Your title here

# Employee guide to essential password security

Your logo here

## In partnership with Password Coach

Version 001000

**The Rexan employee guide to essential password security**



Design and layout by Jana Sokolovskaja at jascreations.com.au



@passwordcoach
www.passwordcoach.com
Patent Pending


# About this book

This e-book presents a solution to the ongoing security challenge of staff password management. In particular, it addresses the difficulties that many have with the creation and protection of security policy compliant passwords.

With the assistance of this simple routine, staff members are guided in the creation and recall of numerous strong and unique passwords, without the need to memorise or record them.

In implementing this routine, the business can ensure that all staff members have the means to be fully comply with the company's security policy without recourse to workarounds, bad security practice and shouting.

The solution works across all platforms and devices, requiring no additional software. It is hosted externally, distributed via email with near zero support from IT and the Risk team. It may be rolled out quickly and efficiently to address a current security pain point. There are a raft of customisation options available for tailoring Password Coach to the business. Full instructions are included, and staff can additionally access a short 60 second training video and supporting content at *www.passwordcoach.com*.

For further details, including **commercials** and **customisation options** please head over to *www.passwordcoach.com/enterprise*. To enquire about Password Coach for your business, please drop us a line at *enterprise@passwordcoach.com*.

Yours sincerely,

Simon
*simon@passwordcoach.com*

Your words here

# Foreword from the CEO

**"Security is not a job for IT, it's a job for all of us"**

Firstly, let me start out by thanking each and every one of you for your collective contribution towards the security and integrity of our business. Without your continued diligence and commitment, we run the very real risk of a system breach, and all of the associated commercial and reputational damage that would inevitably follow. I know that we are all working hard to ensure that such an event never occurs, and I want to re-emphasise our appreciation for your ongoing support and unswerving commitment to the security and future of the business.

And now a word about passwords.

Our passwords are currently our only line of defence in the digital world. It is imperative that we all use strong passwords to secure our systems, both at home and at work. To date, we as a business have pushed the responsibility of creating policy compliant passwords down on each of you individually. And it is fair to say that some of us have struggled with this responsibility. I will be the first to put my hand up and admit that I am one of those people. To be candid, I am not keen on coming up with a new password every month; I find it hard to memorize new passwords, and I really don't take pleasure in burdening our Helpdesk every time I forget one. Sorry Chris!

Well the good news is that we as a business are stepping up to the challenge of great password security and providing everyone with assistance in the form of our very own Password Coach!

Password Coach is a simple routine that helps us all to create and recall policy compliant passwords without the need to commit them to memory or write them down on sticky notes (you know who you are)! I encourage each and every one of you to set aside ten minutes between now and the end of the month to get familiar with the Coach's routine. Thereafter, you will be fully equipped to fully support our critically important security policy, whilst avoiding any of the stress and downtime that occasionally comes with a change of password.

On behalf of the board and the shareholders, I would like to thank you in advance for your participation in the Coach's program and your continued commitment to the security and future of Rexan.

Be safe.

Sincerely,

Lou
President and CEO
Rexan

# Contents

Section **1**

# How to use Password Coach

## It's all about your pattern

The key to Password Coach is having a single, memorable, and yet unpredictable, password pattern. We'll use this pattern in conjunction with the Password Coach keys to generate and retrieve strong and unique passwords.

So let's understand the password pattern in a bit more detail.

## The anatomy of a password pattern

Without knowing it, you may already be using a password pattern in your normal daily business. Keyboard patterns are a pretty common example of a password pattern. The World's Worst Password – **123456** – is a keyboard pattern. But patterns show up in other places, too. I've been using one to derive my ATM PIN for years. In the olden days, when I set my first ATM PIN number, I didn't so much remember the numbers that made up my four-digit PIN, but rather the pattern that my fingers made on the keypad as I tapped in the numbers for the first time. I've remembered the pattern ever since.

Later on, we'll use the same technique, but on a slightly grander scale, to help us generate and recall our strong and unique passwords.

## Shapes and sequences

A password pattern is made up of both a shape and a sequence. Let's use the familiar ATM keypad to understand what we mean by **shape** and **sequence**.

### The pattern shape

In Password Coach, the shape of a password pattern is simply a collection of squares on a Password Coach key card.


**Figure 1.** An ATM PIN password shape

Using our ATM example, we've picked a shape (marked in the dark grey keys) that resembles an L shape on its side. With reference to **Figure 16**, you'll see that the shape chosen for this PIN incorporates the top right corner (number 3), and the entire middle row (numbers 4 to 6) of the ATM keypad.

The shape of our password pattern simply defines which characters are available to us. It doesn't indicate the order the characters will be in to create that super-strong password. For that, we'll need a sequence.

### The pattern sequence

The sequence is the direction in which we travel through our password shape to determine the order of the characters that will make up our password. In this example, our sequence options could include:

- 3456 (horrible, too obvious)
- 3654
- 4563
- and a bunch of less obvious others like 4635


**Figure 2.** An ATM PIN password sequence

As you can see from **Figure 17**, we've elected to start the sequence at 4, go along the entire middle row and then go up to finish on the number 3. This gives us an ATM PIN of 4563.

This is how the password shape and password sequence come together to establish a password pattern. Let's now apply this to the job of securing our sensitive sites and systems.

## Defining your Password Coach password pattern

Like the ATM example above, we are going to define a password pattern in terms of shapes, and a sequence of selections within those shapes. With Password Coach, we've got a much bigger 'keypad' than the 10 digits of our ATMs – we have, in fact, got four 5 by 5 grids.

These grids are based on classic old Bingo cards, which is why we refer to them as Password Coach key cards. Rather than being made up of just numbers, like the example in **Figure 4**, the Password Coach key cards comprise the characters that we need to create secure passwords.

As above, let's work through an example of how we will use Password Coach keys to generate super-secure passwords.

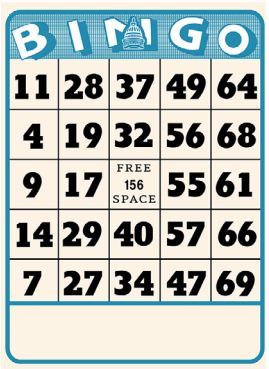



**Figure 3.** A classic Bingo card from the olden days

| ONE | | | | |
|---|---|---|---|---|
| h | x | e | N | + |
| > | d | s | 6 | 5 |
| F | k | m | 9 | V |
| F | 4 | R | m | [ |
| q | ! | W | h | % |

**Figure 4.** A Password Coach key card

## Step 1 – defining your pattern shapes

First off, we need to decide how our pattern will be represented across the Password Coach key cards. The example in **Figure 5** shows an entire Password Coach key, made up of four cards. For clarity, the cards are blank in this example. On each of the cards, we've defined four simple shapes, one per Password Coach key card. These will be the basis of our pattern.

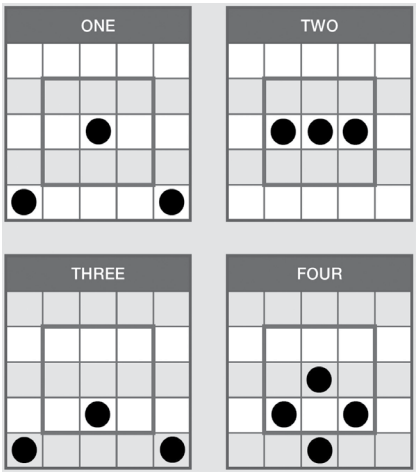



**Figure 5.** Defining a pattern on the key cards

Of course, the shapes can be anything. It's entirely up to you. You can use as many or as few of the cards as you see fit. The only rules are:

### Rule #1 – Don't be predictable

Picking 12 squares in a rectangle on card ONE is about the same as using 123456 as your password. Highly predictable. While you want to be able to remember your pattern, you don't want people to be able to

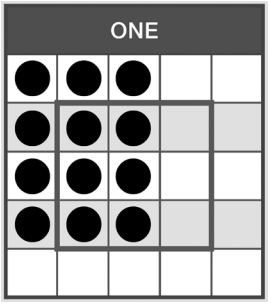



**Figure 6.** How NOT to define your pattern

guess it. Also, marking out an S shape if your name is Sam is also a bit obvious. You get the idea.

### Rule #2 – Make lots of selections

We need our password to be at least 12 characters long. Each of our pattern selections will correspond to a password character, so your pattern should have at least 12 selections in it.

### Rule #3 – Create a pattern that you can remember

You'll find that remembering a pattern is much easier than remembering any of the passwords that it generates. So this shouldn't be a problem.

### Rule #4 – Use the whole key card

Each of the Password Coach key cards includes shading and a guide box in the centre. Both of these features have been designed to help you visually overlay your pattern on each of the key cards. Your pattern can use any part of the key cards – so don't feel that you need to limit your selections to just the inner box.

### Rule #5 – Don't copy the pattern in Figure 6

Copying what you see here breaks Rule #1. It's too predictable. Come up with your own. Remember, you only ever need to come up with one pattern. So make it a good one!

### Inspiration for creating your unique password pattern

Patterns are everywhere. The letters of the alphabet form patterns that can be used to generate a password pattern. So do the letters of the Braille alphabet. So do the letters of the Morse code alphabet. And so do the numbers of the face of a dice. If you'd like some inspiration for coming up with your own unique password pattern, then head over to *www.passwordcoach.com/inspiration*.

## Step 2 – defining your pattern sequence

Much like the shapes that you've picked, the sequence of your selections is entirely your choice.

In **Figure 7**, we've marked our key cards with the sequence that we'll use to travel through our pattern. In this example, we're going in order from card 1 to 2 to 3 and then to 4. Of course, you don't need to do that. You can pick any sequence that you want. You don't even need

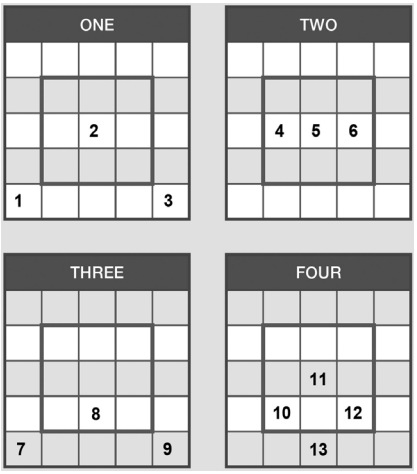



**Figure 7.** Defining the pattern sequence

to use all of the cards. But for now, and for the sake of clarity, we've kept things simple.

That's the preparation done. We have our pattern defined. We only ever need to do that once. Now we can go ahead and use our pattern to create our passwords.

## Using Password Coach to generate strong password after strong password

Now that all the hard work has been done, and we've committed our password pattern to memory, we're ready to start creating super-strong passwords to protect all of our sensitive systems. Let's quickly run through the process for doing that:

1. Decide which system you are going to secure, and pick at random a key in the book with which to secure it
2. Mentally overlay your password pattern on the key cards
3. Journey through the cards according to your sequence and make a note of password characters that you hit on the way through.

## Step 1 – define the system that we are securing

Here's the scenario.

| Tumblr | 15 |
|---|---|

We've just read that the social media website Tumblr got hacked again, and that we should change our Tumblr password. We're going to use Password Coach to help us do that.

Firstly, we'll use the book's index to navigate to the Password Coach Index page, and select a key that we haven't yet used – Key 15 is free so we'll use that one.

Key 15 is of type Strong, which is perfect for a social media platform laden with reputational risk. We type 'Tumblr' into the line of the Index that corresponds to Key 15, and hit Save, to record our selection. It is important that you Save all edits that you make to the document, otherwise you will lose them.

## Step 2 – overlay your pattern on the key cards

Next, we'll click on '15' in the index to be taken to Key 15 in the book. Now we can generate a password using our pattern.

| SYSTEM | Tumblr | KEY 15 |
|---|---|---|

With our password pattern indelibly etched into our memory, we read off the password characters from the key cards based on our pattern and our sequence, ignoring all of the other characters on the cards.

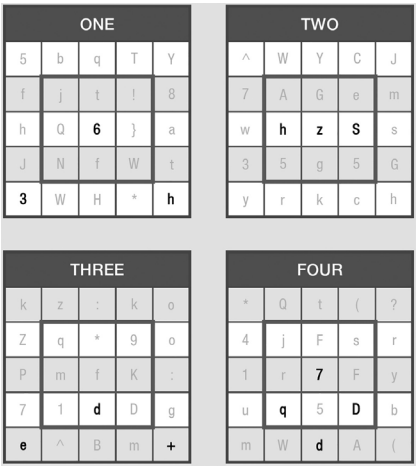



**Figure 8.** Overlaying a pattern onto the key cards

In **Figure 8**, we've marked out our pattern on the sample Key 15 cards, highlighting the password characters that match the selections of our pattern.

### Step 3 – read off the password

Based on our password pattern sequence (see **Figure 7**), Key 15 has given us the following super-strong password for our Tumblr account:

**36hhzSed+q7Dd**

OK. That looks pretty strong, but let's test the strength of our new Tumblr password courtesy of *www.passwordmeter.com*.

| Test Your Password | | Minimum Requirements |
|---|---|---|
| Password: | 36hhzSed+q7Dd | • Minimum 8 characters in length<br>• Contains 3/4 of the following items:<br>- Uppercase Letters<br>- Lowercase Letters<br>- Numbers<br>- Symbols |
| Hide: | ☐ | |
| Score: | 100% | |
| Complexity: | Very Strong | |

As expected, 100%. Rock. Solid.

You're done. Your first strong and unique password is in the bag.

**What if the generated password isn't permitted by the system that you are securing?**

In rare cases, certain systems bar the use of selected symbols or special characters, such as $. If the password that you have generated includes non-supported characters, you can either choose to leave them out (i.e. just skip over the problem characters), or flip to another key and generate a new password that is going to work on their finicky system.

## Retrieving the password

The next time that we want to log into Tumblr with the new password, we just consult the Password Coach book, locate the correct page for Tumblr, and read off the password based on our pattern.

**That's it.**

**You now have all the skills and tools needed to secure all of your critical and sensitive online systems by remembering nothing more than a single pattern.**

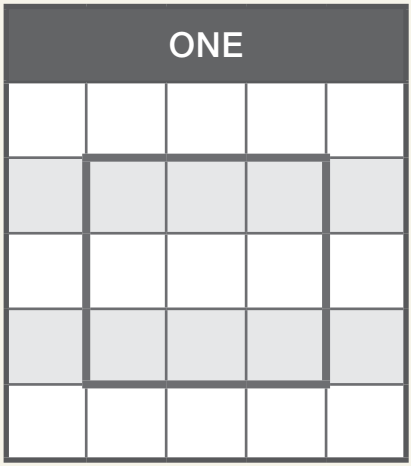
To watch a quick video on how to use Password Coach, head over to *www.passwordcoach.com/use*.

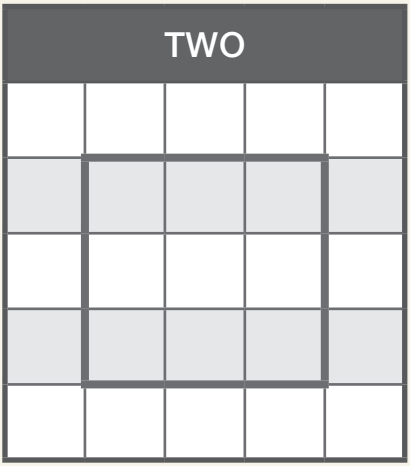
Section **2**

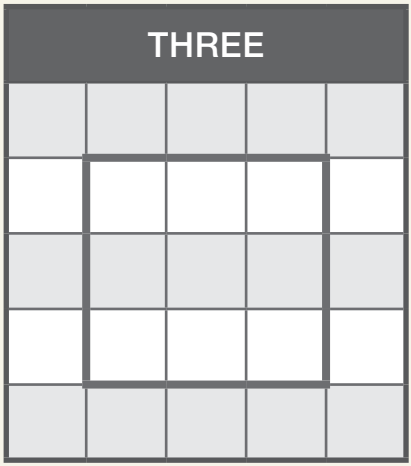
# Pattern Practice

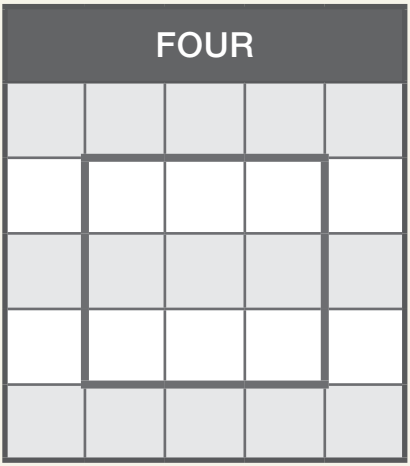
This section has a handful of blank Password Coach keys for you to mark up a pattern or two. If you want to create a reminder of your pattern, print out one of the practice pages, mark it up with your pattern and put it somewhere safe. Check out www.password-coach.com/faq for tips on printing.

NOTES

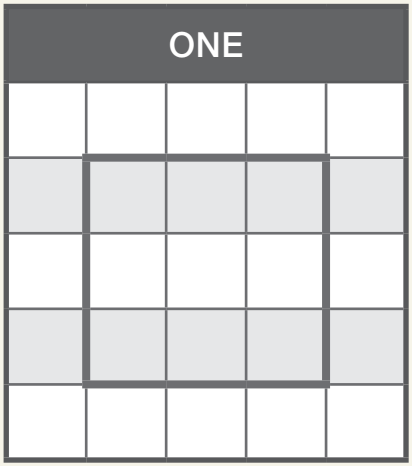


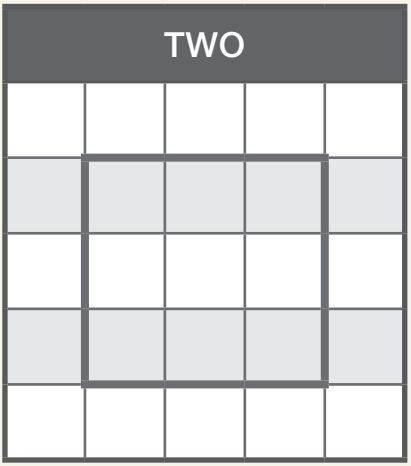



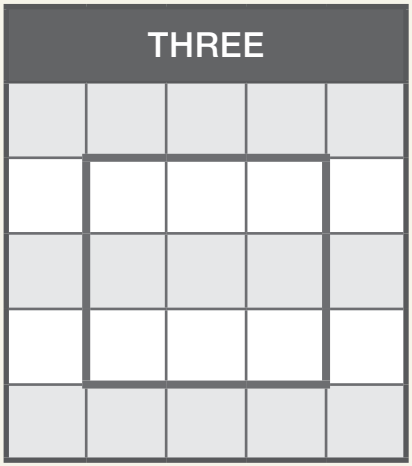



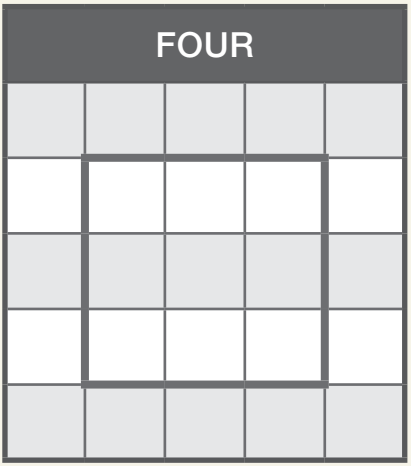



NOTES

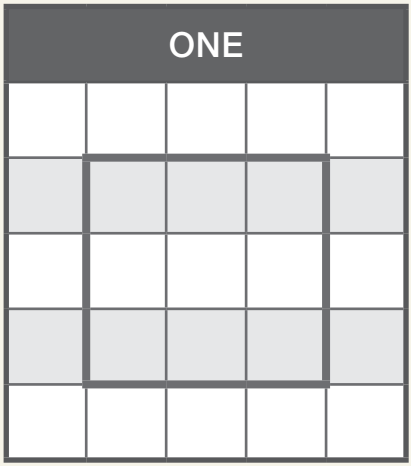


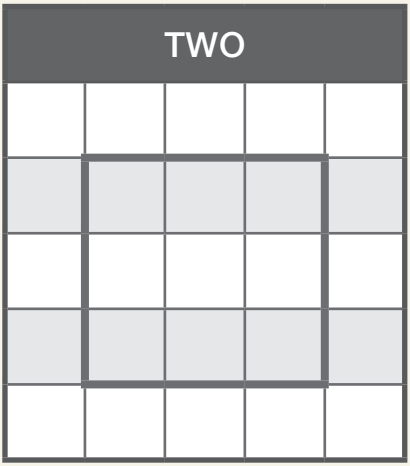



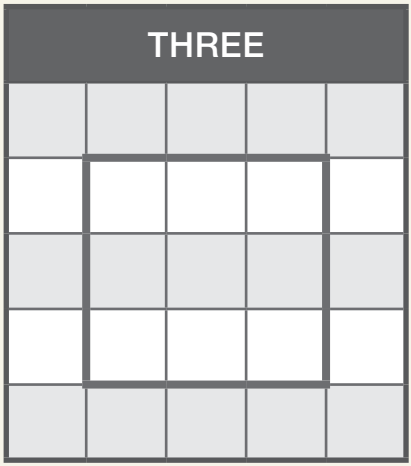



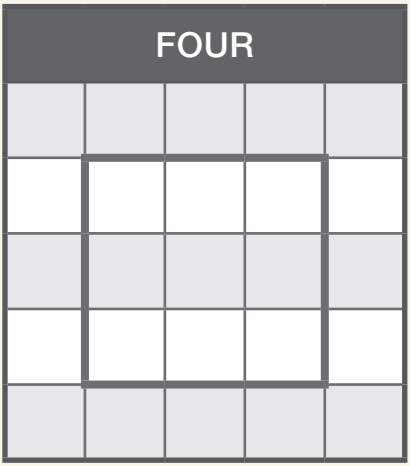



NOTES



Section **3**

# The Password Coach Index

The following pages contain the Index to help you quickly find the appropriate Password Coach key required to generate and recall a password for any given site or system. It's your job to maintain the Index. To do this, you need to write the name of the system that you are securing alongside the number of the key that you used to generate the password for that system.

There are three types of Password Coach key: Strong, Phone-friendly and PIN. The key Type is confirmed at the bottom of each key page. An explanation of each type and when to use it is provided below.

## Strong keys (Keys 1–4)

Used for securing our more critical and most sensitive systems. Strong keys generate strong passwords which can contain up to four keyboard character types: uppercase letters, lowercase letters, numbers and symbols.

## Phone-friendly keys (Keys 101–104)

The soft keyboard on your mobile phone makes entering strong passwords a bit laborious. Phone-friendly keys are included that comprise just lowercase letters and numbers. Although the passwords generated here are not super-strong, a 12-character phone-friendly password is sufficiently strong to secure an online system. You can also add a couple of symbols and uppercase letters at the start or end of a phone-friendly password to beef it up, should you wish.

### Password policy guidance for phone-friendly keys

While phone-friendly keys generate passwords that are a tad easier to enter than strong passwords, they may not comply with the password

policy of the website that you are securing. We have found this to be the case in about 20% of the websites that we reviewed. You won't, for example, be able to secure your Mailchimp, Adobe or Apple accounts with a phone-friendly password. So before you opt for a phone-friendly password, you should check to see if the account that you are securing is going to accept a password just made up of lowercase letters and numbers.

## PIN keys (Keys 201–204)

We use Personal Identification Numbers (PINs) as an alternative to passwords in a number of places – at the ATM, building entry systems, alarm systems, mobile phones, banking apps, phone banking and so on. To support the generation and recall of your PINs, a number of PIN keys comprising just numbers are included.

If you need more keys to secure more systems, then head over to *store.passwordcoach.com/upgrade* to extend your version of the Password Coach e-book with an extra 200 keys.

# Strong keys


| Websites & Systems | Key # |
|---|---|
| Single Sign-on 2017 Q1 | 1 |
| Single Sign-on 2017 Q2 | 2 |

| Websites & Systems | Key # |
|---|---|
| Single Sign-on 2017 Q3 | 3 |
| Single Sign-on 2017 Q4 | 4 |

# Phone-friendly keys


| Websites & Systems | Key # |
|---|---|
| Phone | 101 |
| Tablet | 102 |

| Websites & Systems | Key # |
|---|---|
| Facebook | 103 |
| Webmail | 104 |

# PIN keys


| Websites & Systems | Key # |
|---|---|
| Corp AMEX | 201 |
| Banking app | 202 |

| Websites & Systems | Key # |
|---|---|
| Security door | 203 |
| Alarm | 204 |



always remember to save your changes

Section **4**

# Strong Keys

We need to secure our most sensitive and important systems with strong passwords. These are comprised of a random sequence of uppercase letters, lowercase letters, numbers and symbols. This section is where we generate and retrieve strong passwords.

In this section, you'll find 4 Password Coach keys to enable you to secure your most critical systems.

If you haven't already done so, head over to the section entitled 'How to use Password Coach' for guidance on how to set and retrieve your passwords with Password Coach.

Or catch the video at *www.passwordcoach.com/use*.

For those readers already au fait with the Password Coach system, the following summary assumes that you've settled on your password pattern, and have committed that to memory.

## Generating a new strong password

1. Decide which system you are going to secure with a strong password
2. Pick a strong Password Coach key from the book at random
3. Mentally overlay your pattern on the cards to reveal your password
4. In the 'SYSTEM' box at the top of the selected Password Coach key, write the name of the system that you are securing
5. In the Index, again write the name of the system you are securing on the line corresponding to selected Password Coach key

## Retrieving an existing strong password

1. Refer to the Index to locate the key used to secure the system that you are logging into
2. Flip to the appropriate page in the Password Coach book
3. Mentally overlay your password pattern onto the Password Coach key cards
4. Read off your password from the page

Here are 4 Password Coach keys to help you generate your strong passwords.

NOTES

| ONE | | | | |
|---|---|---|---|---|
| a | / | T | E | 8 |
| = | F | a | t | M |
| 3 | a | 3 | y | u |
| 8 | a | @ | U | 8 |
| % | @ | U | a | 3 |

| TWO | | | | |
|---|---|---|---|---|
| c | / | u | C | u |
| 6 | y | t | s | X |
| > | u | ^ | 8 | u |
| / | 8 | U | 8 | u |
| t | M | u | ^ | 3 |

| THREE | | | | |
|---|---|---|---|---|
| M | u | C | c | = |
| * | > | T | 8 | F |
| 8 | F | u | V | s |
| t | 8 | V | 6 | t |
| > | * | E | u | s |

| FOUR | | | | |
|---|---|---|---|---|
| F | t | ^ | @ | c |
| > | 3 | ! | 3 | 6 |
| 8 | T | u | > | J |
| u | u | * | E | a |
| F | E | 3 | 3 | 8 |

NOTES

| ONE | | | | |
|---|---|---|---|---|
| ^ | c | t | 3 | T |
| d | ^ | t | / | 3 |
| 3 | V | % | c | 3 |
| C | C | % | P | 7 |
| x | 3 | d | Z | / |

| TWO | | | | |
|---|---|---|---|---|
| 8 | Z | c | c | / |
| a | x | V | d | 3 |
| s | C | t | Z | * |
| ^ | C | 7 | c | ^ |
| F | 3 | = | 7 | s |

| THREE | | | | |
|---|---|---|---|---|
| n | x | n | 7 | 3 |
| = | F | ^ | C | s |
| Z | A | % | A | n |
| c | d | / | 7 | c |
| 7 | * | F | ^ | 3 |

| FOUR | | | | |
|---|---|---|---|---|
| 7 | 3 | a | V | A |
| s | H | 3 | a | x |
| c | c | / | d | t |
| 7 | * | 7 | H | = |
| 3 | n | C | T | c |

NOTES

| ONE | | | | |
|---|---|---|---|---|
| $ | s | 6 | r | 6 |
| R | r | c | 7 | # |
| 7 | R | H | x | v |
| V | / | 7 | s | 7 |
| 6 | x | 7 | # | 6 |

| TWO | | | | |
|---|---|---|---|---|
| / | h | r | z | # |
| # | U | 6 | x | / |
| H | / | p | 6 | p |
| x | r | R | v | 7 |
| / | > | $ | $ | R |

| THREE | | | | |
|---|---|---|---|---|
| X | h | z | U | h |
| R | z | R | 7 | h |
| 6 | 6 | 7 | v | 6 |
| 6 | $ | Z | X | V |
| 7 | V | v | X | 6 |

| FOUR | | | | |
|---|---|---|---|---|
| h | 6 | U | 6 | h |
| V | V | h | R | # |
| U | / | 7 | 7 | / |
| X | V | c | V | s |
| $ | X | V | h | Z |

NOTES

| ONE | | | | |
|---|---|---|---|---|
| $ | % | 7 | J | Z |
| F | 8 | ^ | 3 | 8 |
| 8 | p | q | X | z |
| 3 | h | $ | ^ | c |
| 8 | q | P | < | Z |

| TWO | | | | |
|---|---|---|---|---|
| % | c | E | = | $ |
| h | K | m | P | 3 |
| 3 | $ | p | 8 | h |
| < | X | p | p | V |
| = | c | q | m | 3 |

| THREE | | | | |
|---|---|---|---|---|
| A | 8 | / | V | 3 |
| p | z | p | P | A |
| P | 7 | 3 | % | $ |
| $ | > | p | A | z |
| p | > | c | * | F |

| FOUR | | | | |
|---|---|---|---|---|
| 8 | c | c | c | 7 |
| m | M | 3 | p | ! |
| z | Z | ! | p | h |
| 8 | 3 | < | * | V |
| F | 8 | p | p | z |

Section **5**

# Phone-friendly Keys

This section is where we generate and retrieve phone-friendly passwords. Phone-friendly passwords respect the fact that the keyboard on our phone is often smaller than a standard keyboard, and entering a mix of character types can be a pain. For that reason, phone-friendly passwords are limited to lowercase letters and numbers only – the characters that are already (mostly) on your phone's default *soft* keyboard.

In this section you'll find 4 Password Coach keys to enable you to generate and retrieve phone-friendly passwords.

If you haven't already done so, head over to the section entitled 'How to use Password Coach' for guidance on how to set and retrieve your passwords with Password Coach.

Or catch the video at *www.passwordcoach.com/use*.

For those readers already au fait with the Password Coach system, the following summary assumes that you've settled on your password pattern, and have committed that to memory.

## Generating a new phone-friendly password

1. Decide which system you are going to secure with a phone-friendly password
2. Pick a phone-friendly Password Coach key from the book at random
3. Mentally overlay your pattern on the cards to reveal your password
4. In the 'SYSTEM' box at the top of the selected Password Coach key, write the name of the system that you are securing
5. In the Index, again write the name of the system you are securing on the line corresponding to selected Password Coach key

## Retrieving an existing phone-friendly password

1. Refer to the Index to locate the key used to secure the system that you are logging into
2. Flip to the appropriate page in the Password Coach book
3. Mentally overlay your password pattern onto the Password Coach key cards
4. Read off your password from the page

## Converting a phone-friendly password to a strong password

If you run out of strong password keys, you can always add a couple of symbols and uppercase letters to the start or end of a phone-friendly password to convert it to a strong one. For example:

**Strong password = 'B' + phone-friendly password + 'H^'**

## When NOT to use a phone-friendly password

A 12-character phone-friendly password is sufficiently strong to secure an online system (e.g. Gmail), but should not be used to secure any system that can be attacked in an offline attack. Specifically, a phone-friendly password should not be used to secure your home wireless network.

If you need a refresher on the difference between an online and offline system attack, head over to '*Section 5. Guessing your email password*' on page 43.

From here, you'll find 4 Password Coach keys for generating phone-friendly passwords.

NOTES

| ONE | | | | |
|---|---|---|---|---|
| 6 | s | y | g | 6 |
| q | b | 4 | q | 3 |
| x | c | 3 | 6 | h |
| 6 | j | k | y | x |
| 3 | 3 | 4 | b | 6 |

| TWO | | | | |
|---|---|---|---|---|
| q | h | f | 7 | 6 |
| 7 | 6 | q | h | 8 |
| 8 | x | 3 | h | 6 |
| j | t | 7 | q | x |
| 3 | g | 6 | s | y |

| THREE | | | | |
|---|---|---|---|---|
| 3 | 3 | y | 4 | 7 |
| 6 | z | k | 3 | 3 |
| 6 | 3 | 6 | 3 | j |
| 6 | f | 3 | y | 3 |
| 6 | f | g | h | q |

| FOUR | | | | |
|---|---|---|---|---|
| 6 | b | 3 | x | j |
| 8 | s | 3 | x | 4 |
| b | x | z | t | c |
| 7 | h | 6 | k | x |
| k | j | 7 | 6 | k |

NOTES

| ONE | | | | |
|---|---|---|---|---|
| 4 | 9 | 4 | e | w |
| 9 | x | g | 9 | 4 |
| n | w | g | 8 | 7 |
| 9 | u | n | s | 8 |
| 3 | e | j | m | w |

| TWO | | | | |
|---|---|---|---|---|
| b | z | g | 4 | x |
| s | j | 6 | w | 4 |
| w | 7 | 8 | j | e |
| 6 | n | s | x | n |
| 7 | x | x | n | b |

| THREE | | | | |
|---|---|---|---|---|
| b | 9 | 9 | c | 3 |
| t | j | e | c | 6 |
| 6 | w | x | n | 6 |
| c | c | d | e | 6 |
| 9 | 4 | 4 | 3 | b |

| FOUR | | | | |
|---|---|---|---|---|
| z | 8 | n | t | e |
| 4 | b | 8 | c | u |
| 9 | 4 | g | m | n |
| 4 | 8 | c | b | 7 |
| 3 | 4 | s | j | c |

NOTES

| ONE | | | | |
|---|---|---|---|---|
| 4 | 8 | x | 4 | j |
| 8 | 8 | t | p | 4 |
| 6 | 6 | 4 | f | 6 |
| q | k | c | j | 8 |
| 8 | j | 9 | x | 6 |

| TWO | | | | |
|---|---|---|---|---|
| n | 6 | b | b | 4 |
| 9 | c | 9 | j | 8 |
| j | t | 4 | x | 9 |
| q | r | d | n | q |
| 8 | x | t | 7 | t |

| THREE | | | | |
|---|---|---|---|---|
| w | n | f | p | d |
| 9 | r | 4 | p | f |
| r | k | q | b | 4 |
| n | 6 | r | q | 4 |
| 8 | t | x | 6 | 8 |

| FOUR | | | | |
|---|---|---|---|---|
| 8 | 8 | p | 8 | b |
| w | q | p | 4 | r |
| 9 | 8 | q | b | f |
| f | r | n | f | p |
| q | 6 | 6 | 7 | 9 |

NOTES

| ONE | | | | |
|---|---|---|---|---|
| 6 | h | t | t | t |
| 8 | 7 | a | 4 | f |
| d | 7 | 4 | d | h |
| 7 | 7 | v | 3 | k |
| a | 8 | k | 7 | a |

| TWO | | | | |
|---|---|---|---|---|
| 7 | 7 | y | 3 | b |
| z | b | 6 | c | 6 |
| c | b | 3 | k | v |
| k | 3 | b | d | y |
| 6 | b | k | 7 | g |

| THREE | | | | |
|---|---|---|---|---|
| 9 | v | 9 | 4 | b |
| f | k | 3 | 7 | z |
| c | d | d | y | 4 |
| z | 3 | f | 7 | k |
| 4 | 4 | 6 | 7 | j |

| FOUR | | | | |
|---|---|---|---|---|
| 3 | y | 6 | b | d |
| j | 9 | 6 | z | t |
| f | c | v | 3 | b |
| 8 | 3 | 8 | 3 | 6 |
| 3 | 8 | 7 | z | k |

Section **6**

# The PIN Keys

The following Password Coach keys have been designed to help you set PIN numbers. PIN numbers are required on quite a few systems – your bank and credit card, your frequent flyer membership, the code on the home alarm, the security door at work, your tablet device, mobile phone apps and so on.

As your PINs are much shorter than your other passwords, your password pattern will also be shorter. You can either come up with a new pattern just for PINs, or go with any subset of the existing pattern. Your call.

You may also find that you need multiple PIN patterns, because of the variable length of the PINs on the systems you need to secure. In which case, using the first four or six (or however many) selections in your pattern might be a better bet than having to remember multiple patterns. Again, we'll leave that decision to you.

If you haven't already done so, head over to the section entitled 'How to use Password Coach' for guidance on how to set and retrieve your passwords with Password Coach.

Or checkout the video at *www.passwordcoach.com/use*.

For those readers already familiar with the Password Coach system, the following summary assumes that you've settled on your password pattern, and have that committed to memory.

## Generating a new PIN

1. Decide which system you are going to secure with a PIN
2. Pick a PIN Password Coach key from the book at random
3. Mentally overlay your PIN pattern on the cards to reveal your PIN

4. In the 'SYSTEM' box at the top of the selected Password Coach key, write the name of the system that you are securing
5. In the Index, again write the name of the system you are securing on the line corresponding to selected Password Coach key

## Retrieving an existing PIN

1. Refer to the Index to locate the Key used to secure your PIN-protected system
2. Flip to the appropriate page in the Password Coach book
3. Mentally overlay your PIN pattern onto the Password Coach key cards
4. Read off your password from the page

From here, you'll find 4 Password Coach keys for generating PINs.

NOTES

| ONE | | | | |
|---|---|---|---|---|
| 4 | 8 | 9 | 3 | 4 |
| 4 | 8 | 1 | 4 | 8 |
| 7 | 6 | 6 | 3 | 0 |
| 7 | 9 | 8 | 7 | 1 |
| 6 | 3 | 5 | 4 | 9 |

| TWO | | | | |
|---|---|---|---|---|
| 1 | 1 | 5 | 4 | 0 |
| 2 | 7 | 2 | 8 | 3 |
| 5 | 9 | 2 | 7 | 1 |
| 3 | 2 | 6 | 5 | 9 |
| 8 | 2 | 6 | 3 | 8 |

| THREE | | | | |
|---|---|---|---|---|
| 1 | 8 | 8 | 8 | 8 |
| 1 | 3 | 8 | 8 | 7 |
| 7 | 9 | 5 | 7 | 0 |
| 4 | 0 | 4 | 5 | 1 |
| 6 | 9 | 5 | 9 | 3 |

| FOUR | | | | |
|---|---|---|---|---|
| 3 | 8 | 9 | 3 | 4 |
| 2 | 3 | 7 | 6 | 9 |
| 9 | 6 | 7 | 6 | 8 |
| 2 | 4 | 6 | 5 | 1 |
| 8 | 8 | 4 | 0 | 1 |

NOTES

| ONE | | | | |
|---|---|---|---|---|
| 8 | 4 | 0 | 1 | 3 |
| 0 | 8 | 8 | 7 | 8 |
| 0 | 8 | 7 | 1 | 7 |
| 0 | 7 | 7 | 3 | 2 |
| 5 | 1 | 0 | 5 | 3 |

| TWO | | | | |
|---|---|---|---|---|
| 8 | 0 | 0 | 5 | 5 |
| 2 | 1 | 0 | 3 | 0 |
| 1 | 2 | 9 | 1 | 7 |
| 7 | 0 | 0 | 7 | 1 |
| 0 | 2 | 7 | 0 | 6 |

| THREE | | | | |
|---|---|---|---|---|
| 1 | 9 | 7 | 0 | 9 |
| 4 | 1 | 7 | 5 | 6 |
| 1 | 0 | 4 | 6 | 7 |
| 3 | 5 | 0 | 1 | 5 |
| 8 | 2 | 2 | 3 | 6 |

| FOUR | | | | |
|---|---|---|---|---|
| 7 | 1 | 6 | 4 | 2 |
| 8 | 0 | 2 | 4 | 1 |
| 5 | 4 | 1 | 6 | 8 |
| 3 | 3 | 2 | 1 | 7 |
| 8 | 2 | 9 | 7 | 4 |

NOTES

| ONE | | | | |
|---|---|---|---|---|
| 2 | 5 | 2 | 0 | 3 |
| 1 | 4 | 7 | 5 | 5 |
| 3 | 9 | 7 | 6 | 9 |
| 2 | 4 | 8 | 5 | 8 |
| 5 | 0 | 3 | 5 | 5 |

| TWO | | | | |
|---|---|---|---|---|
| 2 | 0 | 0 | 5 | 3 |
| 3 | 1 | 1 | 0 | 5 |
| 3 | 0 | 2 | 9 | 2 |
| 0 | 4 | 0 | 0 | 8 |
| 2 | 3 | 0 | 3 | 6 |

| THREE | | | | |
|---|---|---|---|---|
| 7 | 6 | 7 | 2 | 5 |
| 7 | 9 | 6 | 7 | 4 |
| 0 | 9 | 7 | 3 | 2 |
| 4 | 1 | 4 | 1 | 1 |
| 2 | 4 | 3 | 2 | 4 |

| FOUR | | | | |
|---|---|---|---|---|
| 3 | 1 | 2 | 5 | 9 |
| 8 | 9 | 4 | 2 | 6 |
| 1 | 3 | 9 | 2 | 3 |
| 1 | 4 | 8 | 1 | 8 |
| 7 | 5 | 9 | 4 | 3 |

NOTES

| ONE | | | | |
|---|---|---|---|---|
| 7 | 8 | 6 | 5 | 7 |
| 2 | 1 | 6 | 5 | 3 |
| 9 | 5 | 1 | 0 | 2 |
| 3 | 8 | 9 | 1 | 5 |
| 1 | 2 | 4 | 2 | 3 |

| TWO | | | | |
|---|---|---|---|---|
| 2 | 7 | 6 | 0 | 1 |
| 2 | 9 | 6 | 5 | 2 |
| 0 | 8 | 8 | 2 | 1 |
| 9 | 9 | 6 | 2 | 6 |
| 4 | 1 | 8 | 9 | 1 |

| THREE | | | | |
|---|---|---|---|---|
| 3 | 1 | 2 | 7 | 3 |
| 6 | 4 | 9 | 6 | 9 |
| 9 | 2 | 5 | 2 | 9 |
| 2 | 9 | 7 | 4 | 5 |
| 7 | 6 | 9 | 4 | 4 |

| FOUR | | | | |
|---|---|---|---|---|
| 5 | 5 | 1 | 1 | 1 |
| 3 | 2 | 0 | 1 | 5 |
| 0 | 2 | 0 | 9 | 0 |
| 2 | 5 | 4 | 1 | 9 |
| 4 | 3 | 2 | 4 | 8 |

# Glossary

| | |
|---|---|
| **Password Coach** | A method for creating and retrieving strong passwords without the need to remember them, write them down or store them digitally |
| **The password problem** | The only way to truly secure our password-protected systems is through the use of strong and unique passwords, and yet we choose not to use them because we have no reliable way of remembering them |
| **A strong password** | A password that is made up of an unpredictable sequence of 12 or more uppercase and lowercase letters, numbers and symbols. A strong password will be unique to you and cannot be guessed by even the most powerful computer |
| **Password Coach key card** | A 5 by 5 grid, similar to a Bingo card, containing all of the characters required to set and retrieve strong passwords |
| **Password Coach key** | A page in the Password Coach book comprising four Password Coach key cards used to set and retrieve a single password |
| **A phone-friendly password** | A password comprising an unpredictable sequence of 12 or more lowercase letters and numbers, being easy to enter into a smartphone's soft keyboard |
| **Password Coach key index** | The Index is used to assign a specific Password Coach key to a specific system. The index is manually maintained listing all systems secured, and the corresponding Password Coach key used. |
| **Password pattern** | A set of selections from one or more Password Coach key cards, used as the basis for setting and retrieving passwords |
| **Password sequence** | The order in which selections are made within a password pattern. The password sequence, in combination with the password pattern, will reveal a unique password from every Password Coach key. |
| **Password visualisation** | The process of mentally overlaying a password pattern onto a Password Coach key to reveal a password |

**Character type** The characters used to define strong passwords are of four character types – uppercase and lowercase letters, numbers and symbols

**Characters** Characters are used to form individual passwords. For the generation of strong passwords, Password Coach keys comprise 100 characters from all four character types. For the generation of phone-friendly passwords, Password Coach keys comprise 100 characters from two character types – lowercase letters and numbers. For the generation of PINs, Password Coach keys comprise 100 characters from one character type – numbers only

# Password Coach

fully customisable

We've all got a problem with passwords. The experts have been telling us for years that we are at risk of being hacked if we don't use strong and unique passwords. But we've been powerless to take that advice because of the inherent limitations of human memory. We simply can't remember more than a handful of passwords. It's not our fault. We just weren't born to memorise stuff like $ek*om@s!Q9.

So let's stop trying.

Let's instead try something a bit more people-friendly.

With Password Coach, we can now generate an endless stream of expert-approved passwords by remembering nothing more than a single pattern.

Passwords that we don't need to remember, passwords that we don't need to write down and passwords that don't go anywhere near "the cloud".

Finally, we can all throw away all of our risky, re-used passwords for something a whole lot more secure.

Password Coach. Secure and people-friendly. About time.