The weakest link

PASSWORDS ARE A VITAL ELEMENT OF CYBER SECURITY, BUT NOW EVEN STRONG PASSWORDS ARE NOT ENOUGH FOR CLOUD APPLICATIONS. BY IAN BLOOMFIELD

Cyber security is receiving increased attention in mainstream media, whether it's the latest global cyber crime disaster, or an initiative by government focused on fighting cyber crime. I never thought I would see the day when the Prime Minister of Australia would make a speech that included: "A lot of the vulnerabilities, as you will have seen, are because people do not follow good cyber practice. They don't, for example, use two-factor authentication with cloud-based applications and so forth".[1]

The importance of passwords

The essence of a law firm is the information it holds, whether it is client, third party or internal information. This information is typically stored in a range of systems – email, files storage, practice management systems. Access to these systems is secured by requiring users to have an account and associated credentials – username and password.

If there is not adequate access security, there is a risk the information in these systems is compromised – stolen, modified, corrupted, destroyed or lost. The implications of this can range from annoying to catastrophic including:

- inability to deliver services due to lost or missing information
- loss of reputation, and probably clients, as a result of a data breach
- actions by the Australian Information Commissioner as a result of a data breach. With the imminent introduction of the data breach laws,[2] this could involve legal action in cases where a law firm has more than $3 million in revenue.

What is a strong password?

Until recently a strong password could be defined as a length of 12 characters and a mix of numbers, upper and lower-case letters and symbols. In addition, there would have been a requirement to change each password on a regular basis, typically every three to six months.

Recently, the traditional wisdom about strong passwords has been challenged with the publication of "Digital Identity Guidelines" by the National Institute of Standards and Technology (NIST).[3] NIST is a US federal organisation and a preeminent source of cyber security guidelines. The main changes recommended are that the minimum length for passwords should be eight characters and there should not be a requirement for the periodic changing of passwords.

One of the primary authors, Paul Grassi, explains the thinking behind some of the changes recommended in the NIST publication in a CSO Online article: ". . . we reviewed a lot of research in the space and determined that composition and expiration did little for security, while absolutely harming user experience. And bad user experience is a vulnerability in our minds".[4]

It should be noted that the NIST publication also makes it clear that the longer the password the better, and to underscore this, it recommends that all systems should allow passwords as long as 64 characters.

ADOBESTOCK

Who uses strong passwords?

According to a recent report by password management company Keeper Security,[5] the most popular password used by nearly 17 per cent of people is "123456" and the second most popular is "123456789".

Even long passwords that on face value appear to be strong, may not be. If you go on to YouTube and search "How hackers crack passwords", numerous videos will be listed showing just how frighteningly easy it is.

So the reality is, faced with the challenge of coming up with a unique strong password for every account, most people don't.

Use a password manager

The best option for creating and maintaining strong passwords is to use a password manager – software designed to help you create, store and organise your passwords.

Most password managers require a strong master password during setup, and then you add account credentials (usernames and passwords) to the password manager. The process of recording credentials is automated, with the password manager capturing the username and password each time you access an account for the first time, and when you create a new account. Of course you can also manually record account and credential details.

All password managers encrypt the stored passwords, making them indecipherable without the master password. Most password managers store passwords in the cloud (a secure database located in a remote data centre) but some are stored locally in an encrypted file on your computer, tablet or phone. All password managers require the master password to decrypt and access the stored passwords.

Regardless of how the password manager stores the passwords, the security of a password manager relies heavily on using a strong master password and the need to protect this from being stolen. So there are still risks with using a password manager.

Why put all your eggs in one basket if there is a risk of a hacker getting access to all your passwords? The answer is that the risk of this happening is very low and is far outweighed by the significant benefits of being able to maintain strong passwords and good password practices.

Other benefits to using password managers include:

- most provide the ability to synchronise the stored passwords across a range of Android, Apple and Windows devices, and also provide mobile apps.
- they usually work with the popular browsers (Firefox, Safari, Chrome and Internet Explorer) making it possible for passwords to be filled in automatically when you access the logon page for a cloud application
- most will allow storing sensitive information other than passwords, including IDs, credit card details and software licenses.

Some of the most popular password managers are LastPass, Dashlane, 1Password and KeePass.

Passwords and the cloud

There are additional risks associated with cloud based applications and even using strong passwords is not enough.

When using an application like Microsoft Word that is installed and run locally on your computer, you probably store the resulting Word files locally on your computer, or on your local server computer. Now let's consider the situation where a hacker has acquired the password to access your computer, or even the password to access the server computer. The password is of no use unless the hacker can first get access to your office computer network. Although possible, the risk is relatively low. Your password is analogous to the key to the front door of your home. If your home has a physically secure perimeter fence and a guard dog, then the key is of little use to a criminal unless they can breach the perimeter fence and deal with the guard dog.

With a cloud based application, or online

SNAPSHOT

- Recent events such as ransomware hacks have highlighted the need for all businesses to take action to improve their cyber security.
- Law firms and their employees routinely handle confidential information, and this information is stored in systems protected by passwords.
- Every law firm and their employees should understand the importance of passwords and the role they play in securing access to information.
- A law firm is exposed to significant risk if good access security is not maintained. This risk can be mitigated by using password managers and two-factor authentication.

account, there is no protection from an office network. The logon page to your cloud application is public facing, openly available on the internet to all and sundry to see and try to access. The only thing stopping a hacker accessing a cloud based application is knowing your username and password. The analogy in this case would be where the front door of your home faces directly onto the street, in other words public facing, so all a criminal needs is the key to the front door and they can get into your home.

Two-factor authentication

Two-factor authentication provides an additional layer of security. Authentication is a security term for verifying your identity, and factors of authentication include:

- knowledge factors – something the user knows, such as a password or PIN
- possession factors – something the user has, such as an ID card, security token or a smartphone
- inherence factors (biometrics) – something the user is, typically personal attributes, such as fingerprints, face and voice.

Historically, passwords have been the single authenticating factor required to verify our identities on computers. What if a hacker needed something else in addition to a stolen password? This is the principle behind two-factor authentication, meaning that in addition to knowing a password, something else is required to prove that you are who you claim to be.

You might not realise it, but you regularly use two-factor authentication when you swipe your credit card and then need to enter your PIN code. This authentication process requires two types of authentication, you have to possess your credit card and know your PIN code.

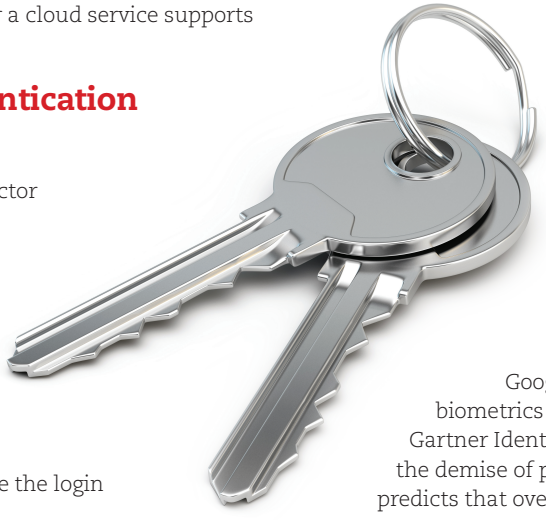
Two-factor authentication, also known as multi-factor authentication, is widely recognised as the best way to improve the security of cloud applications. Many of the common cloud applications now offer the option of using two-factor authentication, including Dropbox, Facebook, Google, Microsoft, Apple, Amazon, Twitter and LinkedIn. There are websites, such as Two Factor Auth List and Turn It On[6] that can help identify whether a cloud service supports two-factor authentication.

How two-factor authentication works

This is one example of how two-factor authentication works. At the logon page you enter your username and password – the first authentication factor. You then receive a text on your phone that contains a numerical code – the second authentication factor. The code is then entered into the logon page in order to complete the login process and you gain access to your account. A two-factor authentication code is called a "one-time passcode", and you are sent a new code each time you log on. An alternative arrangement for a second authentication factor is the use of a dedicated authentication app on your mobile phone. The app generates a fresh one-time passcode every 30 or 60 seconds. When logging onto a cloud application, you get the one-time passcode from the app and type it in as the second authentication factor to complete the logon process.

There are benefits to using an authentication app to generate the one-time passcode rather than receiving it via a text message. There have been many instances where a phone number has been hijacked by a hacker allowing them to receive the text containing the one-time passcode. Hijacking a phone number is surprisingly easy. All the hacker requires is enough identification details to impersonate the owner of the mobile number and convince the mobile phone carrier to transfer the number to another service provider or to another device: "Hi, I have lost my phone and need my number transferred to the new phone I just purchased . . ."

An even better arrangement for a second authentication factor is the use of a push notification. Instead of receiving a one-time passcode via text or from the authentication app on your phone, a push notification is sent to the authentication app on your phone. You get a prompt asking for you to Approve or Deny the log in. If you select Approve, the login process for your cloud application is automatically completed without the need to type in a passcode. If you select Deny, you receive an alert advising that there has been an unauthorised attempt to log into your cloud application. Many cloud applications that support the use of two-factor authentication also support push notification, including Google and Microsoft. The adoption of two-factor authentication should not be seen as an excuse to use weaker passwords. Just because you add a second factor you should not weaken your first factor, and the use of strong passwords and good password practices remains important.



ADOBESTOCK

The future of passwords

The next generation of authentication uses biometrics. There are many who predict this could potentially lead to the demise of passwords. Last year Google revealed that it plans to start killing off traditional passwords in its Android operating system. Instead, Google will rely on a combination of biometrics and other factors.[7] Last year at the Gartner Identity & Access Management Summit,[8] the demise of passwords was a key theme. Gartner predicts that over the next two to three years,

"recognition technologies" using analytics and biometrics will overtake passwords as the dominant means of authentication.

Information held by law firms is extremely sensitive and the potential value of this information to cyber criminals cannot be underestimated. In addition, with the increased focus on privacy, a law firm that fails to protect the information it holds not only faces the likelihood of public scrutiny, but also risks prosecution under the new data breach laws.

Passwords play a crucial role in protecting information, and the level of protection provided by a password is seriously compromised if it is not a strong password. Password managers provide a practical way to create, store and use strong passwords. Every law firm should review its password policy, or create one if one does not exist, and make sure that it clearly identifies the benefits of using a password manager. With password managers costing no more than $2 or $3 per month, law firms should consider providing them to staff.

Almost every law firm uses cloud applications of some sort, and using these without two-factor authentication now represents an unacceptable risk. Prime Minister Turnbull is not the only leader calling for the use of two-factor authentication. Last year the "Lock Down Your Login" public awareness campaign was launched in the US as part of President Obama's cyber security national action plan, calling on Americans to use two-factor authentication.[9]

While two-factor authentication makes it more difficult to log into an application, the inconvenience is minor compared to the added security and the comfort you and your clients can take from knowing you are not at risk, even if someone finds out your password. ■

Ian Bloomfield is managing director of Ignite Systems, with more than 40 years experience working with IT. He is a member of the LIV Technology & the Law Committee.

1. Prime Minister Malcolm Turnbull, 24 January 2017, www.pm.gov.au/media/2017-01-24/doorstop-minister-assisting-prime-minister-cyber-security-hon-dan-tehan-mp.
2. Notifiable Data Breaches: www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches.
3. NIST publication, "Digital Identity Guidelines", March 2017, https://pages.nist.gov/800-63-3/sp800-63b.html.
4. CSO Online, "Vendors approve of NIST password draft", www.csoonline.com/article/3195181/data-protection/vendors-approve-of-nist-password-draft.html.
5. Keeper Security blog, "What the Most Common Passwords of 2016 List Reveals", https://blog.keepersecurity.com/2017/01/13/most-common-passwords-of-2016-research-study.
6. Websites to assist with the use of two-factor authentication – Two Factor Auth List website: www.twofactorauth.org and Turn It On: www.turnon2fa.com.
7. The Guardian, "Google aims to kill passwords by the end of this year", www.theguardian.com/technology/2016/may/24/google-passwords-android.
8. Gartner Identity & Access Management (IAM) Summit 2016, www.silasg.com/the-death-of-passwords-and-three-other-trends-at-the-gartner-iam-summit.
9. Lock Down Your Login, www.lockdownyourlogin.com.