Securing Digital Identities

Digital Identities in a Multi-Service Digital World

PART OF OUR SECURITY SERIES OF WHITE PAPERS

PREPARED BY Michel Drescher

PUBLISHED ON January 2020

How to cope with digital complexity

Abstract Summary

In today's digital world, people are accessing multiple credit cards, networks, online tools and apps for their business and personal lives. The list is endless with passwords, pin codes to remember, and also keep secure.
This means they are increasingly facing the very real problem of having to manage and deal with too many different login credentials.
Remembering them all has become more difficult, especially as online security demands ever more complex passwords and pin codes.
For many this is becoming impossible for them to deal with and they revert to coping strategies, leading to unintentional severe security vulnerabilities.
This white paper seeks how to identify when this is happening inside your organisation and lays out clear advice on how to help people move past the coping strategy phase, thus reducing the risks of weak passwords and potential points of employee failure.

Background

Given all the hype about technology and easy access to information, the reality is it isn't making life any easier or simpler to manage in today's world. Especially as new technologies in some cases are completely taking over many aspects of our personal and business life. It's now become ever more complex if not outright overly complicated to manage.

The natural human response to increasing complication is to use coping strategies in different ways and situations. It's important to call out the distinction:

- **Dealing** with a situation means proactive, conscious or controlled actions fully aware of the consequences of one's actions.
- **Coping** usually happens on a subconscious level and is a symptom of an unhealthy incapacity of managing or being unable to deal with the situation at hand. It is a warning sign of stress or duress, or even both.

Merely coping frequently leads to the wrong choices being made – with devastating results.
In this white paper, we outline two examples to illustrate this behaviour: from the situation, the problem/threat it poses, to the all too frequent coping strategies demonstrated in today's digital life.

Example 1: Credit/debit cards and PINs

The banking industry has taken dramatic and bold strides towards digitalisation and modernisation in the way customers use banks and manage their finances. However, there is one aspect of modern electronic banking that is worrying, because coping strategies of individuals lead to systemic security vulnerabilities.
With today's financial world steering away from cash to electronic currencies, and the extensive uptake of credit, loans, everybody sees their lives and wallets gradually overtaken with "plastic money" - credit cards and debit cards in abundance.

The fact of a huge amount of (quite possibly tempting) credit cards is not the issue here. Rather we are talking about a policy, and in fact the legal requirement that you as the card holder are required to maintain a unique and sufficiently complex PIN to use with electronic payments.

The legal conditions the financial organisations and companies have put on us - with the best of intentions to protect us against illicit behaviour and financial theft - are the wrong ones. In truth they are outsourcing the problem to you the customer.
One debit card? Most people can deal with that. Two or three? Five or more? The onus remains with the customer to remember and safeguard the different PIN numbers and not to resort to writing it down , or sharing it with anyone.
The question is how long can a person keep track of all the pins by memory alone – which you are legally obliged to do by the banks?
There are commonly used coping strategies people use to help them, and can too easily led to fraud if they fall into the wrong hands.

- Written notes, often with the very cards in the same location (wallet or purse)
- Simplify by cycling through few memorised PINs
- Radical simplification of using only one PIN for all cards

Example 2: Passwords, Passwords

Similar to the first example, but in a different digital domain: Identity theft, impersonation and to some extent privilege escalation.

Today, we are dealing with many different aspects of our life in the digital domain: Social, personal, financial, professional and these different aspects of one's life have a digital and electronic link. In the digital realm, however, identity is fractured into multiple disconnected aspects of behaviour, silo'ed into and with the various digital services we are using on the internet.

To comprehend the size of the problem, think of all the different services you use on the Internet, mobile phone, laptop, tablet or other electronic equipment. Probably some 20 or more digital services. And, just as in the Chip and PIN example, it's expected you have to remember the unique usernames and passwords for each one. There are usually more passwords to remember than PIN codes but then there is the extra level of the sheer complexity of passwords required these days requiring numbers, letters, uppercase and lowercase, special symbols, and even with prescribed minimum occurrences. Whilst most people already struggle with memorising a handful of 4-digit PIN's, it's asking too much to then have to memorise even more complex sequences of random characters.

The same mechanics are in play here:

Human coping strategies typically result in radical simplification of passwords to the bare minimum, where the converse would increase security, and the rotation of as few passwords as one can get away with across the digital services they use.

Passwords written on little Post-It notes tacked to the screen, using one of the most popular passwords in the world - usually "12345678" or simply "password" where password complexity filters are not yet employed - and other simplification strategies.

All this reduces complexity for the overburdened human mind, at the expense of overall security: The counter-intuitive result of increasing login security is an overall lower security situation and increased risk of intrusion of any service involved.

Solution:

We offer two solutions of how to deal with a situation that does not compromise security as long basic rules are followed, and the second option being the preferred one.

Solution 1: Password managers

Password managers are tools designed to let you deal with the complexity of having to remember increasing amounts of passwords with the complexity requirements. In effect, password manager serves as your brain to memorise your passwords (and other closely associated identification information).

What they are?

Password managers are essentially little more than databases and are built to securely store passwords by encrypting its contents using strong and secure encryption: In the case of losing this file, no one would want anyone else to be able to decrypt and access all the desirable data contained in it.

Therefore, password managers always use a so called "master password" to encrypt the data and require you to type in the master password before they can decrypt the data and be of service to you. If used correctly and extensively, this may well be the only password you'll ever need to remember! You may have come across password managers built into your browsers (Firefox, Safari, Chrome) or computer operating systems (e.g. Keychain Access in Mac OS X). Recently there has been a warning about potential security flaws in password managers so it's always best investing time in doing your research and applying best practice when using them.

We've prepared a list of best practices and recommendations provided below for using password managers.

Best practice in managing passwords

1 Make your master password as complicated as possible

The password manager is the central place for all your passwords, therefore protecting it is essential. The master password should be complex and long because it is used to encrypt and decrypt the data you store in the application's database. Never, ever share it with anybody.

2 Then make your service passwords as complicated as possible

Once you decided to use a password manager, you needn't worry about having to remember all your passwords. The result is that the passwords you use to log onto services and (web) applications can and should be more complicated - the more the better. This works particularly well in conjunction with best practice #4 below I.e. Using keyboard shortcuts, makes logging onto services very, very easy and convenient

3 Allow storing additional data - using a "notes" facility or similar

While many systems typically require you to enter a user name and a password, it is often necessary to store additional data. For example, some UK banks require you to add some specific characters of a third element, chosen at random every time you log in. This kind of information needs to be stored just as safely as any password. Or you want to store other closely related sensitive information concerning your identity with that particular service alongside your password.

4 Allow using keyboard shortcuts

Frequent use of password managers can be time consuming entering in the usernames and passwords. Learn to use the keyboard shortcuts to navigate through the stored usernames and passwords, and to copy them to the computer's clipboard to use in the login screen of the application.

5 Limit sensitive information only for a short time

When using keyboard shortcuts and the system's memory clipboard, make sure that the password manager automatically deletes sensitive information from the clipboard. You can do that manually, but if the software does it for you, then that cannot be forgotten and remain accessible to any illicit software potentially residing on your system

6 Store password databases on removable media only

This serves two important purposes: Firstly, while online storage sounds attractive, you rely on your storage provider's capabilities and expertise to prevent the leaking of your encrypted password file to unauthorised people. Secondly, once in the hands of prying eyes, they can be taken offline and cracked with all the time in the world without you knowing it. The second purpose is that it prevents any malware on the computer trying to tamper with the password file in the background or prying on it when you are not using your computer.

7 Use a mobile version of the same application

Especially in conjunction with point 4, using removable media, password managers become "mobile" while not compromising security. Good password managers offer apps for your mobile phone (Android and/or iOS) as well. To use the same password database, use removable media only, and only those that can be used with mobile phones as well. Brand names range wildly, but as one example of many (without endorsement!) SanDisk Ultra Dual USB Drives are confirmed to work well in a Laptop/Android phone dual use scenario with password managers. Using a mobile version of password managers allows you to maintain the same level of security when using a different computer than usual (internet cafe, or a colleague's laptop for example). The only drawback is having to type everything in.

8 Mobile password managers using latest authentication technology

Smartphones support multiple ways of personal identification that go beyond PINs we are used to from the early days. Make sure the one you are select allows convenient yet secure personal authentication such as fingerprint scans, pattern drawing or other more recent ways of authenticating. This list of recommendations is far from being exhaustive. However, it allows you to use password managers securely and safely, and to declutter your brain. Reading on, you will realise that password managers, when used correctly, implement security best practices very similar to what large scale infrastructures ought to do for their users in the first place.

This list of recommendations is far from being exhaustive. However, it allows you to use password managers securely and safely, and to declutter your brain.

Single sign-on (SSO) and multi factor authentication

Option 2: Using Single Sign On (SSO) and multi factor authentication

SSO and MFA work very well in a combined approach to digital information security, but they can be deployed independently from each other in slightly different IT architectures.

How MFA works

MFA increases user account security by adding another means of authentication before the system is satisfied that the person claiming to be the account owner is the person who owns the account. This is a key differentiation: MFA is designed to increase account security for humans, i.e. in person-to-machine (P2M) communication and not for M2M (machine to machine) interactions.

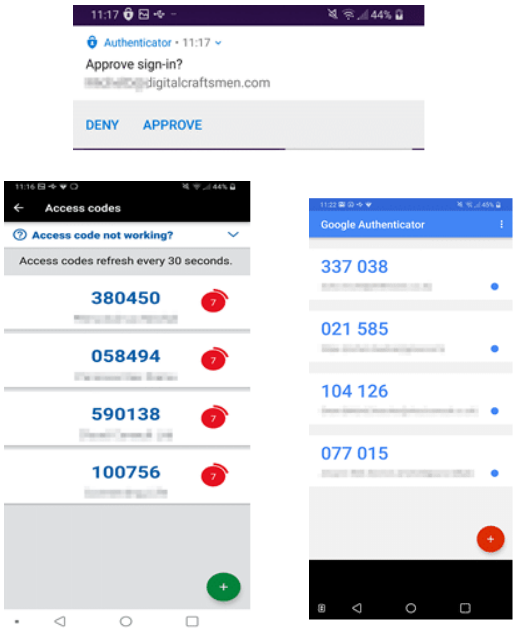
MFA is no different to the usual process of assuring a person's authenticity by means of a challenge/response process: Issue a challenge for the user to respond to, and challenge is satisfied when the supplied data matches pre-configured information. MFA simply adds more challenge/response phases to the mix. The most common form is 2FA, or Two-Factor-Authentication with a second challenge/response phase. Only rarely is MFA deployed with more than two factors.

The key increase in account security is achieved by using separate, independent communication channels for the other authentication factors. For 2FA this is predominantly the user's mobile phone through which the second challenge is delivered. The mobile phone is registered as a trusted device for second factor authentication during the process of account setup, or when enabling 2FA as an add-on.

The first factor is still the correct combination of username and password that must be supplied together. Additional means such as captchas can be used to ensure a person is interacting with the service, but that does not address assuring that the right person is accessing the electronic service. Once that is satisfied, the system moves on to address the second factor.

In the case of mobile phone based 2FA, this second factor always includes the challenge to be delivered to the mobile phone, for example using text messages, or more recently by sending push notifications to a 2FA app installed on the mobile phone.

Some 2FA systems then require the user to type in a code to the electronic service's authentication screen, or simply by tapping "Approve" or "Accept" or similar on the mobile phone app.
Since the technical protocol for implementing 2FA is so similar across solutions, the accepted best practice for services implementing 2FA
authentication is to integrate with one or several generic 2FA applications available for mobile phones, instead of going it alone.



Above screenshots illustrate three different 2FA applications in action; Microsoft Authenticator, UK HMRC tax account authenticator, and Google Authenticator The numeric codes seen in the screenshots periodically refresh in a way that cannot be predicted without the secret information used during authenticating the mobile phone for the service in question: They serve as time-based one-time passwords.

Single sign-on (SSO) and multi factor authentication cont

Deploying MFA standalone

Deciding to roll out MFA on its own already greatly increases user account security, but it doesn't solve the problem of user account and password complexity deluge.
Nonetheless, implementing MFA within a company's IT assets as well as making MFA mandatory by policy when using external IT services is a great step towards overall security in an organisation, and will greatly reduce any CISO's headaches.
Even when usernames and passwords are leaked, stolen or otherwise accessed by unauthorised persons, any MFA-enabled accounts are secure because of the second mandatory authentication factor to which the perpetrator does not have access.

How does SSO work?

MFA addresses the problem of weak account security. In contrast, SSO addresses the problem of the deluge of user accounts for an ever-increasing amount of IT services used in our day to day private and professional lives. When interacting with an electronic service, two elements come into play when determining whether a user is allowed to use the system.Authentication deals with establishing that a person claiming having access to a user account is actually the person who owns that user account - that is dealt with using account names and passwords, and (hopefully) requiring MFA as well.
Authorisation establishes the roles and access rights of a given user account within a given electronic service. For example, in a document sharing scenario, a company director may be able to create and edit a document (such as a company strategy document) whereas some employees in the same company may have only read access, or even no access at all to that document.
This is achieved by attaching different roles and/or access privileges to a user account within that system. In the past, authentication and authorisation were combined together in IT services - and it is still the predominant way of granting and managing access to services today.

Single sign-on separates the process of authentication from the process of authorisation by splitting off authentication into a separate service. While a combined solution increases service independence it at the same time increases user account complexity for the individual person. Separating the two processes (there is no technical necessity that requires them to stay tightly combined into one service) increases the dependency of the electronic service on a separate service. But this technical complexity can be hidden away from the user and is increasingly pushed into the background as much as possible to increase user experience.
In a managed IT environment, deploying and ensuring availability of the authentication service is far easier to achieve than in the public space, which is the reason of slow uptake of SSO in this area - but it is visibly happening: Companies increasingly accept users logging into their websites using predominantly their social media accounts, such as Google, LinkedIn, Facebook, Microsoft Live, and others. When in the SSO scenario users are encouraged or even required to log onto multiple services using only one user account managed separately elsewhere, this invariably leads to the question of account security: The same account used to authenticate against many different services can have a devastating effect when the user credentials are leaked or stolen.
This is no different from the scenario described earlier in the white paper, where a user's coping strategy leads to uncontrolled simplification of the situation and thus to a huge security risk by using inadequate user account security. The crucial difference is that in managed SSO environments heightened user account security is enforced: In exchange for reducing user account uniqueness across integrated services, the individual user account security is increased through a number of measures.

Single sign-on (SSO) and multi factor authentication cont

To understand how SSO works, the three key stakeholders in this scenario are briefly outlined below:

- A Service Consumer (SC) is in this context a user (an employee, or an individual in private life) that wishes to use a given service that is SSO enabled.

- A Service Provider (SP) is the digital application that provides the service the user wishes to use.

- An Identity Provider (IdP) is an IT service taking care of a secure and safe authentication of a SC on behalf of a SP.

The process of logging onto an SSO enabled service is different from the traditional way:
1 - The user (SC) accesses the service provider.
2 - The service provider (SP) decides that the user needs to authenticate first and asks the user to do so by redirecting her to the configured identity provider. While doing so, the SP sends along a unique token.
3 - Upon arriving at the Identity Provider (IdP) the user authenticates herself as required and challenged by the IdP.
4 - If authentication was successful, the IdP sends the user back to the SP, along with the original token as sent by the SP, and account information (frequently an E-Mail address) identifying the user.
5 - The SP examines the user account information and ensures that the token sent back is valid.
6 - Once satisfied, the SP allows the SC access to the service.

Step 4 is a key step in terms of account security and privacy implemented in good SSO systems: The account information sent back to the SP does not have to be personally identifiable information (E-Mail addresses are such information protected by the GDPR) - it can be an entirely artificial unique string specific to the connected service, and a different string for a second connected service. This way, sensitive personal information does not need to leave the domain of the IdP ever.

Streamlining and optimising log-in requests

The process indicated above can be further optimised to include the concept of sessions. Similar to traditional systems, where users are required to log in again from time to time (e.g. after a period of inactivity), sessions are also possible with SSO infrastructures - and it even works across connected services! For this to work, some additional steps need to be inserted into the abbreviated login procedure illustrated above: Instead of redirecting the user straight away to the IdP, the SP first queries the IdP whether the user's session with the IdP is still valid and active. If the IdP affirms, the SP gives the user access immediately.

This is the second meaning of single sign on: Not single in the context of a single user account re-used across possibly many connected services, but the process of logging in only once (or every so often) even when accessing different services.

Conclusion

It is crucial to support users in a safe and secure way to deal with digital infrastructures that are growing ever more complex. We have illustrated a few solutions that are individually already of great help in this situation. However, our strong recommendation - most certainly for managed corporate IT infrastructure - is to implement and deploy SSO and MFA together: Equipped with the information described above, the benefits of this combination are almost self-evident without any further explanation.

We will always recommend deploying SSO and MFA together, and always prefer this over using password managers. While still useful in certain situations, password managers in our minds merely address the symptoms of an inadequately secured IT infrastructure, not the root cause of CISO's headaches.

If you want to find out more about the best security options for keeping you, your employees and business secure and protected against hackers, data breaches, then speak to one of our security experts on best practice, advice and guidance.
We are ISO27001 and CyberEssentials Plus Certified, endorsed by the highest industry standards so you can trust us to offer the very best in cloud hosting, managed services and managed security advice.

Tel the office on **+44 (0)20 3745 7706** or email the team on **info@digitalcraftsmen.com**