals in this thesis were to do research on authentication, passwords, and password managers. Evaluate password managers for enterprises. Choose the best password manager for Cargotec. Enhance information security within Cargotec, and prevent data breaches caused by weak passwords. The main goal in this thesis was to solve the problem known as password fatigue.

1.1 Organization

Cargotec is an international company, and it was founded in 2005. Cargotec's headquarter is located at Helsinki, Finland. Cargotec has over 11 000 employees. Cargotec operates in over 100 countries, and has its own personnel in 45 of them.

Figure 1 Countries (Cargotec 2018)

Cargotec has three business areas which are Kalmar, Hiab, and MacGregor. They are all related to handling shipping of containers and goods. Cargotec is also one of the largest software companies in Finland, measured by sales.

Kalmar's offering comprises industry shaping, sustainable cargo handling equipment and automated terminal solutions, software and services. These are used in ports, terminals, distribution centres and various industries (Cargotec 2018).

Hiab is the global market leader in on-road load handling solutions. Its customers operate in on-land transport and delivery where Hiab's products and services help customers run their businesses efficiently and safely (Cargotec 2018).

MacGregor's engineering solutions and services for marine cargo and offshore load handling are designed to perform with the sea. MacGregor aims to make the sea more accessible, safe and reliable for its customers (Cargotec 2018).

1.2 Research Problem

The average business employee must keep track of 191 passwords, according to a report made by LastPass. This causes the problem known as passwords fatigue within enterprises. Enterprises have also implemented security policies in attempt to enforce strong passwords. One of these policies includes a mandatory password change every three months. Employees are required constantly to change their passwords. This results into commonly used similar passwords as it is impossible for the employees to remember all of their passwords. These passwords are often written down into personal notebooks, post-it notes, or into unencrypted files.

Passwords are designed to be only known by the employee. Even after extensive implementation of security policies, employees are still able to create weak passwords. Weak passwords compromise information security, and create access points for malicious entities. Passwords and their sharing cause unnecessary work for information security team. They receive alerts from shared files that have word password.

Employees are constantly logging into applications, portals, and devices. Employees first must remember their credentials for these services. This takes considerable amount of time, and frustrates employees. Employees, who have forgotten their passwords, have to call helpdesk. Helpdesk has to reset employee's password. This will cost employees and helpdesk agent's time. Study conducted by Ovum in 2017 shows that 64 % of the employees said that they have password usage problems at least once a month.

Password usage is increasing rapidly. It was estimated by password manager company Dashlane that the number of passwords on average business employee doubles every five years. This number can be exaggerated as the source is password manager company, but it is not far from the truth.

1.3 Thesis Goals

Goals in this thesis were to do research on problem known as password fatigue. Create research on authentication methods and passwords. Investigate threats that weak passwords create for enterprises. Enhance information security within enterprises, and prevent data breaches. Main objective in this thesis was to choose the best password manager for Cargotec, and solve the problem known as password fatigue.

According to study conducted by Ovum 69 % of the personnel in enterprises would use a password manager, if their company provided one.

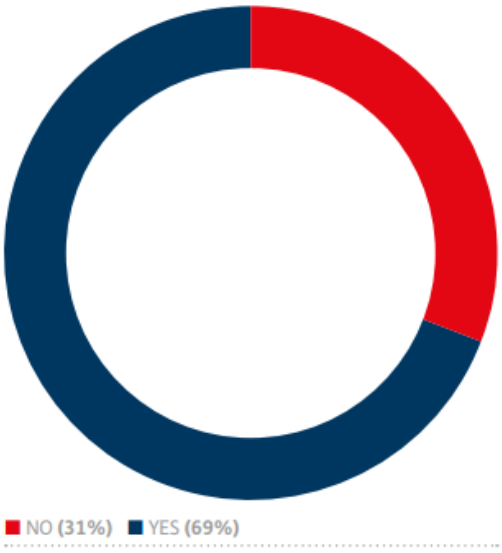

Figure 2: Employees (Ovum 2018)

2 Theoretical Background

Theoretical background was established in this thesis to research on authentication methods, passwords, and passwords managers. Explain the terms that are used in this thesis. Provide background information on how does password manager improve information security within enterprise.

2.1 Authentication

Authentication is a method to confirm user's identity. It ensures that individual is who they say, they are. Authentication is one of central aspects of information security. There are three types of authentications:

"Type 1 authentication factor is something you know. It is any string of characters you have memorized and can reproduce on a keyboard when prompted. Examples include a password, personal identification number (PIN), passphrase, or mother's maiden name" (Stewart, Chapple & Gibson 2012, 9).

"Type 2 A Type 2 authentication factors is something you have. It is a physical device that you must have in your possession at the time of authentication. Examples include a token device, smart card, memory card, or USB drive" (Stewart, Chapple & Gibson 2012, 9).

"Type 3 authentication factor is something you are or something you do. It is a physical characteristic of a person identified with different types of biometrics. Examples in the "something you are" category include fingerprints, voice prints, retina patterns, iris patterns, face shapes, palm topology, and hand geometry. Examples in the "something you do" category

include signature and keystroke dynamics, also known as behavioural biometrics" (Stewart, Chapple & Gibson 2012, 9).

The type 1, which includes password, is the weakest authentication method. Each one of these authentication methods has their benefits and disadvantages. Enterprise has to create threat analysis, when implementing security protocols, and evaluate, what is the required security for that system.

2.2 Password

"A password is a string of characters used to verify the identity of a user during the authentication process. Passwords are typically used in conjuncture with a username; they are designed to be known only to the user and allow that user to gain access to a device, application or website. Passwords can vary in length and can contain letters, numbers and special characters" (Techtarget 2018).

Password is the most commonly used authentication method in the world. Passwords are used by employees every day. They are equivalent to a house-key. Employees gain access to certain system with the correct password.

2.3 Password Weaknesses

"The single most important aspect of information security is strong passwords. Likewise, the single greatest security failure is weak passwords. Network administrators blame users for selecting such poor passwords, and users blame network administrators for the inconvenience of their draconian password policies" (Burnett, Kleiman, & Russell, 2005, 10).

"Character diversity is a key component of strong passwords. The purpose of using many different types of characters is to reduce the predictability and weakness of your passwords" (Burnett, Kleiman, & Russell, 2005, 52).

Passwords are difficult to enforce as employees choose their own passwords, and it is designed to be only known by the employee. After enforcement of security policies, employees are still able to select weak passwords. There are two basic problems with employee's passwords. Employees create weak passwords in the first place, and they reuse these weak passwords constantly.

2.4 Password Attacks

Password attack is an attempt to gain user's password. Malicious entities use programs, and other tools such as social engineering to gain employee's passwords. When malicious entity gains the passwords, they also gain access to a system, or database. Passwords are a high value target for attackers, and provide the easiest way into a system.

2.4.1 Dictionary Attack

Dictionary attack is a method that uses a list of words. These words are commonly used passwords by the users. If malicious entity has thousands of accounts the probability of one account having a password from the most commonly used passwords is high (Tenchopedia 2018).

2.4.2 Brute Force Attack

Brute force attack is a way to obtain user's password by force. Brute force attack tries every single combination possible. The number of characters on the passwords makes enormous difference. Simple 4-character password effortless to crack with this method. The amount of time, it takes to crack a password grows exponentially, when characters are added to passwords. Complicated password with 12-characters takes more than 100 million years (Tenchopedia 2018).

2.5 Social Engineering

"Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources" (Incapsula 2018).

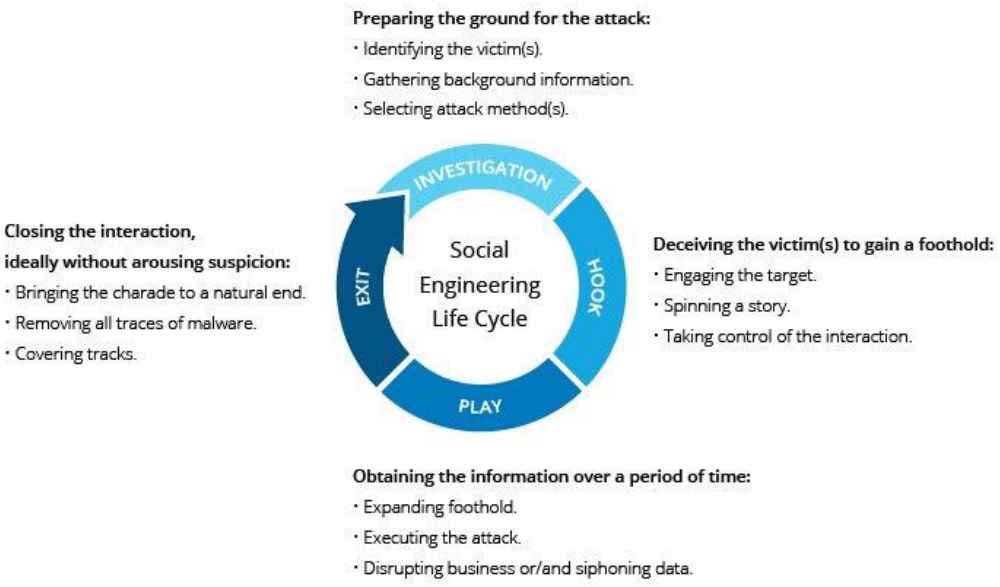

Figure 3: Social Engineering (Incapsula 2018)

Social engineering is a used by malicious entities in order to get employees' passwords. There are multiple different methods, how hackers try to convince users to give their passwords or other sensitive information.

2.5.1 Dumpster Diving

Dumpster diving is a method, where malicious entity looks thought trash in order to find valuable information such as passwords. Most workplaces have a dumpster with a lock, where employees are able to throw sensitive paperwork. However, employees are often inconsiderable, and throw their password notes into regular trash (Tenchopedia 2018).

2.5.2 Phishing and Pharming

Phishing is attempt to gain knowledge and sensitive information by disguising being someone else than they truly are. These attempts are often done by email. In this email, malicious entity pretends to be someone with high position inside the company requesting sensitive information (Searchsecurity 2018).

Pharming is an attempt to direct user to a malicious site. Malicious site is similar to legitimate site. The site is in fact made by entity that wants to steal user's login credentials. User writes down their credentials thinking that they are simply signing in. After signing in, the site steals the credentials, and reveals them to malicious user. (Searchsecurity 2018).

2.6 Data Breaches

Investigation made by Verizon Enterprises in 2017 confirmed that 81 % of data breaches are, because of stolen, default, or weak password. Nothing is 100 % secure, when it comes to information security. Allowing employees of an organization to use weak passwords makes it easy for the malicious entities to gain access into enterprises systems.

2.7 Password's future

Passwords are dead is an old saying in information security. Passwords are going to be replaced with different authentication methods. Currently passwords are still a dominant form of authentication. There is no other authentication method that allows same level of cost-efficiency and usability.

2.8 Password Manager

"Password managers enable the use of strong and unique passwords for each online account, and provide an efficient way to manage all the passwords. The login information is encrypted and stored in either the local memory of the user's system or in cloud storage" (Techopedia 2018).

Password manager creates unique and complex passwords for each different site, device and, application automatically. These passwords will be stored in a vault. Users gain access to this vault by a master password.

2.8.1 Cloud-Based Password Manager

Cloud-based password managers work as extensions on browsers. Browser extension is a plug-in that improves, or creates a new functionality. Essentially, they customize browser, and improves the user experience. Cloud-based password manager provides flexibility, as it can be used on multiple devices (Csonline 2018).

2.8.2 Locally-Based Password Manager

Locally-based password manager encrypts user's passwords locally in their devices, and stores the passwords on the devices. These password managers have better security as it is harder to gain access to computers than into browsers. Locally-based password managers aren't as mobile as their counterparts as they are tied to the device (Csonline 2018).

2.9 Password Manager Features

Password managers have similar core features. These core features include:

- Auto login
- Import from competition
- Automatically generated strong passwords and usernames

Auto login allows user to log-in to a service without having to type credentials. Password managers allow users to export and import their vaults to different password managers. They have a button next to a login screen. Users press that button and password manager creates strong usernames and passwords for that service.

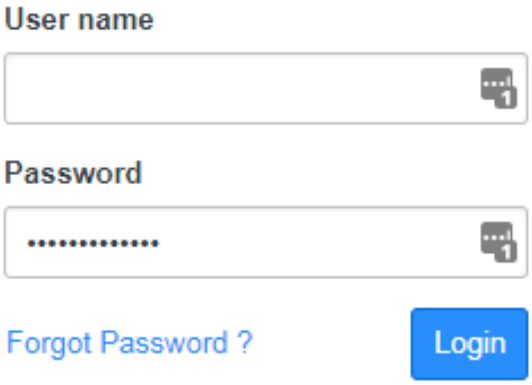

Figure 4: Button

2.10 Password Manager Security Features

These are the most important features from security's perspective within enterprise:

- Centralized Admin Control
- Resetting End-User Accounts
- Compliable with Microsoft Active Directory
- Configuring Custom Security Policies
- Automate Reporting
- 2-Step Verification
- Secure Sharing
- Training Material
- Audits
- Backup
- Reliable Service

Centralized admin control allows the information security team to manage employees, and reset their master passwords, if they forget it. Enterprise password managers are compliable with Microsoft Active Directory. Security team can manage, and configure custom security policies to ensure secure passwords. Automated reporting enables the security team to get accurate reports from passwords usage. 2-Step Verification provides an extra layer of security. Secure sharing enables safe password sharing between employees.

Password manager has training material for security experts and employees. Audits that test password manager's security are valuable information to enterprises. This feature helps to evaluate the security of the password manager. Backup of the system is important aspect of information security. Reliable service is required from the password manager; their services have to be online 24/7.

2.11 Encryption

"In computing, encryption is the method by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key. Encryption is one of the most important methods for providing data security" (SearchSecurity 2018).

Passwords in a password manager cannot be stored in a plain text within the vault. Password vault needs to be encrypted to provide security. Most commonly used encryption formats used by password managers are 256-bit AES encryption and SHA256-hash.

AES 256 stands for Advanced Encryption Standard. The number refers to key size of the encryption. This encryption is used worldwide to protect sensitive data. U.S military uses this encryption as their normal encryption format.

“The Secure Hash Algorithm 256 or SHA 256, is one of the most secure ways to protect digital information. A hash is a mathematical computer program that takes any set of information and turns it into letters and numbers of a certain length. Hashing is used to make storing and finding information quicker because hashes are usually shorter and easier to find. Hashes also make information unreadable and so they become a secret.” (Decryptionary 2018).

Hashing encrypts the passwords within the vault. If a password vault would fall into wrong hands and malicious entity could steal the vault’s contents. The content would still be encrypted and unreadable.

3 Research Methods

Research on authentication methods and passwords was done by reading from valued books in information security field. These two books were Certified Information Systems Security Professional Study Guide 2012 and The Perfect Password 2005.

3.1 Interview

Information security architect was interviewed in order to get assessment of the research problem. He explained the problem that enterprises are having with information security and password management.

3.2 Benchmarking

Benchmarking refers to testing a product or service against a reference point to quantify how much better or worse it is compared to other products. Benchmarking is the standard way of comparing one product to another (Tenchopedia 2018).

Benchmarking was used in this thesis to compare password managers, and to create separate evaluation of each password manager. Password managers were evaluated from material provided by each company.

3.3 Requirements of Cargotec

Cargotec had certain specifications that information security team required from password manager. Password manager has to be intuitive for the employees. It should make their day-to-day life easier, and solve the problem what is known as password fatigue within Cargotec.

Cargotec is interested in the lifetime cycle of the password manager. How it is managed? Is there any auditing? How fast is the password manager reacting to security threats, and patching them? How is it updated, and kept secure? Password manager must be manageable by security team, and it must have a centralized control. Password manager must be able to support platforms that are used by Cargotec and it has to have helpdesk.

4 Results

Passwords are never safe, but implementation of password manager is safer than currently used password policies within an enterprise. Despite systems and applications having immense security protocols and security implementations, weak passwords remain a threat.

Password manager provides protection against commonly used password attacks as, it creates complex passwords. Password manager eliminates the need to write passwords down, which protects against dumpster diving. Password managers are able to detect sites that they have already saved password to. This feature helps to prevent pharming and phishing attacks to sites that employees have already saved their passwords to.

Password managers started with multiple different encryption methods, and supported various platforms. They have evolved into similar applications, and there is no remarkable difference between password managers that are meant for enterprises. These are best practises for password managers.

Password managers have a single point of failure. Regular passwords are encrypted within the vault. If malicious entity gains the master password, they are able to by-pass the security features, and gain access to the vault. Two-step verification that uses different types of authentication methods is important factor to have by enterprise to have extra layer of security to prevent this.

4.1 Implementation of Password Manager for Enterprise

There are only three viable options for enterprises, when it comes to password managers. These options are LastPass Enterprise, Dashlane Business and Keeper Business. Only these three options had the required security and features.

Enterprise will have to define, how it fits into corporate security strategy. Important factors to consider are usability, training materials for employees and employers, lifecycle of the password manager, and costs.

4.2 LastPass Enterprise

LastPass was founded in 2008. It is one of the most popular, and the most advertised password managers on the market. LastPass Enterprise is a version meant for enterprises. It currently has around 33,000 businesses as its customers. LastPass had minor incidents with security. LastPass Enterprise costs 48 dollars a year per license, and it has trial period of 14 days. LastPass provides extensive amount of training materials, and implementation guides.

4.3 Dashlane Business

Dashlane was founded in 2011. It has been evaluated one of the best password manager in the market for average user. Dashlane license costs 48 dollars a year, and it has a trial for 30 days. Dashlane has decent amount of training and implementation material. Dashlane doesn't provide as comprehensive guides as its rivals. Dashlane has had troubles in the past, as it wasn't compliable with Lenovo Yoga, but it has not yet had any known security breaches.

4.4 Keeper Business

Keeper Business was founded in 2011. Keeper Business costs 45 dollars year per license and offers 14-day trial-period. Google security researcher Tavis Ormandy found out in 2017, that the software recommended installing a browser add-on, which contained a vulnerability allowing any website to steal any password.

4.5 Password Managers Compared

Here is a list of password managers compared by factors:

Table 1: Benchmarking

Factors	**LastPass Enterprise**	**Dashlane Business**	**Keeper Business**
Cost per license	48 dollars per year	48 dollars per year	45 dollars per year
Trial Period	14 Days	30 Days	14 Days
Training Material	Extensive	Decent	Extensive
2-Step Verification	Yes	Yes	Yes
Helpdesk	Yes	Yes	Yes
Auditing	Regularly	No information	No information
Platforms	Windows, Mac, Linux and Android, IOS	Windows, Mac, Linux and Android, IOS	Windows, Mac, Linux and Android, IOS
Platforms - Browsers	Chrome, Firefox, Safari, Internet Explorer, Opera, Microsoft Edge	Chrome, Internet Explorer, Microsoft Edge	Chrome, Firefox, Safari, Internet Explorer, Microsoft Edge

Enterprises are able to evaluate what is required from the password manager. If they are worried about the supported platforms, they can choose the password manager that supports the most platforms.

Costs play a huge part in this decision. Large enterprise, which implements a password manager for 1000 employees, must pay considerably more if they choose to have all of the supported platforms. Keeper Business implemented for 1000 employees will cost enterprise 45 000 dollars in a year while LastPass will cost 48 000. This cost rises higher with each employee.

5 Conclusion and Discussion

Best password manager for Cargotec is LastPass Enterprise. LastPass Enterprise is expensive, but it has most to offer. LastPass has extensive material on training end-users, and security experts. They have materials how to implement LastPass into enterprises environment, and implementation is done within days. LastPass has ready email-templates to send end-users that inform employees that they will receive a solution for password fatigue. LastPass provides helpdesk for Cargotec, and it is available 24/7.

LastPass was one of the first password managers to come into market. It has the most customers, and it is most likely to have longest lifecycle. They have learned from their security breaches, and are conducting regular audits to provide security for their customers. Lastpass is using strong security encryptions to ensure security of customer's vaults. LastPass is manageable by information security team, and they are able to configure security policies such as master password policies and enforcement of 2-step verification. These policies ensure the security of Cargotec. LastPass supports various platforms which are in use at Cargotec such as Mac, Windows, Linux and Chrome, Firefox, Safari, Internet Explorer, Opera, Microsoft Edge.

LastPass enables employees to have a productive work-day as they don't constantly have to remember their passwords and are automatically logged into a service. This results in a positive end-user experience while enhancing information security. LastPass fills Cargotec's needs from password manager, and solves the problem what is known as password fatigue.

References

Burnett, M., Kleiman, D. & Russell, R. 2005. *Perfect Password*. Rockland: Syngress.

Cargotec. 2018. Referenced 6.4.2018
https://www.cargotec.com/

Dashlane. 2018. Referenced. 15.5.2018
https://www.dashlane.com/

Dashlane. Infographic Online Overload. Referenced 18.5.2018
https://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/

Decryptionary. Dictionary. Secure Hash Algorithm. Referenced 11.5.2018
https://decryptionary.com/dictionary/secure-hash-algorithm-256/

Enterprise. LastPass. Referenced 17.5.2018
https://enterprise.lastpass.com/

Incapsula. 2018. Web Application Security. Social Engineering Attack. Referenced 8.5.2018
https://www.incapsula.com/web-application-security/social-engineering-attack.html

Keeper Security. 2018. Blog. Referenced 14.5.2018
https://keepersecurity.com/blog/2017/12/15/update-for-keeper-browser-extension-v11-4/

LastPass. Report. 2017. Referenced 13.5.2018
https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/LastPass-Enterprise-The-Password-Expose-Ebook-v2.pdf

LastPass. Report. Referenced 16.5.2018
https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/ovum-lastpass-whitepaper.pdf

Laurila, T. 2018. Information Security Architect Interview. Cargotec Oyj. Helsinki

Stewart, JM, Chapple, M, & Gibson, D 2012, CISSP: Certified Information Systems Security Professional Study Guide, John Wiley & Sons, Incorporated, Somerset

Searchsecurity. Techtarget. 2018. Definition. Encryption. Referenced 12.5.2018
https://searchsecurity.techtarget.com/definition/encryption

Searchsecurity. Techtarget. Definition. Password. Referenced 13.5.2018
https://searchsecurity.techtarget.com/definition/password

Searchsecurity. Techtarget. Definition. Phishing. Referenced 17.5.2018
https://searchsecurity.techtarget.com/definition/phishing

Searchsecurity. Techtarget. Definition. Pharming. Referenced 17.5.2018
https://searchsecurity.techtarget.com/definition/pharming

Techopedia. 2018. Definition. Benchmarking. Referenced 3.6.2018
https://www.techopedia.com/definition/17053/benchmarking

Techopedia. 2018. Definition. Brute Force Attack. Referenced 15.5.2018
https://www.techopedia.com/definition/18091/brute-force-attack

Techopedia. 2018. Definition. Dumpster Diving. Referenced 16.5.2018
https://www.techopedia.com/definition/10267/dumpster-diving

Techopedia. 2018. Definition. Dictionary Attack. Referenced 15.5.2018
https://www.techopedia.com/definition/1774/dictionary-attack

Techopedia. 2018. Definition. Password Manager. Referenced 15.5.2018
https://www.techopedia.com/definition/31435/password-manager

T.Ferrill. 2018. The 6 Best Password Managers. Referenced 13.5.2018
https://www.csoonline.com/article/3198507/security/the-6-best-password-managers.html

Verizon Enterprises. Resources. Reports. 2016. Referenced 9.5.2018
http://www.verizonenterprise.com/resources/reports/rp_dbir-2016-executive-summary_xg_en.pdf

Verizon Enterprises. Resources. Reports. 2018. Referenced 15.5.2018
https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

Figures

Tables