Solving the Password Problem

Simplify Your Life (Without Compromising Your Security or Privacy)

advance

Introduction

Imagine a system so secure, that to access it required possession of a physical key card, a 100-character password and a biometric face scan.

Now imagine a system so easy to access it didnt need a password or user name to be entered, just required the ‘logon’ button to be clicked, then a glance at a smart phone.

Now imagine all the security of the first system, combined with all the ease of the second system. This is what modern tooling can achieve, with just a few minutes spent setting it up.

This paper looks at password techniques, password managers and multi-factor authentication and how modern versions of these tools can make everyone’s lives easier and much more secure.

Does Length Really Matter?

While there are many new safeguards designed to prevent password guessing, the length, complexity and uniqueness of a password are still important factors to make an account secure.

Computer programs designed to guess passwords work by harnessing new technologies to make millions of guesses per second. The longer and more complex a password the more guesses are required before the correct combination is found. Modern password guessing programs will also try dictionary words, common variations and commonly used passwords, which makes unique passwords important.

Many safeguards have been developed to protect against these guessing methods and are often extremely effective where they are implemented.
In some cases, systems may only allow three incorrect login attempts, or there may be inherent limitations, such as bandwidth and processing power, that stop multiple login attempts.

Additionally, new cryptographic storage techniques are making it harder for attackers to guess passwords, even in 'offline' attempts.

Unfortunately, while these safeguards are very effective when implemented, they are not implemented universally, and are not completely full proof.
Individuals should never rely on security features which may or may not be present.

It is for this reason that making passwords long (lots of characters), strong (using lower case, upper case, special characters, and numbers) and unique (only used for one system/login) is still an important baseline for personal security.

Is Multi-Factor Authentication A Silver Bullet?

Multi-Factor Authentication (MFA) or Two Factor Authentication (2FA or TFA) is when a secondary (or more) authentication method is used to verify the users identify. This is normally carried out by validating the user has something physically (such as a smart phone, token, smart card etc) or that they are something (such as biometrics including fingerprint and face scan technologies). Modern MFA techniques leverage smart phones and one time codes via SMS or app based login approval.

Its now commonly accepted that modern MFA techniques block 99.9% of attempts to take over an account, but why is this?

In traditional criminal investigations, investigators often look at three key elements, means, motive and opportunity.

Unfortunately, with account take over, particularly when the system is internet based, all that is required to carry out an attack is an internet connected device, anywhere in the world. This means that billions of people have both the means and the opportunity to commit account take over attacks.

Multi Factor Authentication combats this problem by requiring a secondary verification method which is much harder to fake from different physical locations.

When a Modern smart phone is used for MFA, a third verification is often added, seamlessly to the user.
Most modern phones will require either a pin code or face/fingerprint scan to unlock them, and in doing this the user has provided a third identity verification.

It may not seem like a much, but by glancing at an iPhone and pressing the accept button within an authentication app, the user attempting to login has verified that their face biometrically matches the face of the approved user, and they have performed this biometric check on the only device in the world that will allow access.

Defeating MFA is not completely impossible, but in most cases gaining access to an account protected by MFA becomes far too hard for an attacker, and they look for easier targets.

The usual process of a criminal breaking into an account would involve them using a list of a million or more email address, along with a database of billions of possible passwords, and using a high powered computer to attempt combinations over and over again until one works.

When an account is protected by MFA, breaking into that single account would require targeted physical action, such as pickpocketing a device or sim-swapping, then the attacker would have to overcome the devices biometric verification, only then could the criminal begin attempting to guess the password, and each guess would take several seconds, rather than millions per second for non-MFA protected accounts. Its for these reasons that MFA is able to block 99.9% of attempts to illegitmately access accounts.

Almost no criminals have the means to overcome MFA, and even those that do know that they will have much more lucrative results pursuing the other 999,999 accounts, each of which can be targeted in a matter of hours, rather than spending many weeks trying to break into a single MFA protected account.

MFA should be set up where ever it is available, but if that is not possible at the very least it should be enabled for a users more important accounts, such as internet banking and email.

Why is Email so Important?

It's not something often considered, but most modern online system rely on email accounts as a backup verification. If the user forgets their password, the '*I've forgotten my password*' functionality will send a message with password reset instructions to the users emails address.

If a criminal were to gain access to an email account, they can use it to reset many other passwords and ultimately gain access to many other accounts. This is why it's important to have a very strong password/passphrase, which is not used anywhere else, and to enable MFA for email accounts.

Enter Password Managers

Password managers are growing in popularity, and are highly recommended for all business and users.

Password managers randomly generate very complex, very long and unique passwords. They store them securely, along with other account details, so the user doesn't need to remember them on each login. Password managers will also automatically prefill account and password information, greatly improving the experience of users who regularly login into multiple different websites or systems.

Once set up, the user will only need to type one password and then enjoy a seamless, one click login experience while simultaneously getting the benefit of very secure passwords.

Key features of a good password manager are:

- **'No Trust' architecture** – this means all data is encrypted before leaving the device, so even if the password manager infrastructure suffers a breach, the criminals can't read any passwords.
- **Generate passwords** – In order to be effective a Password Manager must generate long, strong, unique and random passwords.
- **Multifactor Authentication** – As a Password Manager will hold all passwords, it is critically important that it is highly secure. A good password manager will have the option for MFA to be used on every login.
- **Breach Monitoring** – No matter how strong a password is, accounts can be compromised if passwords are given to the wrong person as a result of being tricked. Good Password Managers will monitor various dark web and underworld websites, and notify the user if their email addresses are included in the data criminals are exchanging.

Unfortunately, password managers don't always work for every corporate and personal application. They also need an initial password or passphrase from the user, and so the ability to create and remember strong passwords is still an extremely important skill for all users.

Why do I need different passwords?

There are many ways that a criminal could come to learn a password through no fault of the users. Once a criminal has a password, the length and complexity no longer matter.

As soon as the criminal has a password, they will begin trying it on as many systems as possible to see if the user has used the same password on facebook, Instagram, Hotmail, gmail, and so on.
Often this will be automated, with the email address and password combination tried on thousands of websites within seconds.

Other times the process my be more targeted, with the criminal using the email address to locate the user on LinkedIn, finding out where they work, then attempting to use the user name / password combination to access corporate data.

The uniqueness of the password prevents this, and ensures tthat if a password does become known, the breach is contained and the criminal only has access to a single system where the password was first set.

How do criminal's actually steal passwords?

There are several methods criminals could use to obtain a password/passphrase, they include:

- **Brute forcing** - This is the term given to the method discussed earlier of using a computer program to make lots of random guesses very quickly. This is the primary reason we need long and complex passwords/passphrases, as it makes this process much harder, and take much longer.

- **Phisihing** - Pronounced 'fishing', is a social engineering technique where criminals create emails and websites, often using well-known brands, such as google, amazon or financial institutions. They then trick users into entering a username and password, which is then sent to the criminals rather than the legitimate organisation.

- **Breaches** - A breach is when a criminal gains access to a website or system's list of usernames and passwords, often through a security flaw. When this happens the criminals usually gain access to every username and password registered with that website.

  This doesn't just happen to small websites that can't afford good security, some recognisable names have suffered very large breaches of varying severity.

  - **Facebook** - 540,000,000 user records breached
  - **eBay** - 145,000,000 user records breached
  - **Equifax** - 147,900,000 user records breached
  - **LinkedIn** - 165,000,000 user records breached
  - **Yahoo** - 3,000,000,000 user records breached

- **Criminal Collaboration** - after one of the above techniques has been used successfully, criminals will often sell and share the usernames and passwords they have gained access to. In some cases, these are then compiled into large databases that contain millions of stolen email address and password combinations. Manytimes, these large databses will be published publically online, giving access to anyone and everyone.

Feature: How to Create Easy to Remember, Highly Secure Passwords

The best way to set a strong password is to use a password manager, which is covered above. If, however, this is not possible, the below represents the best advice on how to create strong passwords you can easily remember.

Years of '*at least 8 characters, must include lower case, upper case, numbers and special characters*' have actually made our passwords less secure and easier for criminals to guess?

While creating these passwords is better than using a single word, the complexity leads to them being hard for the human brain to remember, and result in passwords being written down and reused with only minor changes. Both of these factors greatly undermine a password's security.

There is a much better way to create passwords that are easy to remember, but still long and strong, which is a Passphrase. A Passphrase is a short phrase in place of a password.

It's unlikely most people could remember lots of different 20 random character passwords, but most people can remember lyrics from their favourite songs, which will contain more than 20 words and hundreds of characters.

To create a passphrase, try this:

First, take six random words, for example: '*crystal apple long truck high jump*'

Next, create a picture of the words in your head, like so:

Finally, make it unique by adding in the name of the service in a random way: '*crystal apple long truck Facebook high jump*' or '*insta crystal apple long truck high jump*'.

Now you have a password that's quite easy to remember, but also 40 characters long and almost impossible to guess.

Even using the best modern computers and techniques, it would take a guessing program longer than the life expectancy of the earth to guess that password!

So, next time your asked to create or change a password, think passphrase.

Conclusion

Cybercriminals have modernised and progressed their capability and collaboration in recent years, and it is no longer acceptable to use the same or similar passwords between systems. Modern software and safeguards have also progressed, and it is no longer necessary to remember or write down large numbers of passwords.

By implementing MFA wherever available, using a modern Password Manager, and creating easy to remember Passphrases when they are needed, anyone make all of their accounts virtually unbreachable, while also reducing the need to remember passwords, all while improving their experience across multiple websites and systems.

Contact Info

+61 8 8238 6500

sales@advance.net.au

https://www.advance.net.au/