GRA

GIBRALTAR REGULATORY AUTHORITY

(26A) Credential Stuffing Guidelines

Gibraltar General Data Protection Regulation and the Data Protection Act 2004

28th June 2022

IR01/22

FOREWORD

Gibraltar's data protection law consists of both the Gibraltar General Data Protection Regulation ("Gibraltar GDPR") and the Data Protection Act 2004 ("DPA").

The legislation in Gibraltar maintains the data protection standards that applied in Gibraltar as a result of EU Law i.e. the EU General Data Protection Regulation 2016/679 and the Law Enforcement Directive 2016/680, prior to Brexit and the end of the transition period.

Organisations involved in the processing of personal data need to be aware of the obligations that the Gibraltar GDPR and/or the DPA impose on them.

The Gibraltar Regulatory Authority, as the Information Commissioner, regularly publish guidance notes that aim to –

- *raise awareness amongst controllers and processors of their data protection obligations; and,*
- *assist them in ensuring compliance.*

Guidance notes also aim to promote public awareness of the risks to personal data that may arise from data processing activities.

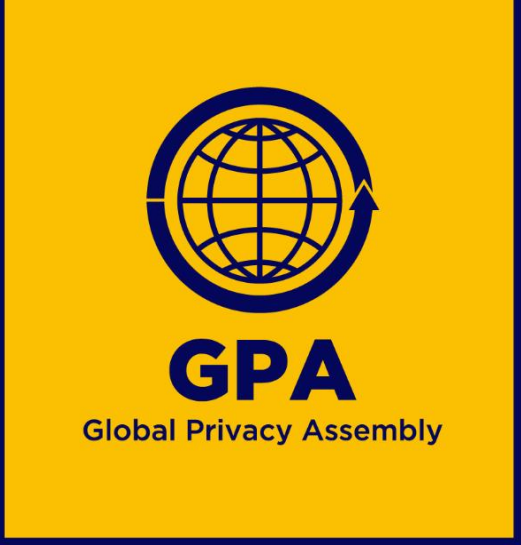
CREDENTIAL STUFFING GUIDELINES

Credential stuffing is a cyber-attack method that exploits people's tendency to use the same username and password combination across multiple online accounts. These attacks are automated and often large scale, using stolen, legitimate credentials obtained from unrelated data breaches to access people's accounts across websites.

The Gibraltar Regulatory Authority **("GRA")** as the Information Commissioner, participated in a sub-working group **("SWG")** of the International Enforcement Working Group of the Global Privacy Assembly **("GPA")**, which focused on the threat of credential stuffing to personal data. The SWG comprised of the GRA and data protection authorities from Canada, Jersey, Switzerland, Turkey and the United Kingdom. The SWG conducted research on credential stuffing, collating information from data protection and privacy authorities worldwide, and engaging with external experts and stakeholders on the matter. On the basis of said research and engagement, the GPA published guidelines for organisations on how to prevent, detect and mitigate the risks of credential stuffing attacks.

The guidance highlights how data protection laws require appropriate security measures to be implemented to prevent unauthorised processing of personal data (including access), as is the case under the local Gibraltar General Data Protection Regulation **("Gibraltar GDPR")**.

Therefore, given the threat to personal data from credential stuffing (particularly to organisations with user accounts that may be accessed online), and the unauthorised processing that could result, the guidelines are provided overleaf, in order to assist local organisations in meeting applicable legal obligations, in particular, that personal data be processed securely, as required under the Gibraltar GDPR.



International Enforcement Cooperation Working Group

Credential Stuffing Guidelines – 27th June 2022

Credential stuffing sub-working group authorities:

- Office of the Privacy Commissioner of Canada
- Gibraltar Regulatory Authority
- Jersey Office of the Information Commissioner
- Switzerland's Federal Data Protection and Information Commissioner
- Turkey's Data Protection Authority
- United Kingdom's Information Commissioner's Office

Table of Contents

Executive Summary 3
Acknowledgements 4
1. Introduction 9
2. How does credential stuffing work? 10
3. Why are credential stuffing attacks carried out? 12
4. Growing global concerns 15
5. Examples of credential stuffing cases 17
6. Data security in privacy and data protection law 19
7. Measures to detect, prevent and mitigate the risk of credential stuffing 20

Executive Summary

The International Enforcement Cooperation Working Group (IEWG) is a permanent Working Group of the Global Privacy Assembly (GPA), which is co-chaired by: the Office of the Privacy Commissioner of Canada; the Office of the Privacy Commissioner for Personal Data, Hong Kong, China; the Superintendence of Industry and Commerce of Colombia; and the Norwegian Data Protection Authority.

The work of the IEWG is integral to the GPA, supporting its strategic ambitions around leadership, cooperation, and advancing global privacy in a digital age. In particular, the IEWG has primary responsibility for leading on delivery of actions under the Regulatory and enforcement cooperation Pillar of the GPA's 2021-23 Strategic Plan.

Credential stuffing was identified as an area of concern by the IEWG at a Closed Enforcement Session[1] in March 2021. As a result, follow up action was agreed and a sub-working group (SWG) of the IEWG was created to work on the topic and produce material that aims to assist authorities to address the rising threat of credential stuffing.

These guidelines identify the threat of credential stuffing to personal data and recognised measures that organisations can use to mitigate the risk to personal data. While these guidelines do not represent a statement of legal obligations across all jurisdictions, they may assist organisations in complying with data protection and privacy laws, which will generally require organisations to adequately protect personal information against threats like those posed by credential stuffing attacks.

[1] Closed Enforcement Sessions are the way in which the IEWG identifies and examines significant issues or organisations, with global implications for people's data protection and privacy rights, and acts as a platform to promote and support practical enforcement cooperation, as appropriate. Typically, Closed Enforcement Sessions begin with a presentation on a topic, followed by an open discussion on key concerns, regulatory approaches, and opportunities for cooperation.

Acknowledgements

These guidelines have benefitted from, and incorporate, as appropriate, relevant material published by a range of organisations. The list below is intended to recognise and acknowledge the material used/ referred to. References are also included throughout the document.

In addition to the material referred to below, this guidance has benefitted from engagement with, consultation, and contributions from experts in the cyber security domain[2], namely:

- The Global Privacy Assembly's Reference Panel –
    - Bojana Bellamy, Centre for information Policy Leadership (with the involvement of Lisa Sotto, Hunton Andrews Kurth).
    - Clarisse Girot, Asian Business Law Institute (with the involvement of James McLeary, Kroll and Rajesh Sreenivasan, Rajah & Tann LLP).
- The United Kingdom's National Cyber Security Centre.
- The Open Web Application Security Project – Shuman Ghosemajumder, F5.

Akamai

Akamai, *[State of the Internet]/security credential stuffing: attacks and economies* (vol. 5 | 2019)

Akamai, *[State of the Internet]/security web attacks and gaming abuse* (vol. 5 Issue 3| 2019)

Akamai, *[State of the Internet] phishing for finance* (vol. 7 Issue 2| 2021)

Arkose Labs

'Click Farm: What is it and How to Stop it'
https://www.arkoselabs.com/explained/click-farm/

British Broadcasting Corporation News

'Yahoo 2013 data breach hit 'all three billion accounts'
https://www.bbc.com/news/business-41493494

Canadian Centre for Cyber Security

'Password Managers – Security'
https://cyber.gc.ca/en/guidance/password-managers-security-itsap30025

'Rethink Your Password Habits to Protect Your Accounts from Hackers'
https://cyber.gc.ca/en/guidance/rethink-your-password-habits-protect-your-accounts-hackers-itsap30036

[2] The collaborative approach adopted allowed the working group to draw on the experience and expertise of specialists to support and strengthen the work carried out. Said external engagement and collaboration also contributes to the development of the GPA's voice and influence as per the GPA's Strategic Priority 2.

‘Statement on GCKey Credential Service and recent credential stuffing attacks’
https://cyber.gc.ca/en/news/statement-gckey-credential-service-and-recent-credential-stuffing-attacks

Cloudflare

‘What Is Credential Stuffing?’
https://www.cloudflare.com/learning/bots/what-is-credential-stuffing/

ComputerWeekly.com

‘Over 15 billion credentials for sale on dark web’
https://www.computerweekly.com/news/252485713/Over-15-billion-credentials-for-sale-on-dark-web

Digital Shadows Photon Research Team

‘From Exposure to Takeover: The 15 billion stolen credentials allowing account takeover’:
https://resources.digitalshadows.com/whitepapers-and-reports/from-exposure-to-takeover

European Union Agency for Cybersecurity

‘Main Incidents in the EU and worldwide January 2019 to April 2020’
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents

F5

‘2021 Credential Stuffing Report’
https://www.f5.com/labs/articles/threat-intelligence/2021-credential-stuffing-report

Google

‘Online Security Survey’
https://services.google.com/fh/files/blogs/google_security_infographic.pdf

Ireland Data Protection Commission

‘Know your obligations – data security’
https://www.dataprotection.ie/en/organisations/know-your-obligations/data-security-guidance

Microsoft

‘Your Pa$$word doesn’t matter’
https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984

Norway National Security Authority

'Password Recommendations'
https://nsm.no/aktuelt/passordanbefalinger-fra-nasjonal-sikkerhetsmyndighet

Open Web Security Project Foundation

'Credential stuffing'
https://owasp.org/www-community/attacks/Credential_stuffing

'Credential Stuffing Prevention Cheat Sheet'
https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html

'Cross- Site Request Forgery Prevention Cheat Sheet'
https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html

Shape Security

Shape Security, *The 2018 credential spill report* (2018)

Shape Security, *Attacker economics* (2020)

UK Information Commissioner's Office

'ICO fines Uber £385,000 over data protection failings'
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/ico-fines-uber-385-000-over-data-protection-failings/

'Passwords in online services'
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/passwords-in-online-services/

UK National Cyber Security Centre

'Multi-factor authentication for online services'
https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services

'NCSC Glossary'
https://www.ncsc.gov.uk/information/ncsc-glossary

'Password administration for system owners'
https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

'Preventing lateral movement'
https://www.ncsc.gov.uk/guidance/preventing-lateral-movement

'Secure system administration: Use privileged access management'
https://www.ncsc.gov.uk/collection/secure-system-administration/use-privileged-access-management

'Three random words or #thinkrandom'
https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0

'Top tips for staying secure online'

https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/activate-two-factor-authentication-on-your-email

'Use of credential stuffing tools'
https://www.ncsc.gov.uk/news/use-credential-stuffing-tools

US Bureau of Internet and Technology (BIT) of the New York Attorney General's Office

'Business Guide for Credential Stuffing Attacks
https://ag.ny.gov/sites/default/files/businessguide-credentialstuffingattacks.pdf

US Electronic Code of Federal Regulations

'Standards for safeguarding customer information'
https://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=1e9a81d52a0904d70a046d0675d613b0&rgn=div5&view=text&node=16%3A1.0.1.3.38&idno=16

US Federal Bureau of Investigation (FBI)

'Cyber Actors Conduct Credential Stuffing Attacks Against US Financial Sector'
https://www.documentcloud.org/documents/7208239-FBI-PIN-on-credential-stuffing-attacks.html

'Private Industry Notification 20200910-001'
https://www.ic3.gov/media/news/2020/200929-1.pdf

'Scams and safety: Business email compromise'
https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise

US Federal Trade Commission

'Operator of Online Tax Preparation Service Agrees to Settle FTC Charges That it Violated Financial Privacy and Security Rules'
https://www.ftc.gov/news-events/press-releases/2017/08/operator-online-tax-preparation-service-agrees-settle-ftc-charges

'Stick with Security: Require secure passwords and authentication'
https://www.ftc.gov/news-events/blogs/business-blog/2017/08/stick-security-require-secure-passwords-authentication

'Taxslayer complaint, Docket NO. C-1623063'
https://www.ftc.gov/system/files/documents/cases/1623063_taxslayer_complaint.pdf

'Taxslayer Decision and Order, Docket NO. C-1623063'
https://www.ftc.gov/system/files/documents/cases/1623063_taxslayer_decision_and_order.pdf

US National Institute of Standards and Technology

'Digital Identity Guidelines'
https://pages.nist.gov/800-63-3/sp800-63b.html#throttle

US New York State Office of the Attorney General

The People of the State of New York by Letitia James, Attorney General of the State of New York v Dunkin' Brands, Inc (2019) Complaint Index No. 451787/2019
https://ag.ny.gov/sites/default/files/dunkin_complaint.pdf

The People of the State of New York by Letitia James, Attorney General of the State of New York v Dunkin' Brands, Inc (2020) Judgement and Consent Order Index No. 451787/2019
https://ag.ny.gov/sites/default/files/proposed_consent_order_and_judgment.pdf

US Securities and Exchange Commission, Office of Compliance Inspections and Examinations Officers

'Cybersecurity: Safeguarding Client Accounts against Credential Compromise'
https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf

US Securities and Exchange Commission v Altaba Inc., f/d/b/a Yahoo! (2018)
https://www.sec.gov/litigation/admin/2018/33-10485.pdf

Verizon

'2019 data breach investigations report'
https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

1. Introduction

A credential stuffing attack is a cyber-attack method that exploits an individual's tendency to use the same credentials (e.g. username/email address and password combination) across multiple online accounts. The attacks are automated and often large scale, using stolen credentials (e.g. that are leaked in connection with data breaches and made available on the 'dark web'), to unlawfully access users' accounts on unrelated websites.

Successful credential stuffing attacks may result in fraud or other means of financial loss, as attackers may, for example, make purchases using the compromised account or transfer funds to their own account. Upon establishing a secure foothold, an attacker may attempt to obtain further access to data and systems through the harvesting of other visible or accessible credentials. Such attacks may also be used to cause intangible harm such as reputational damage by spreading disinformation or making false statements about an individual whilst using their compromised account

Both the public and private sectors have reported credential stuffing to be an increasingly significant issue, one which poses a risk to personal data on a large and global scale. Our reliance on digital services shows no sign of slowing, and it appears that neither do the exploitative methods nor means used by cyber-criminals to carry out attacks on such services.

These guidelines serve as recognition of the global threat to personal data from credential stuffing, by the IEWG. These guidelines should assist organisations protect data from credential stuffing attacks. The manner in which these guidelines can support the work of an authority will be determined by each authority. For example, the guidelines may – act as a point of reference for authorities, in the context of knowledge sharing; assist authorities to issue guidance, a warning, or notice on credential stuffing; and, help establish a set of measures that are recognised as being effective against credential stuffing risks, which authorities can use in their assessment of the security measures employed.

2. How does credential stuffing work?

Although credential stuffing attacks are sometimes considered a subset of brute force attacks, it is important to differentiate between them:

(a) A **brute force attack** involves an attempt to gain unauthorised access to online accounts or services by using software that automatically generates and enters a huge number of possible value combinations on website log-in pages, until the correct password is discovered, and access is gained.[3]

(b) By contrast, a **credential stuffing attack** involves the fraudulent obtaining of valid account credentials (e.g. pairs of usernames/email addresses and passwords) from compromised accounts and "stuffing" these into the account log-in sections of online sites until correct matches are found.

Credential stuffing attacks are widely recognised as a cyber threat to data security by key cyber security organisations[4]. Credential stuffing attacks are relatively straightforward to launch and there is a wide range of easily accessible automated software to facilitate them.[5] In this regard, tools such as botnets (i.e. collections of internet robots or internet connected devices) and account checker apps are used to automatically insert the credentials into the relevant fields on a large number of online sites.[6] Examples of such tools include: Sentry MBA, Account Hitman, Vertex and Apex.[7]

Attacks may be carried out with relative ease by acquiring one of the above-mentioned tools as well as a configuration file for the online site, along with a list of legitimate credentials.[8] Once the attack is launched, log-in attempts are typically directed through one or more proxies in order to hide the source of the attack and avoid detection.[9] In a further attempt to bypass increasingly robust organisational security measures, attackers may also 'outsource' their fraudulent activity to low-paid, unskilled workers in a 'click farm' or 'fraud farm'[10]. These workers are usually paid a small, set fee to complete CAPTCHA's or any other authentication 'challenges' that cannot be completed by bots to successfully complete an attack[11].

A typical credential stuffing attack consists of the following steps, as further illustrated in Figure 1.

---

[3] See definition in the UK's National Cyber Security Centre (NCSC), 'NCSC Glossary': https://www.ncsc.gov.uk/information/ncsc-glossary accessed 25 May 2021.

[4] For example, the NCSC: https://www.ncsc.gov.uk/news/use-credential-stuffing-tools accessed 25 May 2021; the Canadian Centre for Cyber Security: https://cyber.gc.ca/en/guidance/rethink-your-password-habits-protect-your-accounts-hackers-itsap30036 accessed 25 May 2021; the Open Web Security Project Foundation: https://owasp.org/www-community/attacks/Credential_stuffing accessed 25 May 2021.

[5] NCSC, 'Use of credential stuffing tools': https://www.ncsc.gov.uk/news/use-credential-stuffing-tools accessed 25 May 2021.

[6] Canadian Centre for Cyber Security, 'Rethink Your Password Habits to Protect Your Accounts from Hackers': https://cyber.gc.ca/en/guidance/rethink-your-password-habits-protect-your-accounts-hackers-itsap30036 accessed 25 May 2021.

[7] NCSC, 'Use of credential stuffing tools': https://www.ncsc.gov.uk/news/use-credential-stuffing-tools accessed 25 May 2021.

[8] Ibid.

[9] Ibid.

[10] Arkose Labs, 'Click Farm: What is it and How to Stop it': https://www.arkoselabs.com/explained/click-farm/ accessed 18 March 2022.

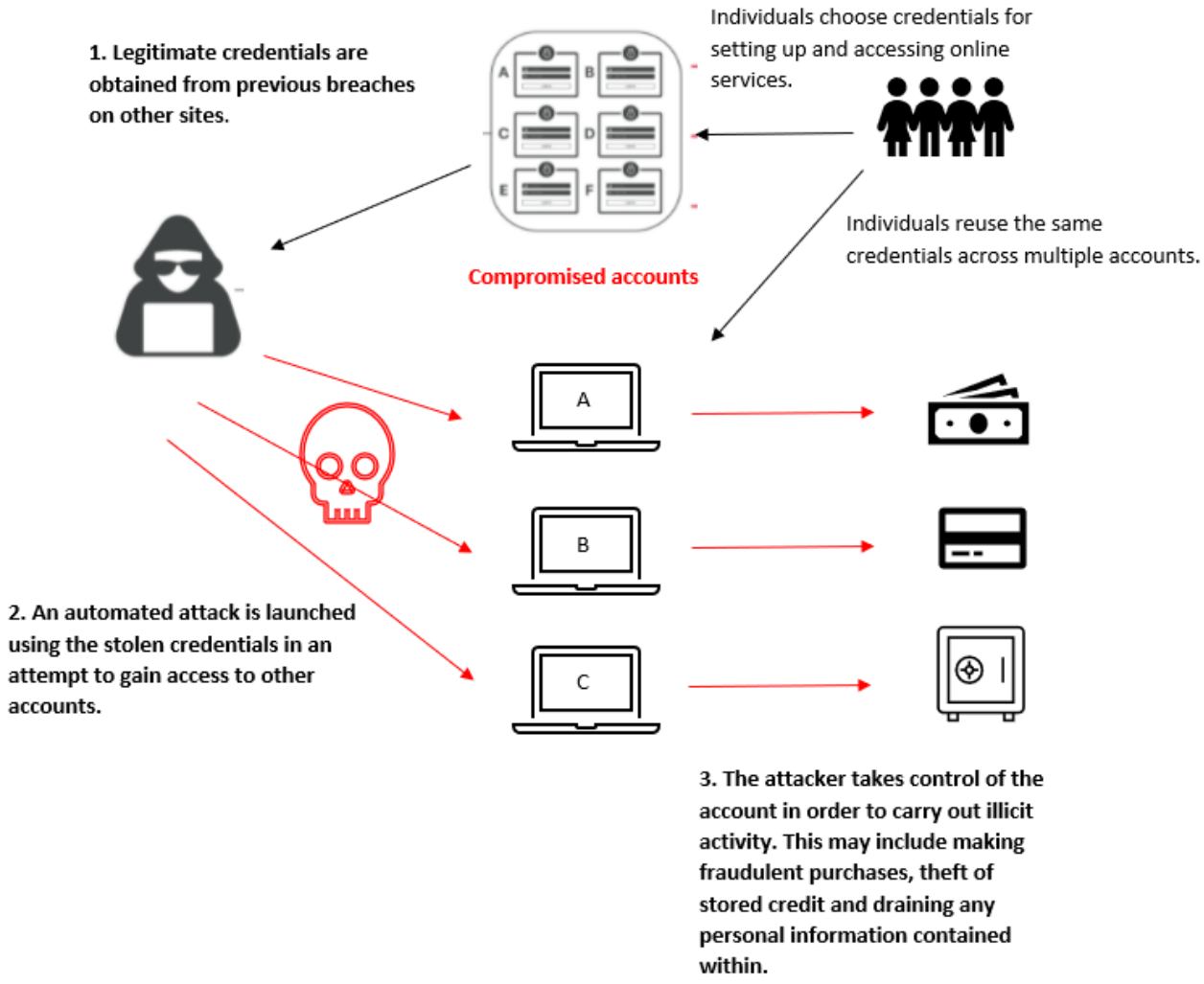
[11] Ibid.

(a) **Obtain legitimate credentials:** The attacker obtains a large quantity of leaked usernames/email addresses and passwords. Whilst an attacker may pay to obtain such credentials, a recent study found that there are more than 15 billion credentials being freely shared online, as a result of more than 100,000 different breaches[12].

(b) **Launch the attack:** The attacker acquires an 'account checker' tool, which subsequently launches automated bots to target online sites in an attempt to gain access to accounts within those sites. It is due to the automated nature of such attacks that the attacker can attempt to access large numbers of accounts at great speed. Some tools enable the bots to bypass a site's security, with some even able to successfully complete CAPTCHAs.[13]

(c) **Successful takeover:** The 'account checker' tool will test all available credentials and notify the attacker of those that have been successful. This will allow the attacker to take control of the account.

Figure 1:



[12] Digital Shadows Photon Research Team, 'From Exposure to Takeover: The 15 billion stolen credentials allowing account takeover': https://resources.digitalshadows.com/whitepapers-and-reports/from-exposure-to-takeover accessed 27 January 2022.

[13] CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart.

As is evident from Figure 1 above, user accounts on any website requiring an online log-in are potentially susceptible to credential stuffing attacks, and successful attacks that remain undetected may leave users and other organisations at risk of future attacks in respect of other accounts that use the same compromised credentials. The result is a risk of a 'domino effect' of data breaches.

3. Why are credential stuffing attacks carried out?

The primary motivation for this type of cyber-attack is financial gain. In particular, and as noted above, the perpetrator is potentially able to make fraudulent purchases using the compromised account, transfer funds to their own account, 'drain' the account of any stored credit, copy bank account information, as well as selling any personal data within the compromised account for further profit along with the 'used' credentials. The acquiring of financial information such as credit card details could also result in identify theft, this being a secondary motive for the carrying out of said attacks.[14]

Whilst credential stuffing attacks are predominantly financially motivated, attackers may also seek to cause more intangible harm to the account holder. For example, attackers may leak sensitive personal information on a public domain in an attempt to cause reputational damage to organisations or prominent public figures. Upon gaining access to a business account, an attacker may attempt to utilise 'user privileges' to infiltrate an organisation's internal network to carry out more serious cyber-attacks[15]. Additionally, an attacker may also use a compromised business account to pose as a known source sending out 'legitimate' requests to unsuspecting members of staff or external vendors and stakeholders. This is known as Business Email Compromise (BEC).[16]

Reports online indicate that large volumes of valid credential lists are being traded online at a growing rate.[17] Further, 'step-by-step' tutorials (e.g. YouTube videos) on how to carry out effective credential stuffing attacks are also available online, particularly within the media, online gaming and entertainment sectors.[18]

With this growing prevalence in mind, the following list identifies some of the catalysts behind the rise in credential stuffing attacks:

(a) 'Username and password' combinations are a simple and universal means used to set up and access online accounts.

[14] NCSC, 'Use of credential stuffing tools': https://www.ncsc.gov.uk/news/use-credential-stuffing-tools accessed 25 May 2021.

[15] NCSC, 'Preventing lateral movement': https://www.ncsc.gov.uk/guidance/preventing-lateral-movement accessed 23 November 2021.

[16] Federal Bureau of Investigation (FBI), 'Scams and safety: Business email compromise': https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise accessed 08 February 2022.

[17] Cloudflare, 'What Is Credential Stuffing?': https://www.cloudflare.com/learning/bots/what-is-credential-stuffing/ accessed 25 May 2021; ComputerWeekly.com, 'Over 15 billion credentials for sale on dark web': https://www.computerweekly.com/news/252485713/Over-15-billion-credentials-for-sale-on-dark-web accessed 25 May 2021.

[18] Akamai, *[State of the Internet]/security credential stuffing: attacks and economies* (vol. 5 | 2019) | p 5-6.

Almost all websites requiring a user to create an account require an individual to create a username, which is often an email address, and to create a password. Without the use of multi-factor authentication, user accounts are left open to these types of attacks.

(b) The tendency to reuse the same password across multiple accounts.

In view of this ubiquitous requirement to create a password for each online service, it becomes more difficult for individuals to come up with and remember each password that they set. For this reason, the same password is often reused by individuals across multiple applications and accounts. In an online security survey carried out by Google in 2019[19], 52% of people admitted to reusing the same password for multiple accounts and 13% of people confirmed that they use the same password for **all** of their accounts.

(c) The occurrence of 'mega breaches'.

In recent years, a number of so-called 'mega breaches' have occurred, which has resulted in the exposure of billions of credentials. One of the most well-known attacks occurred in August 2013[20] whereby Yahoo fell victim to a credential stuffing attack and reported that at least 1 billion accounts were compromised resulting in the theft, unauthorized access, and acquisition of hundreds of millions of its users' data, including usernames, birthdates, and telephone numbers[21]. In 2017, it was confirmed that this attack likely affected all three billion of Yahoo's users[22].

(d) The low cost to launch an attack compared with the high return.

Reports suggest that credential stuffing attacks typically have a success rate of 0.2 to 2%[23]. Whilst this rate may appear low, the threat is high given the large scale of credential stuffing attacks. For example, private sector research identified 55 billion credential stuffing attacks in the gaming industry between November 2017 and March 2019[24], equating to over 3,000 million attacks per month and over 107 million attacks per day. Further research identified 193 billion credential stuffing attacks globally during 2020[25], which equates to over 16,000 billion attacks per month and over 500 million attacks per day.

If an attacker obtains credentials, at very little cost, they may be able to access a significant number of accounts, which the attacker can 'drain' for themselves, and they can profit further from selling the 'used' credentials.

(e) Attackers have a significant amount of time to carry out their attacks.

Attackers have a significant amount of time to carry out their attacks as there is a substantial delay between an incident and detection. In 2018, it was reported that it took on average 15 months for an organisation to

[19] Google, 'Online Security Survey': https://services.google.com/fh/files/blogs/google_security_infographic.pdf accessed 25 May 2021.

[20] Although the breach occurred in 2013 it was not reported by Yahoo until 2016.

[21] *US Securities and Exchange Commission v Altaba Inc., f/d/b/a Yahoo!* (2018): https://www.sec.gov/litigation/admin/2018/33-10485.pdf accessed 08 February 2022.

[22] BBC News, 'Yahoo 2013 data breach hit 'all three billion accounts': https://www.bbc.com/news/business-41493494 Accessed 23 November 2021

[23] Shape Security, *Attacker Economics* (2020).

[24] Akamai, *[State of the Internet]/ security web attacks and gaming abuse*, (vol. 5 issue 3 | 2019).

[25] Akamai, *[State of the Internet] phishing for finance* (vol. 7 issue 2 | 2021).

discover a security incident stemming from credential stuffing and inform its users[26]. Although research suggests that there have been improvements over the last three years, it is reported that a delay nevertheless still exists[27]. Therefore, such delays provide the attackers with plenty of time to exploit the stolen credentials.

[26] Shape Security, *The 2018 credential spill report* (2018) | p 6-7 and 14.

[27] F5, '2021 Credential Stuffing Report': https://www.f5.com/labs/articles/threat-intelligence/2021-credential-stuffing-report accessed 08 February 2022.

4. Growing global concerns

This section identifies reports from public and private sectors, along with example cases that illustrate the global concerns regarding this method of cyber-attack.

(a) Reports from the public bodies:

(i) **The European Union Agency for Cybersecurity (ENISA)** published a report on the "Main incidents in the EU and worldwide" from January 2019 to April 2020[28], from which the following is noted –

- *"the amount of stolen financial information and user credentials is growing."*
- *"During 2019, the techniques used most frequently to start a cyberattack include brute force with stolen credentials, social engineering, configuration errors and exploitation of web applications."*
- *"Companies experience an average of 12 credential-stuffing attacks each month, wherein the attacker is able to identify valid credentials."*

(ii) **The Federal Bureau of Investigations (FBI)** in the USA issued an alert in September 2020[29] warning the financial services industry about cyber risks from credential stuffing threats. The alert noted that –

- Since 2017 the technique had led to *"nearly 50,000 account compromises"* in the sector which has resulted in financial costs to individuals and businesses.
- *"Credential stuffing accounted for the greatest volume of security incidents against the financial sector at 41 percent of total incidents".*

(iii) **The Securities and Exchange Commission's Office of Compliance Inspectors and Examinations (OIEC)** issued a risk alert[30] on credential stuffing on 15th September 2020, warning about a rise in said attacks.

(iv) **The UK National Cyber Security Centre (NCSC)** released an alert advisory notice in November 2018 in relation to credential stuffing[31].

(b) Reports from the private sector:

[28] European Union Agency For Cybersecurity (ENISA), 'Main Incidents in the EU and worldwide January 2019 to April 2020': https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents accessed 25 May 2021.

[29] Federal Bureau of Investigation (FBI), 'Private Industry Notification 20200910-001': https://www.ic3.gov/media/news/2020/200929-1.pdf accessed 25 May 2021.

[30] Office of Compliance Inspections and Examinations Officers, 'Cybersecurity: Safeguarding Client Accounts against Credential Compromise': https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf accessed 25 May 2021.

[31] NCSC, 'Use of credential stuffing tools': https://www.ncsc.gov.uk/news/use-credential-stuffing-tools accessed 25 May 2021.

(i) In 2019, **Verizon's data breach report**, revealed that 29 percent of breaches involve the use of stolen credentials, with a high volume of attacks from credential stuffing[32].

(ii) According to a report by **Shape Security** in 2017, 2.3 billion credentials were reported compromised. In terms of costs, Shape Security estimated losses at $300M, $400M, $1.7B and $6B on the airline, hotel, consumer banking, and retail industries, respectively, per year[33].

(iii) Cyber-security company **Akamai** identified 193 billion credential stuffing attacks globally during 2020[34].

[32] Verizon, '2019 Data Breach Investigations Report': https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf accessed 25 May 2021.

[33] Shape Security, '*The 2018 credential spill report*' (2018) | p 25.

[34] Akamai, *[State of the Internet] phishing for finance* (vol. 7 issue 2 | 2021).

5. Examples of credential stuffing cases

TaxSlayer

In 2017, the Federal Trade Commission (FTC) in the USA took action against TaxSlayer for violating data security requirements which resulted in attackers gaining full access to almost 9,000 TaxSlayer accounts between October and December 2015, allowing them to obtain tax refunds by completing fraudulent tax returns.[35]

The FTC found that TaxSlayer failed to implement adequate risk-based authentication measures that would have helped reduce the chances of an attack from hackers who had used stolen credentials to gain access to TaxSlayer customer accounts, according to the complaint. In this respect, the FTC charged TaxSlayer with violating the Gramm-Leach-Bliley Act's Safeguards Rule, which requires financial institutions to implement safeguards to protect the security, confidentiality and integrity of customer information, and the Privacy Rule, which requires financial institutions to deliver privacy notices to customers[36].

Dunkin' Brands, Inc.

In 2019, the New York Attorney General's (NY AG's) office filed a complaint[37] against Dunkin' Brands, Inc. (Dunkin') for failing to act in respect of successful cyberattacks (including credential stuffing attacks).

The attacks dated back to 2015, when a series of credential stuffing attacks were able to compromise tens of thousands of customers' accounts[38]. Many of the accounts held Dunkin' stored value cards which, once compromised, were re-sold online or used by the attacker to make fraudulent purchases. Consequently, tens of thousands of dollars were stolen from customers' Dunkin' cards. The investigation found that Dunkin' was made aware of the attacks by a third-party app developer, who even provided Dunkin' with a list of almost 20,000 customer accounts that had been compromised by attackers over a five-day sample period. However, Dunkin' *"failed to take any action"*[39].

Attacks continued during 2018, when a vendor notified Dunkin' that over 300,000 customer accounts had been accessed[40]. While Dunkin' contacted affected customers in this instance, Dunkin' failed to inform them that their accounts had been accessed without authorisation, and instead stated that a third party had unsuccessfully *"attempted"*[41] to access their accounts.

---

[35] Federal Trade Commission (FTC), 'Operator of online tax preparation service agrees to settle FTC charges that it violated financial privacy and security rules': https://www.ftc.gov/news-events/press-releases/2017/08/operator-online-tax-preparation-service-agrees-settle-ftc-charges accessed 25 May 2021; FTC, Taxslayer Complaint, Docket NO. C-1623063': https://www.ftc.gov/system/files/documents/cases/1623063_taxslayer_complaint.pdf accessed 25 May 2021; FTC, 'Taxslayer Decision and Order, Docket NO. C-1623063': https://www.ftc.gov/system/files/documents/cases/1623063_taxslayer_decision_and_order.pdf accessed 25 May 2021.

[36] Ibid.

[37] *The People of the State of New York by Letitia James, Attorney General of the State of New York v Dunkin' Brands, Inc* (2019) Complaint Index No. 451787/2019: https://ag.ny.gov/sites/default/files/dunkin_complaint.pdf accessed 08 February 2022.

[38] Ibid, para 4.

[39] Ibid, para 7.

[40] Ibid, para 64.

[41] Ibid, para 68.

In 2020, Dunkin' settled the lawsuit. The settlement required Dunkin' to notify customers impacted by the attacks, reset those customers' passwords and provide refunds for unauthorised use of customers' stored value cards. Dunkin' was also required to implement appropriate measures to protect against future attacks, adhere to incident response procedures when attacks occur, and pay $650,000 in penalties and costs to the state of New York[42].

Uber

In 2018, Uber was fined £385,000 by the UK Information Commissioner's Office (ICO) for failing to protect customers' personal information from a credential stuffing attack during October and November 2016[43]. The ICO confirmed that a number of *"avoidable data security flaws"* had allowed the attackers to expose the personal details of 2.7 million UK customers, including full names, email addresses and phone numbers along with the records of an estimated 82,000 UK drivers, including payment and journey details[44]. During the ICO's investigation, it was established that Uber had not informed its customers for over a year as they had paid the attackers $100,000 to destroy the data they had obtained[45].

[42] *The People of the State of New York by Letitia James, Attorney General of the State of New York v Dunkin' Brands, Inc* (2020) Judgement and Consent Order Index No. 451787/2019, paras 4-19: https://ag.ny.gov/sites/default/files/proposed_consent_order_and_judgment.pdf accessed 08 February 2022.

[43] UK Information Commissioner's Office (ICO), 'ICO fines Uber £385,000 over data protection failings': https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/ico-fines-uber-385-000-over-data-protection-failings/ accessed 25 May 2021.

[44] Ibid.

[45] Ibid.

6. Data security in privacy and data protection law

Data security requirements in data protection and privacy law are typically general in nature and do not include requirements that are specific to the protection of data from credential stuffing. For example, the EU General Data Protection Regulation 2016/679 (GDPR) specifies that organisations should process data in a manner that *"ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss…"*[46]. The 'Safeguards Rule' in the USA refers to the implementation of "*administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of the customer information at issue…*" and to "*protect against unauthorised access*"[47].

Both examples refer to the implementation of "*appropriate"* security and the protection against unauthorised processing/access. Given the evident threat to personal data from credential stuffing attacks (particularly to organisations with user accounts that may be accessed online), and the unauthorised processing/access that could result, the implementation of measures to protect personal data from credential stuffing attacks will generally be required, at least implicitly, under data protection and privacy laws. The measures detailed in these guidelines are not a statement of legal requirements, but can assist organisations in meeting their legal obligations across jurisdictions.

Notwithstanding the abovementioned general requirements, more specific regulations are possible to address specific security concerns. For example, the Federal Trade Commission updated the 'Safeguards Rule' in 2021 which, amongst other amendments, provides more detailed requirements on safeguards that must be implemented by financial institutions to protect personal data from cyberattacks. This includes the adoption of multi-factor authentication, access controls, encryption and designating a *"Qualified Individual"* to be responsible for the overseeing, implementing, and reinforcing of an organisation's IT security program[48].

[46] Article 5(1)(f) of the GDPR: https://eur-lex.europa.eu/eli/reg/2016/679/oj accessed 25 May 2021.

[47] Electronic Code of Federal Regulations, 'Safeguards Rule s314, Standards for safeguarding customer information' : https://www.ecfr.gov/current/title-16/part-314 accessed 22 November 2021.

[48] Ibid.

7. Measures to detect, prevent and/or mitigate the risk from credential stuffing

Having recognised and established the threat to personal data from credential stuffing attacks, which for many organisations is now no longer simply a 'threat' but an unavoidable reality, organisations should implement measures to mitigate the risks of, and arising from, said attacks.

The nature of a credential stuffing attack (i.e., that a malicious actor is using valid credentials) can make it difficult for organisations to defend their customers effectively against such attacks. However, several measures can be implemented in attempts to detect, prevent, and mitigate the risk from credential stuffing attacks. This section includes a list of measures that are recognised as being relevant and recommended to mitigate the risks arising from credential stuffing.

The list may serve as guidance for organisations on the measures that they should consider implementing to protect against credential stuffing. Equally, the list may also serve as a useful benchmark for authorities to assess an organisation's measures to protect against credential stuffing. However, data protection and privacy law is typically flexible in that it often adopts a risk-based approach[49] to security. An organisation is therefore not necessarily expected to implement all the measures that will be explained in further detail below, as every processing activity is different and will require different approaches and/or levels of security. Importantly, an organisation should be able to demonstrate that it has appropriate and effective measures and be able to justify decisions not to implement measures that are recognised as being relevant to protect against credential stuffing.

(a) Guest Checkout

The website of an organisations could allow for 'guest checkout' where possible. This would allow and/or encourage individuals to use the service without having to create an account, subsequently lowering the risk of credential reuse and credential stuffing cyber-attacks.

(b) Passwords

The continual growth in online services that require individuals to create online accounts often results in individuals reusing the same username and password combinations across multiple accounts. It is this 'defaulting' to the same credentials that cyber-criminals rely on to carry out successful credential stuffing attacks. When considering the application of a password system, there are various considerations that organisations should take into account, including but not limited to, the following –

(i) Password protection[50]

Passwords should never be stored in plaintext, and instead, a specifically designed password hashing algorithm should be implemented to securely store passwords[51]. Importantly, passwords

[49] For example, Article 32 of the GDPR and Recital 76 on risk assessment: https://eur-lex.europa.eu/eli/reg/2016/679/oj accessed 25 May 2021.

[50] Office of Compliance Inspections and Examinations Officers, 'Cybersecurity: safeguarding client accounts against credential compromise': https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf accessed 25 May 2021.

[51] ICO, 'Passwords in online services': https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/passwords-in-online-services/ accessed 25 May 2021.

should be hashed rather than encrypted as it is extremely difficult (if not impossible) to reverse a hash and reveal the original text, whereas encryption is a two-way function that can be a futile measure if the decryption key is not kept secure.

Although a hash is generally irreversible, in some circumstances it is possible to 'crack'[52] a hash and expose the underlying password. Therefore, applications should add a 'salt'[53] to a password before hashing. This makes it more difficult for an attacker to gain access to a user's credentials as the salt is unique to every user, which results in the attacker having to crack one hash at a time, which significantly increases the time and effort to do so.

It is important that organisations undertake regular reviews of the hashing algorithm they decide to use as such techniques can quickly become outdated, and therefore less secure, given the rapid advances in technology. Organisations should replace any hashing algorithms that become obsolete to prevent any security weaknesses from being exploited.

(ii) Enforce strong password policies[54]

When implementing a password system, there are three requirements that should be considered:

(1) Password length – In order to set a strong password, it should contain a minimum number of characters, to avoid short and weak passwords. A maximum password should not be set too low, or at all, so as to allow users to create longer passwords or passphrases.

(2) Special characters – Users should be allowed to include special characters. However, users should not be **required** to do so as this can often make it difficult for users to remember their passwords, which may encourage the re-use of the same passwords.[55]

(3) Password 'deny lists' – A 'deny list' prevents users from creating a commonly used, and therefore easily guessed, or weak, password by denying the user from creating the following passwords:

- Passwords exposed by previous breaches (see "identifying leaked passwords" section).
- Repetitive or sequential characters (e.g. 12345).
- Words or phrases that relate to the service (e.g. 'payroll' as a password to log-in to a staff payroll application).

[52] A hash is 'cracked' by an attacker taking a guess at what the password could be and then hashing this to compare the value to the actual hashed password. If they match, then the hash is considered to have been 'cracked'.

[53] A salt is a unique, randomly generated sequence of characters that is added to each password as part of the hashing process.

[54] Office of Compliance Inspections and Examinations Officers, 'Cybersecurity: safeguarding client accounts against credential compromise': https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf accessed 25 May 2021; Norway National Security Authority, 'Password Recommendations': https://nsm.no/aktuelt/passordanbefalinger-fra-nasjonal-sikkerhetsmyndighet accessed 27 April 2022.

[55] NCSC, 'Password administration for system owners': https://www.ncsc.gov.uk/collection/passwords/updating-your-approach accessed 25 May 2021.

Organisations can incorporate a password 'deny list' into their software or they can create their own by obtaining published lists of common passwords available on publicly available websites[56].

(iii) Provide education and assistance for users[57]

Users are often overburdened with creating and remembering passwords. Organisations should assist and provide guidance to their users in order to help them manage this.

Upon creating any new account requiring a password, users should be informed of the risks involved in using the same password across multiple sites, including the importance of avoiding using easily guessed passwords, such as names, pets and sports teams.

Organisations may also recommend the NCSC's technique of using 'three random words', which is considered a compromise between security and usability as it involves choosing three random words that are memorable to a user, but difficult for an attacker to guess[58]. It is important that these words are completely random such as "teahousefish" and not common phrases, famous quotations, song lyrics or predictable patterns such as "onetwothree"[59].

Organisations may also recommend the use of a password manager[60], which not only creates strong, unique passwords, but also acts as a password 'vault' by storing credentials for different websites, applications and services[61]. In particular, where 'high privilege' credentials are used, a robust password vault, 'Privilege Access Management' (PAM) solution, should be used. PAM requires additional authentication and provides more control over access and permissions for accounts, processes and systems which can mitigate the risk of both external attacks and internal malfeasance[62].

Organisations enabling the use of password managers must ensure that their use is supported on all current and intended platforms and that it is compatible with all current and intended browsers. Password managers that cannot be enabled across different devices may force users to use an alternative, less secure password management approach.

(iv) Other considerations

---

[56] For example, www.haveibeenpwned.com accessed 25 May 2021.

[57] NCSC, 'Password administration for system owners': https://www.ncsc.gov.uk/collection/passwords/updating-your-approach accessed 25 May 2021; Office of Compliance Inspections and Examinations Officers, 'Cybersecurity: safeguarding client accounts against credential compromise': https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf accessed 25 May 2021.

[58] NCSC, 'Three random words or #thinkrandom': https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0 accessed 27 May 2021.

[59] Ibid.

[60] Canadian Centre for Cyber Security, 'Password Managers - Security': https://cyber.gc.ca/en/guidance/password-managers-security-itsap30025 accessed 27 May 2021.

[61] Although password managers are beneficial in helping them cope with password 'overload', there are also risks involved. The biggest risk is that, if an attacker is able to access the password manager, all passwords stored within will be compromised.

[62] NCSC, 'Secure system administration: Use privileged access management': https://www.ncsc.gov.uk/collection/secure-system-administration/use-privileged-access-management accessed 08 February 2022.

Aside from the above, users should not be further restricted when creating a password as this may have a negative impact[63]. For example, enforcing regular password changes can lead to predictable changes such as sequentially increasing a number, for example from *Johnsmith1* to *Johnsmith2* etc. This can result in a user changing their original strong password to a series of weaker passwords. In this respect, it is recommended to only require a password reset if there has been a data breach whereby an account may have been compromised, or upon receiving other information suggesting the same[64].

An alternative to enforcing regular password updates would be to automatically 'lock' accounts that have been inactive for a specified period of time and encourage users to engage with the organisation directly if they have noticed suspicious activity on their account.

(c) Alternatives to passwords[65]

Before implementing a password-based system, it is important to consider whether such a system is appropriate or whether there are any alternatives. One alternative is the use of a single sign-on system (SSO), which is often a web-based portal that allows users to enter one set of credentials and gain access to multiple applications and/or services.

An SSO can be beneficial in reducing the number of passwords that a user has to create and remember. However, if compromised, an attacker would have access to **all** systems and services and may be able to exploit far more information. In this respect, if an organisation decides to implement an SSO, MFA should be a requirement for all user accounts.

Another alternative is to implement functions such as 'Hide My Email'. This allows a user to create accounts on an app or website using random, unique email addresses that automatically forward any emails to a user's personal inbox. A user is able to read and respond directly to these emails whilst obfuscating their personal email.

(d) Multi-factor authentication (MFA)[66]

MFA means that more than one identifying factor is required for an individual to gain access to their account. MFA is considered to be the most effective measure in securing online accounts against credential stuffing, due to the requirement of an additional factor, or factors, which can prevent an

[63] ICO, 'Passwords in online services': https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/passwords-in-online-services/ accessed 25 May 2021.

[64] Ibid.

[65] Ibid.

[66] OWASP, 'Credential Stuffing Prevention Cheat Sheet': https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html accessed 25 May 2021; NCSC, 'Use of credential stuffing tools': https://www.ncsc.gov.uk/news/use-credential-stuffing-tools accessed 25 May 2021; Canadian Centre for Cyber Security, 'Statement on GCKey Credential Service and recent credential stuffing attacks': https://cyber.gc.ca/en/news/statement-gckey-credential-service-and-recent-credential-stuffing-attacks accessed 25 May 2021; FTC, 'Stick with Security: Require secure passwords and authentication': https://www.ftc.gov/news-events/blogs/business-blog/2017/08/stick-security-require-secure-passwords-authentication accessed 25 May 2021; Office of Compliance Inspections and Examinations Officers 'Cybersecurity: safeguarding client accounts against credential compromise': https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf accessed 25 May 2021.

attacker from gaining access when a password has been compromised[67]. Analysis by Microsoft suggests that MFA would stop virtually all credential stuffing attack account compromises.[68]

In addition to preventing initial access, the implementation of MFA can limit an attacker from gaining **further** access, should they infiltrate an internal network. This is known as 'lateral movement'[69] and refers to the techniques deployed by an attacker to navigate through a network or gain privileged access whilst appearing as a legitimate user. Their end goal once inside a compromised network may be to take over a domain controller, sabotage a critical system or exfiltrate sensitive/ valuable personal data. Whilst this activity can be difficult to detect due to appearing as 'normal' traffic, implementing MFA for access to internal systems, applications and data can limit, or even prevent, lateral movement[70].

Typically, the additional factor(s) will be something the individual *has* and may require a biometric print (e.g. a fingerprint) or the inputting of a passcode which has been sent to an alternative communication channel such as a secondary email address, phone number or device.[71] In addition, there are other devices such as smart cards or 'tokens' which authenticate a user by generating a one-time PIN that must be entered or that contain a chip that authenticates with the system.[72]

In view of the threat posed to personal data from credential stuffing attacks, the state of the art and the relatively low cost of implementation, MFA should be considered as an essential security measure. Whilst the use of MFA may not be practical in all situations, it should be implemented wherever possible. In some cases, MFA may be optional, however for any accounts that contain sensitive information, or external cloud-based accounts, MFA should be mandatory.[73]

In addition to providing the option, or enforcing the use, of MFA at the point of account creation, organisations can also enable risk-based MFA to implement a balanced approach to security, which triggers the need for MFA in suspicious circumstances, such as a log-in from[74]:

- A new browser/device or IP address.
- An unusual country or location.
- Specific countries that are considered untrusted.
- An IP address that appears on known block lists.

---

[67] NCSC, 'Top tips for staying secure online': https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/activate-two-factor-authentication-on-your-email accessed 25 May 2021.

[68] Microsoft, 'Your Pa$$word doesn't matter': https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984 accessed 25 May 2021.

[69] NCSC, 'Preventing lateral movement': https://www.ncsc.gov.uk/guidance/preventing-lateral-movement accessed 15 October 2021.

[70] Ibid.

[71] Ireland Data Protection Commission, 'Know your obligations - data security': https://www.dataprotection.ie/en/organisations/know-your-obligations/data-security-guidance accessed 25 May 2021.

[72] Ibid.

[73] NCSC, 'Multi-factor authentication for online services': https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services accessed 25 May 2021.

[74] OWASP, 'Credential Stuffing Prevention Cheat Sheet': https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html accessed 25 May 2021.

- An IP address that has tried to log-in to multiple accounts.
- A log-in attempt that appears to be scripted rather than manual.

While there are many forms of MFA to take advantage of, it is important to acknowledge the differences between different MFA methods and the need to ensure that these are implemented appropriately, with regular reviews to ensure that they provide effective security from attackers.

(e) Secondary passwords and PINs[75]

Users may be prompted to provide additional security information, such as a PIN or specific characters from a secondary password. This measure adds an extra layer of protection where MFA cannot be implemented.

(f) Device fingerprinting[76]

Various attributes that are "visible" from a device's connection can be used to fingerprint a device e.g. the operating system, browser and language (these can be obtained from the HTTP headers). Other features such as screen resolution, installed fonts and browser plugins can be obtained using javascript. The device fingerprint can then be used to flag a connection from an unknown/suspicious device. Additional measures can then be taken when there is a mismatch, as appropriate.

(g) Unpredictable usernames[77]

Credential stuffing attacks rely on both the password and username. Websites commonly use the email address as the username, and as most users will have a single email address they use for all their accounts, this makes the combination of an email address and password very effective for credential stuffing attacks.

Requiring users to create their own username when registering on the website makes it harder for an attacker to obtain valid username and password pairs for credential stuffing. Providing the user with a generated username, or with guidance on how to create a custom username, can provide a higher degree of protection (as users are likely to choose the same username on most websites). However, care needs to be taken to ensure that the generated username is not predictable (such as being based on the user's full name, or sequential numeric IDs) and that it is not so complex that that user is unable to recall it, as this could result in a poor user experience and disengagement with the service.

(h) Identifying leaked passwords[78]

---

[75] Ibid.

[76] Ibid; Office of Compliance Inspections and Examinations Officers, 'Cybersecurity: safeguarding client accounts against credential compromise': https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf accessed 25 May 2021; NCSC, 'Use of credential stuffing tools': https://www.ncsc.gov.uk/news/use-credential-stuffing-tools accessed 25 May 2021.

[77] OWASP, 'Credential Stuffing Prevention Cheat Sheet': https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html accessed 25 May 2021.

[78] OWASP, 'Credential Stuffing Prevention Cheat Sheet': https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html accessed 25 May 2021; NCSC, 'Use of credential stuffing tools': https://www.ncsc.gov.uk/news/use-credential-stuffing-tools accessed 25 May 2021; Office of Compliance Inspections and Examinations Officers, 'Cybersecurity: safeguarding client accounts against

As well as checking a new user's chosen password against a list of known weak passwords, it can also be checked against passwords that have previously been breached. An example of a public service providing such lists is 'Pwned Passwords'[79]

(i) Rate limiting or 'throttling'[80]

This is a security measure devised to limit the number and frequency of multiple failed log-in attempts in the following ways:

- Limiting the number of connections from a single IP address. If multiple connections are made from one IP address, this could be the sign that a cyber-attack is underway, and therefore, limiting these connections can assist in blocking the attack.

- Limiting the number of failed log-in attempts within a certain period, also known as 'account lockout', whereby a user account will be 'frozen' for either a specified period of time or until the legitimate user contacts the organisation to reset their account. When using this method, 5 to 10 log-in attempts is recommended[81], to avoid a legitimate user accidentally locking their account. Organisations may consider exponential backoff algorithms to manage and limit log-in attempts and lockout.

(j) Log-in page and processes[82]

Most off-the-shelf tools are designed for a single step log-in process, where the credentials are posted to the server, and the response indicates whether or not the log-in attempt was successful. Adding steps to this process, such as requiring the username and password to be entered sequentially, or requiring that the user first obtains a random CSRF Token[83] before they can log-in, makes the attack slightly more difficult to perform, and doubles the number of requests that the attacker must make.

Given that many credential stuffing tools require site-specific configuration files, these can be rendered neutral by making small changes in the log-in pages once detected.

(k) Account monitoring/ detection[84]

---

credential compromise': https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf accessed 25 May 2021.

[79] 'Pwned Passwords': https://haveibeenpwned.com/Passwords accessed 25 May 2021.

[80] US National Institute of Standards and Technology (NIST), 'Digital Identity Guidelines': https://pages.nist.gov/800-63-3/sp800-63b.html#throttle accessed 25 May 2021.

[81] NCSC, 'Password administration for system owners': https://www.ncsc.gov.uk/collection/passwords/updating-your-approach accessed 25 May 2021.

[82]OWASP, 'Credential Stuffing Prevention Cheat Sheet': https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html accessed 25 May 2021; NCSC, 'Use of credential stuffing tools': https://www.ncsc.gov.uk/news/use-credential-stuffing-tools accessed 25 May 2021.

[83] OWASP, 'Cross- Site Request Forgery Prevention Cheat Sheet': https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html accessed 25 May 2021.

[84] Ibid; Office of Compliance Inspections and Examinations Officers, 'Cybersecurity: safeguarding client accounts against credential compromise': https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf accessed 25 May 2021; NCSC, 'Use of credential stuffing tools': https://www.ncsc.gov.uk/news/use-credential-stuffing-tools accessed 25 May 2021.

Account monitoring is often carried out alongside throttling or account lockout as a method of detecting any abnormal behavior that may be the sign of an attack. Organisations should establish, maintain and review indicators of suspicious activity, such as:

- Multiple failed attempted log-ins across multiple accounts.
- Higher than usual volumes of foreign Ips.
- Anomalies in browser activity such as headless browsers or browsers that lack JavaScript execution engines[85].
- Patterns in log-in attempts that indicate the use of automation.
- Failed attempts to log-in at the second stage of MFA.
- Log-in attempts from unusual IP addresses, including attempts from virtual private server providers, such as Amazon Web Service or commercial data centers[86].
- Unusually high number of account lockouts.

The above list should not be considered definitive as, for example, a log-in attempt from an unusual IP address may not always be indicative of an attack and could simply be that a user has gone on holiday or is using a VPN[87].

Advanced analytics should be used by organisations using data such as historical log-in details, location, device fingerprinting etc. to make a credibility judgement of a log-in request.

For most organisations, it is recommended that account monitoring be at least partially automated to provide consistent, comparable metrics and round-the-clock surveillance[88].

(l) Additional checks for anonymity networks[89]

Anonymity networks such as the TOR Project facilitate anonymous communication by concealing a user's IP address through encryption and a series of self-described anonymous and private connections. Although such networks can have legitimate uses, traffic can also be significantly

[85] Bureau of Internet and Technology (BIT) of the New York Attorney General's Office, 'Business Guide for Credential Stuffing Attacks': https://ag.ny.gov/sites/default/files/businessguide-credentialstuffingattacks.pdf accessed 27 January 2022.

[86] Ibid.

[87] A VPN is a Virtual Private Network which allows remote users to securely access an organisation's services.

[88] Bureau of Internet and Technology (BIT) of the New York Attorney General's Office, 'Business Guide for Credential Stuffing Attacks': https://ag.ny.gov/sites/default/files/businessguide-credentialstuffingattacks.pdf accessed 27 January

[89] NCSC, 'Use of credential stuffing tools':https://www.ncsc.gov.uk/news/use-credential-stuffing-tools accessed 25 May 2021.

malicious[90]. Therefore, additional checks should be carried out on authentication attempts from such networks[91].

(m) CAPTCHAs[92]

CAPTCHAs are puzzles or small challenges required to be completed before accessing an account. These are often used as a defence mechanism against cyber-attacks, as it is assumed that only a human will be able to solve/complete the challenge due to the requirement to often select or tick certain parts of a larger grid. Unfortunately, CAPTCHAs may not always be successful in preventing a credential stuffing attack due to the use of CAPTCHA farms and advances in computer software which can recognise and solve CAPTCHAs[93]. In this respect, the use of CAPTCHAs should only be considered as **part** of an organisation's security regime.

To improve usability, CAPTCHAs may be implemented so that they are only required when the log-in request is considered suspicious (see MFA section).

(n) Web Application Firewall (WAF) [94]

A firewall is essential when engaging in external activity to both other networks and to the internet. A correctly configured WAF can be key to blocking a credential stuffing attack as it can detect and prevent the use of automated programs and advanced 'bots'. A WAF can also detect whether stolen credentials are being used in a log-in attempt by comparing usernames and passwords against a known list of 'compromised' credentials. This allows organisations to prepare for a potential credential stuffing attack by monitoring where multiple log-in attempts have failed.

Due to the increase in both organisational and individual reliance on "always-on" internet connections, firewalls are of upmost importance given the increased exposure to cyber-attacks.

(o) IP block-listing[95]

A block-list denies a specified list of IP addresses, for example where the said IP addresses have been linked to malicious online activity such as being part of a botnet. This block-list will be uploaded into a WAF and will block any connection attempts made from an IP address on the list. However, it is important to note that block-listing may at times be ineffective against credential stuffing attacks as attackers will use botnets to distribute traffic from different IP addresses to appear as a legitimate

---

[90] Ibid.

[91] Ibid.

[92] OWASP, 'Credential Stuffing Prevention Cheat Sheet': https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html accessed 25 May 2021; Office of Compliance Inspections and Examinations Officers, 'Cybersecurity: safeguarding client accounts against credential compromise': https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf accessed 25 May 2021.

[93] OWASP, 'Credential Stuffing Prevention Cheat Sheet': https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html accessed 25 May 2021.

[94] Office of Compliance Inspections and Examinations Officers, 'Cybersecurity: safeguarding client accounts against credential compromise': https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf accessed 25 May 2021.

[95] OWASP, 'Credential Stuffing Prevention Cheat Sheet': https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html accessed 25 May 2021.

user. In this respect, even if one IP address is on the block-list, if an attacker was using 100 IP addresses, this would mean that he would still have 99 attempts to bypass this measure.

(p) Allow-listing 'good' IP addresses

In comparison to block-listing, allow-listing is specifying trusted IP addresses that will be uploaded into a WAF to grant them access, whilst any IP addresses that have not been included on the list, would be denied access. Allow-listing can be less effective than block-listing for 'standard' user accounts, as most domestic internet connections use dynamic IP addresses, meaning that over time, users will access their account from different IP addresses, which if not included on the allow list, would deny their access.

(q) Incident response plans and user notifications[96]

When suspicious activity is detected, it may be useful to notify or warn the user.

However, care should be taken so as not to overwhelm users with notifications as they may begin to ignore or delete them. In this respect, it would not be worthwhile to inform a user of a single failed log-in attempt, as this could simply be a legitimate user who has forgotten their password or spelt it incorrectly. However, if unusual activity has been detected on an account, for example a password had been correctly entered yet the subsequent MFA failed, it would be appropriate to contact the user as soon as possible so that their password can be changed, and importantly, to allow users to change the passwords of any other accounts secured with the same credentials, so as to prevent further attacks.

Users should also be provided with details related to recent log-ins to their accounts, such as date, time and location of previous log-in attempts, and wherever possible, users should be able to view all active sessions and terminate any which are illegitimate[97].

In certain circumstances, existing law may mandate the method, content and timing of notice, depending on the consequences of credential stuffing attacks. This guide should be interpreted in a manner that is consistent with those laws.

Organisations should also consider systematically monitoring user reports of fraud and unauthorised account access[98] which may indicate signs of a credential stuffing attack. For example, organisations should conduct regular and periodic reviews of fraud reports in order to detect spikes or patterns in activity. Organisations should also ensure that customer service teams are appropriately trained to recognise signs of credential stuffing attacks and are able to efficiently communicate any unusual or nefarious activity to information security teams, so as to prevent or mitigate incoming attacks.

[96] Ibid.

[97] Ibid.

[98] Bureau of Internet and Technology (BIT) of the New York Attorney General's Office, 'Business Guide for Credential Stuffing Attacks': https://ag.ny.gov/sites/default/files/businessguide-credentialstuffingattacks.pdf accessed 27 January