PROFiT
Prevention of Fraud in Travel

THE COUNTER FRAUD CAMPAIGN 2019

PART 19: PASSWORDS

Prevention of Fraud in Travel (PROFiT) and the Fraud Intelligence Network (FIN) are working with the City of London Police to reduce fraud in the travel industry. PART 19 is about the 'front door' to your accounts and applications.

PROFiT is the only official travel industry counter fraud body. We work on your behalf to carry out analysis and research, disseminate best practice and disrupt crime.

Find out how you can join the fight against crime. Contact via: contactus@profit.uk.com

BACKGROUND

1.0 Passwords are the key to securing your personal data, money and business. Everything that is valuable to you sits behind a password. It is therefore important to ensure the passwords that you use are fit for purpose. There is a lot of advice and opinions given about passwords, but rarely are we told why the advocated steps are necessary. In fact, the competing opinions are so numerous and sometimes contradictory that it is hard to know what to do. Couple the confusion with our own apathy and you get to the point where we all do what we think is correct and often what is easiest for us.

1.1 The average person has to remember about 22 passwords, and uses the same password for 4 websites.[1] Before we look at passwords in detail you need to always keep in mind the following adage: 'What one person can make, another person can break'. The following is an illustration of the truth of this maxim.

1.2 During World War 2 the German military used a machine called 'Enigma' for secure transmissions. This consisted of 3 rotors, each carrying the 26 letters of the alphabet at separate settings. Each rotor took in a letter and outputted it as a different one. That letter passed through all three rotors, bounced off a "reflector" at the end, and passed back through all three rotors in the other direction. Enigma had a possible 150,738,274,937,250 possible states. Alan Turing's team at Bletchley Park began trying to decipher the Enigma codes during 1939. Without seeing the machine by 1940 they had cracked the Luftwaffe version of Enigma and by 1941 the Kriegsmarine version.

1.3 Even more astonishingly Bill Tutte's team at Bletchley Park cracked the Lorenz cipher (the British called it 'Tunny'). From June 1941 Tunny was used by the German High Command and only 20 machines existed across Europe. Tunny had twelve rotors giving a possible 1.6 quadrillion possible settings. That is 1.600,000,000,000,000 possible settings. No one in the UK had seen Tunny. In November 1941 Tutte was given the cipher and by January 1942 the team had built a rudimentary machine to achieve this. In turn this led Tommy Flowers to build the first programmable computer, Colossus, by December 1943 which automated the process.

1.4 In other words, no matter how good the security, and no matter how complex a password is, if someone really wants it and they have the time and money they will probably get it. BUT, don't despair because the only people that can really go to this expense and time are foreign powers and they are generally not interested enough in your emails. If you have a strong enough password backed by another form of authentication it will be adequate to protect against virtually every threat

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf

that is out there. But to achieve that level of comfort you need to ensure that your password follows some basic rules. Let's see if your password is up to scratch.

PASSWORDS – THE BASICS

2.0 We give you the official and best view later in this edition of the campaign, but let's start with the received wisdom. When developing a password the following rules should be considered:

- Passwords need to be strong,
- Passwords need to be memorable to you,
- Passwords need to unapparent to others,
- Passwords need to be kept confidential, and
- Passwords need to be changed periodically.

2.1 There are various opinions as to what constitutes a strong password, but they all have some common themes. The most commonly given advice states that a strong password:

- should be at least 8 characters long.
- should have alphanumeric characters (that's letters and numbers to you can me).
- if predominantly lower-case letter then at least one should be capitalised, and if you use predominantly upper case then at least one should be lower case.
- should use symbols (that's the dots, commas, signs, dashes, hashes, and slashes on the keyboard.

2.2 What is this advice based on? Well, it's all to do with mathematics and the probability of cracking the password. The more variations and types of printable characters used; the greater the number of possible combinations there are that must be worked through in order to guess or accidentally identify the actual password. Consider the following table; the 8-character password is emboldened:

Character Sets Used As Passwords	Calculation	Possible Combinations
Dictionary words (in English): (Let's assume that is ~ 600,000 words)	---	600,000
Numbers Only	10^8	100,000,000
Lowercase Alpha Set Only	26^8	208,827,064,576
Full Alpha Set	52^8	53,459,728,531,456
Full Alpha + Number Set	62^8	218,340,105,584,896
Full Set of allowed printable characters set 8-character	**(10+26+26+19) ^8**	**645,753,531,245,761**
Full Set of allowed printable characters set 9-character	(10+26+26+19) ^9	45,848,500,718,449,031
Full Set of allowed printable characters set 10-character	(10+26+26+19) ^10	3,255,243,551,009,881,201

You can see from the above table that the most commonly recommended format of a strong password gives 645,753,531,245,761 possible combinations. It is also clear that the more randomness and characters that you can add the stronger your password will be.

2.3 Whilst this looks impressive, unfortunately, the significance is never explained to people and so there are several factors that might weaken the effectiveness of passwords and increase the chances of accounts being compromised. Equally passwords have been around for a long time and attackers have developed various ways of compromising them.

FACTORS THAT WEAKEN PASSWORDS

2.4 According to psychologists people typically remember more letters than words, and more digits than letters.[2] Because the average person can only comfortably remember a sequence of 7 characters without training, and passwords are recommended to be 8 characters or more, this causes problems for the average person's abilities to remember them.

2.5 This problem is magnified by the need to have different passwords for each application requiring you to hold and remember numerous multi-character passwords and drop off in cognitive ability

[2] Cowan N. (2010). The Magical Mystery Four: How is Working Memory Capacity Limited, and Why?. Current directions in psychological science, 19(1), 51-57

with age. This is one of the reasons that people are tempted to write down their passwords and keep them in proximity to the computer. It is not a failing in the person, but rather a failure to understand the average human capabilities by the people recommending random, complex, character length to create password strength.

2.6 The memory factor also causes people to use over-simple and easy to crack passwords. The most commonly employed passwords are used by hackers to crack your password if they have nothing else to go on. Therefore, you should avoid these passwords at all costs. The 25 most commonly used passwords are:

1. 123456	6. 111111	11. Princess	16. Football	21. Charlie
2. Password	7. 1234567	12. Admin	17. 123123	22. aa123456
3. 123456789	8. Sunshine	13. Welcome	18. Monkey	23. donald
4. 12345678	9. Qwerty	14. 666666	19. 654321	24. password1
5. 12345	10. iloveyou	15. abc123	20.. !@#$%^&*	25. qwerty123

2.7 Other terms to be avoided as they can be found out or guessed and are easy to crack include:

- Your name in any form -- first, middle, last, maiden, spelled backwards, nickname or initials.
- Any ID number or User ID in any form, even used backwards.
- Part of your User ID or name.
- Any common name, e.g., Tim, Sue, Joe.
- The name of a close relative, friend, or pet.
- Your phone or office number, address, post code, birthday, or anniversary.
- Acronyms, geographical or product names, and technical terms.
- The place of birth or residence of you or a family member.
- The name of a Country.
- A place where you have been educated.
- Your favourite sports team, e.g., Arsenal, Chelsea, Manchester United etc.
- Any all-numeral passwords, e.g., your NHS number, social-security number.
- Names from popular culture, e.g., Harry Potter, Sleepy.
- A single word either preceded or followed by a digit, a punctuation mark, up arrow, or space.
- Words or phrases with all the vowels or white spaces deleted.
- Words or phrases that do not mix upper and lower case, or do not mix letters or numbers, or do not mix letters and punctuation.
- Any word that exactly matches a word in a dictionary, forward, reversed, or pluralized, with some or all the letters capitalized, or with any substitutions.

HOW PASSWORDS CAN BE COMPROMISED

3.0 There are several ways that passwords can be compromised:

SOCIAL ENGINEERING. Attackers can use social engineering skills to coerce users into revealing their passwords.

MANUAL GUESSING. Attackers use personal information ‘cribs’ such as name, date of birth, etc. to guess common passwords.

INTERCEPTION. Passwords can be intercepted as they are transmitted over a network. See Man In The Middle attacks in part 18 of the email campaign.

STEALING PASSWORDS. Attackers can steal passwords that are stored insecurely. This can include handwritten passwords that are hidden close to a device or those stored electronically.

SHOULDER SURFING. Observing someone typing in their passwords.

KEY LOGGING. Attackers can install a keylogger to steal passwords when they are typed into a device. See Keyloggers attacks in part 18 of the email campaign.

BRUTE FORCE. Automated guessing of billions of passwords until the correct one is found. Brute Force attacks are carried out using net bots.

SEARCHING. Searching the IT infrastructure for electronically stored password information. This is often carried out using Malware. See the mail campaign part 17.

PASSWORD SRAYING. Attackers use a small number of commonly used passwords to attempt to gain access to many accounts.

DATA BREACHES. Attackers use passwords that have been compromised from other sources and the user does not change the password.

THEFT OF PASSWORD HASH FILE. Where the hash can be broken to recover the original passwords.

SPEARPHISHING. By sending an email saying that your account has been compromised and recommend that you use the 'link' in the email to reset it criminals can harvest your password.[3]

THE OFFICIAL ADVICE

4.0 The Centre for the Protection of the National Infrastructure (CPNI) is the UK Government authority which provides selective security advice to protect the national infrastructure. CPNI comes under MI5 and operates within the Security Services Act 1989. Part of CPNI's remit is to help secure businesses from external threats by issuing advice. CPNI's advice is also available from the National Cyber Security Centre (NCSC) which is based is part of GCHQ.

HOME USERS

4.1 The official guidance recognises the difficulties that users have in remembering several complex passwords. They therefore recommend that for HOME USERS a simpler approach is to use three random and unconnected words which are memorable to the user such as 'coffeetrainfish' or 'walltinshirt'.[4] NCSC advises that HOME USERS should avoid using words which might be easy to guess such as 'onetwothree' or are closely related to the user personally, such as the names of family members or pets. This approach is called '**Three Little Words**'.

BUSINESS USERS

4.2 Official advice for business users[5] is that passwords have been around for a long time and they are no longer as effective as they once were. Therefore, businesses are advised to:

i. **Reduce the organisations reliance on passwords.**
Only use passwords where they are necessary such as for the company Wi-Fi access. Technical solutions (such as a single sign-in) will help reduce the burden of too many passwords on staff.

ii. **Use multi-factor authentication (MFA) for important accounts.**
Because the MFA involves a password along with some other form of authentication known only to you (text message, random number generator, fingerprint scan etc.) then even if the password is compromised the attacker will still not be able to gain access.

iii. **Use single sign-in systems.**
Single sign-in allows staff to use one set of highly secure credentials to access multiple applications meaning that once they log-on they have access to everything they need to do their job. This massively reduces the pressure on users to create and remember several strong passwords.

iv. **Use throttling or account lockout.**
Password systems can be configured so that there is a progressively increasing time-delay between log-in attempts (known as throttling). This allows users that have forgotten their password several attempts to remember it whilst restricting the number of guesses an attacker can make. An alternative is lock-out where the user only has a certain number of attempts to log-in before the account becomes locked. Throttling is preferred because:

- Account lock-out can leave legitimate users unable to use their accounts and requires an access recovery method to be implemented.
- Account lock-out can provide an attacker with an easy way to launch a denial of service (DDoS) attack especially for large online systems.

[3] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf

[4] https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0

[5] https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

v. **Security monitoring.**
You can use security monitoring to detect and alert you to abnormal activity such as login attempts that fail the second Multi Factor Authentication step, or brute force attacks, or login attempts from unexpected geographical areas.

vi. **Password blacklisting.**
Where users are choosing their own passwords, it is helpful to employ a password blacklist to prevent users choosing the most common or easily guessed passwords.

vii. **Protect passwords in transit.**
Passwords can be intercepted during transit. To protect them you should ensure that all corporate web apps requiring authentication use HTTPS. A common type of attack involves stealing a security token to gain access to another device or server.

viii. **Protect the access management system.**
The access management system needs to be protected to prevent attackers using it to gain access to your system (for example by modifying password policies, or stealing tokens), whether this is within your own organisation or a cloud or other online service. While you can't influence the defences of the third-party systems, you should take steps to protect the access management systems you manage internally, and you should find out how third-party suppliers do the same.

ix. **Protect passwords at rest.**
Make sure the systems you deploy do not store passwords as plain text, even if the information on the protected system is relatively unimportant. Periodically search systems for password information that is stored in plain text.

All passwords should be stored in a hashed format, using multiple iterations of the hash function. Hashing is a one-way cryptographic function which converts a plain text password into a 'hash', an unreadable string of characters designed to be impossible to convert back. However, attackers can still use brute-force attacks and rainbow tables (pre-computed tables for reversing cryptographic hash functions) to retrieve passwords from stolen hashes.

An attacker who has accessed a password hash file will not know the actual passwords. But if the passwords have been hashed poorly, or the attacker has enough computing power, it may be possible for them to recover some of the passwords. For this reason, it is important to protect access to the user database. As well as being a target for attackers looking to compromise your system, these are a target, even if the information is out of date.

x. **Prioritise securing important or vulnerable accounts.**
While all passwords should be protected, accounts that have highly privileged access to systems, services and data (or accounts that are accessible externally such as cloud services or remote access) are especially attractive to attackers. Multi Factor Authentication should be the primary method for protecting these accounts.

xi. **Change default passwords.**
Many apps and devices come with factory pre-set passwords. Many of these factory passwords will be known and shared by attackers. Make sure that you change all pre-set passwords to something stronger.

xii. **Use password management software or other secure storage.**
You should provide appropriate facilities to store passwords. The NCSC recommend the use of password managers for secure storage wherever appropriate. As well as providing secure storage, password managers can help users by generating and auto-filling passwords when required.

If a password manager is not suitable you should provide physical storage for recorded passwords such as a secure cabinet. You may also need secure storage for Multi Factor Authentication tokens. This should be separate from the stored password.

xiii. **Don’t enforce regular password expiry.**
Regular password changing harms rather than improves security. Many systems will force users to change their password at regular intervals, typically every 30, 60 or 90

days. This imposes burdens on the user and there are costs associated with recovering accounts.

Instead of forcing expiry, you can counter the illicit use of compromised passwords by:

- ensuring an effective movers/leavers process is in place.
- automatically locking out inactive accounts.
- monitoring logins for suspicious behaviour (such as unusual login times, logins using new devices).
- encouraging users to report when something is suspicious.

You can also mitigate the risk of compromised accounts by using Multi Factor Authentication, which will make a compromised password less useful to an attacker. Some Multi Factor Authentication methods (such as SMS or email notifications) can even warn the user that they have been compromised, as they will receive a code when they did not request it. If you are using this form of Multi Factor Authentication, you should encourage users to report this behaviour through your training.

xiv. Manage shared access.

Sharing work accounts, or even occasional use by anyone other than the account holder, introduces several risks. As well as the possibility of users gaining access to unauthorised resources, sharing accounts negates the benefit of authenticating a specific user. In particular, the ability to audit and monitor a specific user's actions is lost, an essential forensic requirement for some accounts.

If passwords are being shared, try and find alternative solutions that support the business need for sharing. For example, many accounts will have a way to delegate privileges to another account (such as access to a document or inbox). Delegation should be used instead of sharing accounts wherever possible.

If alternatives are not possible, and there remains a strong business need for shared access to an account or device, then access to the password should be monitored and continually reviewed to manage the risk:

- The password should only be shared within the smallest possible group of known and trusted users.
- The password should not be exposed to users who do not have permission to access it.
- If someone is no longer allowed access, the password should be changed.

Some password managers allow users to share passwords in a more secure way (for example, they can audit access to the password and automatically sync password changes). If you have a business need to share a password, then consider using a password manager to do this.

MISSED A PREVIOUS EDITION?

If you have missed a previous edition of the email campaign let us know and we can send you FREE a copy: contactus@profit.uk.com

Like what we do to protect you?

We are always short of funds and need your support.

Find out how you can join PROFiT and fight fraud by emailing contactus@profit.uk.com

Next Week: Part 20 Defensive Software