GRA

GIBRALTAR REGULATORY AUTHORITY

(26B) Credential Stuffing Raising Awareness

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 RAISING AWARENESS

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 guidance identifying the threat posed by credential stuffing to personal data and how the general public can protect themselves from associated risks.

The guidance is provided overleaf to assist the general public locally in preventing, detecting and mitigating the risks of credential stuffing attacks.

GPA
Global Privacy Assembly

International Enforcement Cooperation Working Group

Credential Stuffing Awareness Raising - 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
Summarised Guidance....8
1. Introduction....9
2. What is credential stuffing?....10
3. What are the risks of credential stuffing?....12
4. Why is credential stuffing such a problem?....13
5. Recommendations to the general public to reduce the risk of a credential stuffing attack. 14
Annex 1 – Top tips to protect against 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 will assist authorities address the rising threat of credential stuffing.

This document identifies the threat posed by credential stuffing to personal data and provides guidance for the general public on how they can protect themselves from associated risks.

The document serves as recognition of the global threat to personal data from credential stuffing, by the IEWG. The manner in which this document can support the work of an authority will be determined by each authority. For example, the guidance may – act as a point of reference for authorities, in the context of knowledge sharing; assist authorities when looking to issue guidance, a warning or notice on credential stuffing; and assist authorities in raising awareness as to how the general public can protect themselves from the risks of such 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 act 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

This guidance has benefited from, and incorporates, as appropriate, relevant material published by a range of organisations. The following list is intended to recognise and acknowledge the material used and referred to. References are also included throughout the document.

In addition to the material referred to below, this guidance has benefited 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)

Canadian Centre for Cyber Security

'Best practices for passphrases and passwords (ITSAP.30.032)'
https://cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032

'Password Managers' – Security (ITSAP.30.025)'
https://cyber.gc.ca/en/guidance/password-managers-security-itsap30025

'Rethink Your Password Habits to Protect Your Accounts from Hackers (ITSAP.30.036)'
https://cyber.gc.ca/en/guidance/rethink-your-password-habits-protect-your-accounts-hackers-itsap30036

'Secure your accounts and devices with multi-factor authentication (ITSAP.30.030)'
https://cyber.gc.ca/en/guidance/secure-your-accounts-and-devices-multi-factor-authentication-itsap30030

[2] The collaborative approach adopted allowed the working group to daw 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.

European Union Agency for Cybersecurity

'Authentication Methods'
https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/authentication-methods

'How to Avoid SIM-Swapping – Leaflet'
https://www.enisa.europa.eu/publications/how-to-avoid-sim-swapping-leaflet

F5

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

International Business Machines Corporation

'IBM Survey: Pandemic-Induced Digital Reliance Creates Lingering Security Side Effects'
https://newsroom.ibm.com/2021-06-15-IBM-Survey-Pandemic-Induced-Digital-Reliance-Creates-Lingering-Security-Side-Effects

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 Application Security Project

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

Ponemon Institute

Ponemon Institute, *The cost of credential stuffing* (Oct 2017)

Shape Security

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

Shape Security, *Attacker economics* (2020)

UK Information Commissioner's Office

‘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

‘Cyber Aware’
https://www.ncsc.gov.uk/cyberaware/home#action-1

‘Most hacked passwords revealed’
https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security

‘Paws-word change recommended on National Pet Day’
https://www.ncsc.gov.uk/news/national-pet-day-password-advice

‘Recovering a hacked account’
https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account

‘Setting up two-factor authentication (2FA)’
https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa

‘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

‘Top tips for staying secure online’
https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers

‘Top tips for staying secure online’
https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/use-a-strong-and-separate-password-for-email

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

‘Using passwords to protect your devices and data’
https://www.ncsc.gov.uk/information/infographics-ncs

US Cybersecurity and Infrastructure Security Agency

‘Security Tip (ST05-012) Supplementing passwords’
https://us-cert.cisa.gov/ncas/tips/ST05-012

US Federal Bureau of Investigation

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

US National Institute of Standards and Technology

‘Special Publication 800-63-3 Digital Identity Guidelines: 4.3.1 Authenticators’
https://pages.nist.gov/800-63-3/sp800-63-3.html#431-authenticators

Verizon

‘2021 data breach report’
https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf

Summarised Guidance

- Credential stuffing attacks rely on an individual's tendency to reuse the same log-in credentials (i.e. username and password) across multiple accounts.
- Passwords should **not be reused** in respect of multiple accounts. A strong **unique** password should be created for each online account, app and service.
- Do not use short passwords.
- **Users should not use predictable passwords**, such as those based on personal information e.g. a birthday or a pet's name.
- Users should consider using the **'three random words'** technique to help create memorable and strong passwords.
- Consider using a **'password manager'** to assist in securely storing and using separate passwords.
- **Multi-factor authentication** should be used where possible.
- If an online account has been compromised, the account holder should change the password **immediately** along with that for any other accounts protected by the same or similar password.
- **Users should routinely check account information** for unusual activity or unauthorised transactions, in particular if an account has been compromised or is suspected to have been compromised.
- The relevant financial institution should be contacted if there is a card or other financial information linked to an account that has been compromised or is suspected to have been compromised.
- **Users should contact the relevant organisation** if an account has been locked by an attacker.
- **Devices should be updated and patched regularly** to ensure the latest security software has been installed.

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 by data breaches and made available on the 'dark web'), to unlawfully access users' accounts on unrelated websites.

Successful credential stuffing attacks may result in financial loss, as attackers may, for example, make purchases using the compromised account or transfer funds to their own account. Such attacks may also be used to cause intangible harm such as reputational damage by spreading sensitive personal information, disinformation or making false statements about an individual whilst using their compromised account.

The 'reuse' of passwords may increase the chances of successful credential stuffing attacks and may be the means through which an attack on an organisation can occur, even when high levels of cyber security have been implemented.

Concerns surrounding password security have increased as the effects of the Covid-19 pandemic resulted in overnight changes to our working and personal life and an unprecedented shift towards online services. In the United Kingdom alone, 27% of the population created at least four new password protected accounts and 6% reported to have opened more than ten new accounts in the last 12 months[3]. Further, a global survey also found that individuals created 15 new accounts on average during the Covid-19 pandemic (equating to billions of new accounts created around the world), and 44% of said individuals reported that they do not plan to delete or deactivate these new accounts[4]. In addition, it was reported that more than half of the millennials surveyed would rather place an order using an app or website as opposed to calling or visiting a location in person[5].

As our reliance on digital services shows no sign of slowing, it appears that neither do the exploitative methods nor means used by cyber-criminals to carry out attacks on such services. Reports from both public and private sectors have cited credential stuffing as an increasingly significant issue, one which threatens personal data on a large[6] and global scale.

These guidelines serve as recognition of the global threat to personal data from credential stuffing, by the IEWG. The guidelines may be used by authorities to raise public awareness about the risks posed by credential stuffing and to advise the public on how they can protect themselves from said risks.

---

[3] UK National Cyber Security Centre (NCSC), 'Paws-word change recommended on National Pet Day': https://www.ncsc.gov.uk/news/national-pet-day-password-advice accessed 27 May 2021.

[4] International Business Machines Corporation **(**IBM), 'IBM Survey: Pandemic-Induced Digital Reliance Creates Lingering Security Side Effects': https://newsroom.ibm.com/2021-06-15-IBM-Survey-Pandemic-Induced-Digital-Reliance-Creates-Lingering-Security-Side-Effects accessed 29 July 2021.

[5] Ibid.

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

2. What is credential stuffing?

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.

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

(a) Obtain legitimate credentials: Legitimate credentials that have been previously leaked by data breaches[7] are made available, for example on the 'dark web'. Cyber-criminals purchase often large quantities of these credentials and attempt to unlawfully access user accounts on unrelated websites.

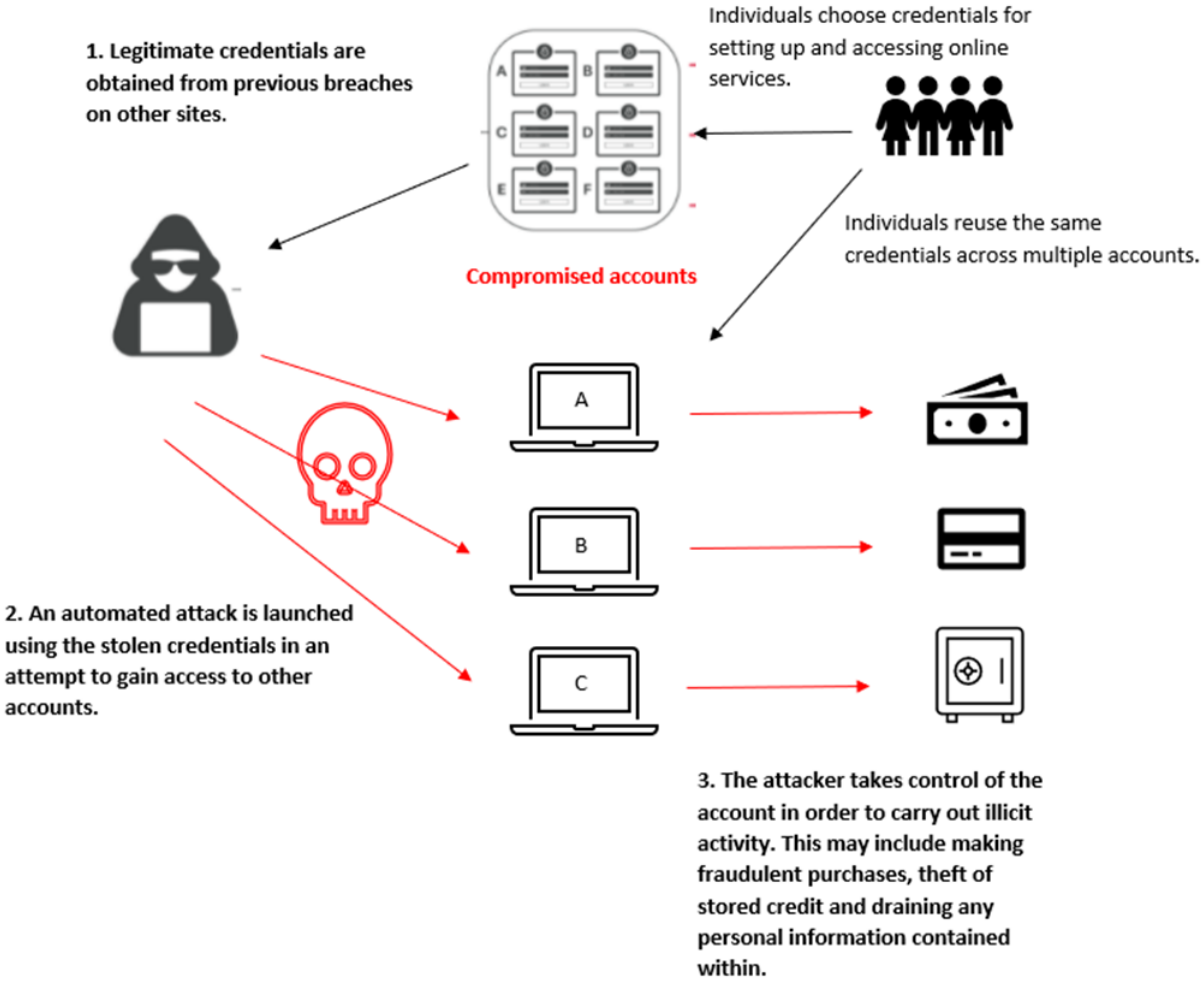
(b) Launch the attack: In order to launch a credential stuffing attack, tools that are typically automated such as botnets, which are groups of internet 'bots' coded with malicious software to 'obey' the attackers' commands, and 'account checker' tools are used to automatically insert the stolen credentials into the relevant fields across other websites[8].

(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 over' the account and for example, drain the account of any stored credit, make fraudulent purchases, copy bank account information, or access any available personal or other data.

[7] A data breach occurs when information held by an organisation is stolen or accessed without authorisation.

[8] Canadian Centre for Cyber Security, 'Rethink Your Password Habits to Protect Your Accounts from Hackers (ITSAP.30.036)': https://cyber.gc.ca/en/guidance/rethink-your-password-habits-protect-your-accounts-hackers-itsap30036 accessed 27 May 2021.

Figure 1:


1. Legitimate credentials are obtained from previous breaches on other sites.
Individuals choose credentials for setting up and accessing online services.
Compromised accounts
Individuals reuse the same credentials across multiple accounts.
A
B
C
2. An automated attack is launched using the stolen credentials in an attempt to gain access to other accounts.
3. The attacker takes control of the account in order to carry out illicit activity. This may include making fraudulent purchases, theft of stored credit and draining any personal information contained within.

3. What are the risks of credential stuffing?

Upon successfully gaining entry to an account, an attacker can use the information contained within to cause both **material** and **non-material** harm to individuals.

(a) Examples of material harm may include:

- Financial loss as attackers may make purchases using the compromised account, steal associated credit card/ bank account information, or transfer funds or accumulated loyalty points to their own personal account[9].

- Attackers may also attempt to capitalise on their gains by selling or posting online validated credentials, along with any personal data harvested from the account, making it available to other criminals who may subsequently commit fraud, identity theft or conduct other malicious activity[10].

(b) Examples of non-material harm may include:

- Emotional distress if the attacker, for example, makes false statements or spreads disinformation from a user's compromised account.

- Attackers may also leak sensitive personal information on a public domain which could cause reputational damage or affect an individual's personal relationships.

- A successful credential stuffing attack provides an attacker with unlimited access to **all** personal data within **each** compromised account which may include financial details, medical information or other types of sensitive data. This 'draining' of information can result in individuals feeling a 'loss of control' over their personal data.

[9] NCSC, 'Use of credential stuffing tools': https://www.ncsc.gov.uk/news/use-credential-stuffing-tools accessed 27 May 2021.

[10] Ibid.

4. Why is credential stuffing such a problem?

Due to the need to create a password for each online account, a dependence on memory and 'force of habit' often results in individuals choosing a password that can easily be remembered, such as a significant date or a pet's name[11], which they then reuse across multiple online accounts. According to a survey carried out by the UK's National Cyber Security Centre (NCSC) in 2019, individuals continue to use predictable and easily guessed passwords. The report discovered that there were 23.2 million victim accounts worldwide whereby a user had used '123456' as their password[12].

In addition, due to the validity of credentials, it can be difficult for organisations to differentiate between an attacker and a legitimate user, resulting in credential stuffing attacks often going unnoticed[13]. In 2018, it was reported that it took on average 15 months for an organisation to discover a security incident stemming from credential stuffing and inform its users[14]. Although research suggests that there have been improvements over the last three years, it is reported that a delay nevertheless still exists[15]. Therefore, if a compromised password has been used elsewhere, an attacker has plenty of time to carry out further attacks and attempt to access other vulnerable accounts.

Notably, compared with the minimal effort required to launch, the potential for financial gain is often significant, thereby making this type of attack attractive. Low-cost automated tools are readily available and relatively straightforward to use, allowing attackers to launch large scale attacks at great speed[16]. Reports suggest that credential stuffing attacks typically have a success rate of 0.2 to 2%[17]. 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[18], 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*[19]*, which equates to over 16,000 billion attacks per month and over 500 million attacks per day.*

[11] Results from an NCSC survey showed that 15% of people used a pet's name and 13% used a date of significance as their password. NCSC, 'Paws-word change recommended on National Pet Day': https://www.ncsc.gov.uk/news/national-pet-day-password-advice accessed 27 May 2021.

[12] NCSC, 'Most hacked passwords revealed': https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security accessed 27 May 2021.

[13] Ponemon Institute, *The cost of credential stuffing* (Oct 2017) p 2.

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

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

[16] NCSC, 'Use of credential stuffing tools': https://www.ncsc.gov.uk/news/use-credential-stuffing-tools accessed 27 May 2021.

[17] Shape Security, *Attacker economics* (2020).

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

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

5. Recommendations to the general public to reduce the risk of a credential stuffing attack.

The following provides guidance for individuals on the measures they can take to mitigate the risk of a credential stuffing attack.

PREVENTATIVE MEASURES

(a) Password creation.

When creating any new password, it is imperative that this is not shared with anyone else and it is **not reused**. Reusing passwords, even those considered 'strong', may leave an account just as vulnerable given that one compromised password may allow an attacker access to multiple accounts[20]. This is particularly important for any accounts which contain financial information, a lot of personal information or particularly sensitive information, as the repercussions could be significantly worse if the accounts were compromised.

Passwords remain a common form of account protection and, in order to ensure their effectiveness, users should avoid making common mistakes. In this respect, users should[21]:

- Avoid using predictable patterns such as "12345", "qwerty" or "password", even if they include the addition of special characters such as "Password1!".
- Avoid using personal details such as a birthday, sports team or pet's name.
- Avoid using words which relate to the service being provided such as the name of the respective bank to log-in to online banking.

Do not use short passwords[22]. Longer passwords are recognised as being more difficult for attackers to compromise[23].However, as technology develops, longer passwords may not always equal stronger passwords.

In this respect, the UK's National Cyber Security Centre recommends the '3 random words' technique. This technique is considered a compromise between security and usability as it involves choosing three random words which can be memorable to a user, but difficult for an attacker to guess[24]. It is important

[20]ENISA, 'Authentication Methods': https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/authentication-methods accessed 27 May 2021.

[21] Canadian Centre for Cyber Security, 'Best practices for passphrases and passwords (ITSAP.30.032)': https://cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032 accessed 27 May 2021.

[22]UK Information Commissioner's Office (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 27 May 2021; Norway National Security Authority, 'Password Recommendations': https://nsm.no/aktuelt/passordanbefalinger-fra-nasjonal-sikkerhetsmyndighet accessed 27 April 2022.

[23]European Union Agency for Cybersecurity (ENISA), 'Authentication Methods': https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/authentication-methods accessed 27 May 2021.

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

that these words are completely random such as "teahousefish" and not common phrases, famous quotations, song lyrics or predictable patterns such as "onetwothree"[25].

Adding special characters, numbers, or uppercase letters may make a password more difficult to 'crack', and therefore, would be helpful in preventing certain cyber-attacks. However, this may also make a password less memorable, which can be counterproductive in mitigating against credential stuffing attacks if users choose to reuse the same password over multiple accounts so that they do not need to remember more than one complex password.

Using a password manager can also assist in creating, storing and remembering strong, unique passwords as they promote the creation of complex passwords and discourage password reuse[26].

Email accounts in particular must be protected with a strong, unique password, as, once compromised, an attacker is able to abuse the 'forgot your password' feature and change the passwords to **all** other accounts linked to that email[27].

(b) Password protection.

Although it is important to create a strong password for each online account, it is equally important that, when passwords are stored, this is done securely.

Writing down a list of passwords is certainly not the most secure option, however, it is one way to manage multiple passwords. Should users opt to do this, it is vital that the list be kept in a secure place, ideally in a locked safe, **away** from the computer or device that the password has been created to protect[28]. Adding three random letters to the beginning and end of each password is another precaution that users can take to protect their passwords, should the list be discovered by an unauthorised party.

An alternative to keeping a handwritten list is to use a password manager, which not only creates strong, unique passwords, but also acts as a password 'vault' by storing credentials for different websites, applications and services[29]. Whilst password managers are beneficial in helping users cope with password 'overload', there may be risks. One of the biggest risks is that, if an attacker is able to access the password manager, all passwords stored within will be compromised. Therefore, multi-factor authentication (as detailed in point (c) below) should **always** be enabled and passwords that are required for more 'sensitive accounts', such as online banking, or those with administrative privileges such as emails, should not be stored within a password manager[30].

---

[25] Ibid.

[26] Canadian Centre for Cyber Security, 'Password Managers – Security': https://cyber.gc.ca/en/guidance/password-managers-security-itsap30025 accessed 17 March 2022.

[27] NCSC, 'Top tips for staying secure online': https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/use-a-strong-and-separate-password-for-email accessed 26 January 2022.

[28] NCSC, 'Using passwords to protect your devices and data': https://www.ncsc.gov.uk/information/infographics-ncsc accessed 27 May 2021.

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

[30] Ibid.

Another alternative is to store online passwords on a web browser using the 'remember me' function[31]. This removes the burden from the user as they are able to access the account using the saved password from any device where they are signed into the same web browser[32]. However, a password should never be saved on a public browser (e.g. at a library or internet café), as saved credentials could be exposed to unknown individuals. For shared computers with family members or housemates, it is also recommendable for each person to create their own account and ensure that they log out after each browsing session[33].

(c) Enable multi-factor authentication.

Multi-factor authentication (MFA) means that more than one identifying factor is required for an individual to gain access to an account. Although adding a second factor does in itself present varying advantages and associated risks, **setting up any type of MFA is a highly effective protective measure and is better than not having it at all**[34]. It is important to note that when MFA is used, the second factor is usually requested only after the correct username and password have been entered, meaning that an attacker will in that instance know the correct credentials of the account. At that point the attacker could then aim to compromise the second factor e.g. by sending a phishing message, and this is something that should be considered.

Examples of identifying factors that may be used, in addition to entering a password, passphrase or PIN, include the following:

- Receiving an SMS message or verification PIN on a mobile device. These codes can usually only be used once and become 'void' after use[35]. Wherever possible, avoid using SMS to receive one-time codes and consider using tools such as two factor authentication apps, due to known attacks against SMS known as 'SIM swap' attacks[36]. These attacks involve a hacker redirecting the phone number used to receive the SMS in order to access the second factor code without needing the physical phone.

- Requesting a phone call to a landline or mobile number.[37]

- Installing an 'authenticator app', such as Google Authenticator or Microsoft Authenticator, which can be used on smart phones and tablets for setting up two factor authentication on all accounts offering this as an option[38]. These types of apps can be more beneficial than text messages in that they do not require mobile signal or receipt of an SMS.

---

[31] Ibid.

[32] NCSC, 'Cyber Aware': https://www.ncsc.gov.uk/cyberaware/home#action-1 accessed 27 May 2021.

[33] NCSC, 'Top tips for staying secure online': https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers accessed 09 February 2022.

[34] NCSC, 'Setting up two-factor authentication (2FA)': https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa accessed 29 July 2021.

[35] US Cybersecurity and Infrastructure Security Agency, 'Security Tip (ST05-012) Supplementing passwords': https://us-cert.cisa.gov/ncas/tips/ST05-012 accessed 27 May 2021.

[36] ENISA, 'How to Avoid SIM-Swapping - Leaflet': https://www.enisa.europa.eu/publications/how-to-avoid-sim-swapping-leaflet accessed 07 March 2022.

[37] Ibid.

[38] NCSC, 'Setting up two-factor authentication (2FA)': https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa accessed 27 May 2021.

- Using a hardware token such as a 'security key', which is a small device that can be purchased and is plugged into a computer or laptop to authenticate a user account[39].

- A biometric characteristic provided by the user, such as a fingerprint, retina scan, facial or voice recognition.[40]

MFA is considered 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 attacker from gaining access when a password has been compromised[41]. Analysis by Microsoft suggests that MFA would stop virtually all (99%) credential stuffing attack account compromises.[42]

Some online services will automatically have MFA enabled whereas others will require a user to manually switch it on. The option to enable MFA is usually found within the security settings of an account. Note that other terms may be used to refer to an MFA feature, such as 'two-step verification', 'two-factor-authentication', '2FA' etc.[43], these being a subset of MFA.

There may be some online services that have an alternative to MFA, for example, allowing users to access an account after entering a memorable word or a set of security questions such as, 'What is your mother's maiden name?'. However, these measures **do not** offer the same level of protection as MFA, and are no longer considered to offer a secure means of account protection in today's threat environment[44].

It is recommended that users enable MFA specifically on email accounts and all accounts considered to be 'important'[45]. Email accounts are particularly attractive to attackers as access to a user's inbox allows them to reset passwords to other accounts or forward emails containing additional personal information to their own account[46]. Access to a business email account may allow an attacker to pose as the 'legitimate' account holder and send out scam emails in an attempt to defraud either an organisation or an individual. This is known as Business Email Compromise (BEC). Therefore, as an additional measure, all payment or purchase requests, as well as changes to payment details or procedures, should be verified in person or over the phone to ensure that the request is genuine. Caution should also be taken when actioning requests marked as 'urgent' or where the requester appears to be hurried.[47]

---

[39] Canadian Centre for Cyber Security, 'Secure your accounts and devices with multi-factor authentication (ITSAP.30.030)':https://cyber.gc.ca/en/guidance/secure-your-accounts-and-devices-multi-factor-authentication-itsap30030 accessed 27 May 2021.

[40] NCSC, 'Setting up two-factor authentication (2FA)': https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa accessed 27 May 2021.

[41] 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.

[42] 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.

[43] NCSC, 'Setting up two-factor authentication (2FA)': https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa accessed 27 May 2021.

[44] National Institute of Standards and Technology (NIST), 'Special Publication 800-63-3 Digital Identity Guidelines: 4.3.1 Authenticators': https://pages.nist.gov/800-63-3/sp800-63-3.html#431-authenticators accessed 09 February 2022.

[45] NCSC, 'Setting up two-factor authentication (2FA)': https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa accessed 27 May 2021.

[46] Akamai, *[State of the Internet]/security web attacks and gaming abuse* (vol. 5 Issue 3| 2019) p 18.

[47] 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.

(d) Update devices.

Out of date software, apps and systems can contain software weaknesses which make them more vulnerable to cyber-attacks[48]. Whilst this measure is not specific to credential stuffing attacks, as a general rule, all devices should be regularly updated and patched to ensure that the latest security 'fixes' have been installed.

REMEDIAL ACTION FOR AN ACCOUNT THAT HAS BEEN COMPROMISED

Having established the measures users can implement to more effectively protect their online accounts from the threat of a credential stuffing attack, there are also steps that a user can take if an account is suspected, or is confirmed, to have been compromised.

(a) Change the password (or passphrase) immediately[49].

This should be done as soon as possible as attackers will often change the password themselves to prevent the user from regaining legitimate control and to give themselves unlimited time and access to the account. Passwords for any other accounts protected by the same, or similar, password **must also be changed** as soon as possible to prevent other accounts from being compromised.

(b) Check account information and transactions.

There are many indicators that an attacker has gained access to an account, including unusual and unauthorised transactions, or log-in attempts from unusual locations or at unusual times, for example during the night[50]. In this respect, it is important to check the account history (and set up alerts where possible) and contact the bank if a credit card or bank account is linked to the account, even if funds have not left the account[51]. Users who have fallen victim to a credential stuffing attack, or any other cyber-crime, should also report it to the relevant authorities.

Other red flags to look out for are changes made to security settings or unknown messages that have been sent from the account[52]. When used[53], security questions and answers should also be changed. In

---

[48] NCSC, 'Cyber Aware': https://www.ncsc.gov.uk/cyberaware/home#action-1 accessed 08 February 2022.

[49] Canadian Centre for Cyber Security, 'Rethink your password habits to protect your accounts from hackers (ITSAP.30.036)': https://cyber.gc.ca/en/guidance/rethink-your-password-habits-protect-your-accounts-hackers-itsap30036 accessed 27 May 2021.

[50] NCSC, 'Recovering a hacked account': https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account accessed 27 May 2021.

[51] Canadian Centre for Cyber Security, 'Rethink your password habits to protect your accounts from hackers (ITSAP.30.036)': https://cyber.gc.ca/en/guidance/rethink-your-password-habits-protect-your-accounts-hackers-itsap30036 accessed 27 May 2021.

[52] NCSC, 'Recovering a hacked account': https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account accessed 27 May 2021.

[53] As noted in the foregoing, security questions **do not** offer the same level of protection as MFA and are no longer considered to offer a secure means of account protection in today's threat environment. However, when used they need to be monitored.

addition, friends, family and followers should be informed of the account that has been compromised and to open messages or notifications with caution[54], in particular to avoid being hacked themselves.

(c) Check for compromised email accounts[55].

Verify email filters and forwarding rules to ensure that an attacker has not set up a 'rule' to have a copy of all received emails forwarded to them. Information regarding how to check for this, and how this can be removed, can usually be found on the email provider's support page.

(d) Contact the account provider.

If access has been denied to an account due to being 'locked out' by an attacker, the relevant organisation will often have a 'help' or 'support' page providing information on how to recover the account[56]. If the account is recoverable and MFA has not yet been enabled, it would be recommendable to do so where the option is available.

If the account is unrecoverable, a new account would need to be created. In order to recover information that has been lost or stolen, users should ensure that they regularly 'back up' saved data to another device or to an online cloud storage[57].

(e) Check for compromised passwords.

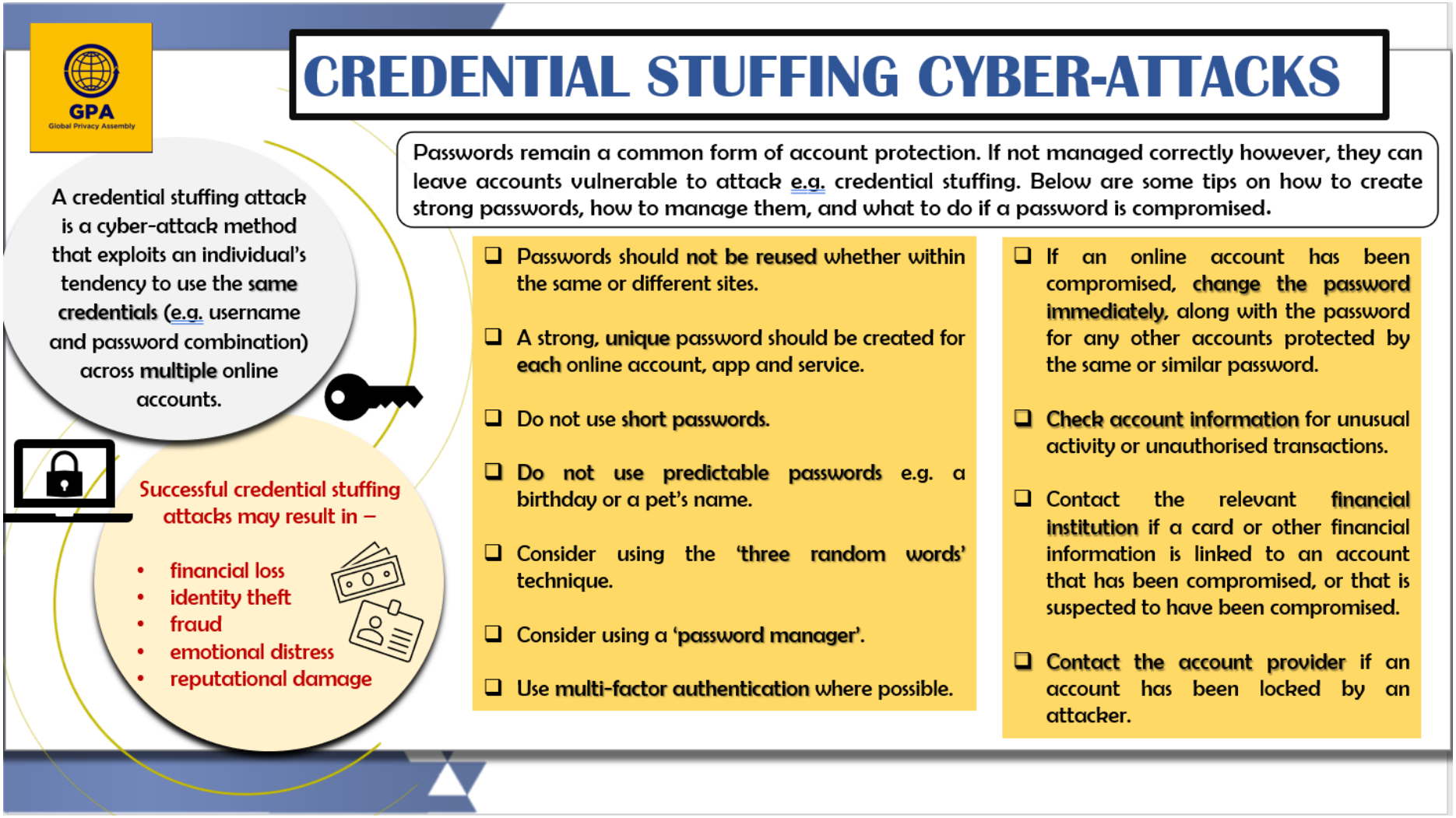
There are also publicly available websites, which provide lists of 'Pwned Passwords'[58], where users can check if their credentials have been compromised in a data breach. Users may also check for compromised passwords on a regular basis as a preventative measure and a means of monitoring the security of their online accounts.

[54] NCSC, 'Recovering a hacked account': https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account accessed 27 May 2021.

[55] Ibid.

[56] Ibid.

[57] NCSC, 'Cyber aware': https://www.ncsc.gov.uk/cyberaware/home#action-1 accessed 27 May 2021.

[58] 'Pwned Passwords': www.haveibeenpwned.com accessed 27 May 2021.

Annex 1 – Top tips to protect against credential stuffing