THE PROOF SERIES

A SENIOR'S SIMPLE GUIDE TO PASSWORDS

Password Proof

One safe sign-in at a time.



John Marshall

PROUDLY CANADIAN



PROUDLY CANADIAN

FREE SAMPLE CHAPTER

By John Marshall

www.buyproof.ca

UNDERSTAND THE LOCKS

Why passwords matter

A password protects whatever sits behind it: messages, money, photos, or identity.

Account › Password › Second factor › Safer sign-in

1. List the kinds of information in the account: personal messages, purchases, health details, or financial records.

2. Ask what someone could do if they entered as you: read, buy, impersonate, or reset other accounts.

3. Treat the password as one part of the lock, not the whole security plan.

4. Protect important accounts with a unique password and a second factor.

! **Good to know:** Your email password deserves extra care because email is often used to reset other accounts.

Take care: A low-balance or rarely used account can still reveal useful personal information.

TALE

PASSWORD PROOF STORY

A familiar moment

Frank once said his grocery account was not important. Then he remembered it stored an address, order history, and payment method.

UNDERSTAND THE LOCKS

Email is the master key

Control of your main email can lead to control of many other accounts.

Main email › Reset links › Other accounts

1. Identify the email address used for banking, shopping, social media, and password resets.
2. Give that email a password used nowhere else.
3. Turn on multi-factor authentication for it.
4. Check that its recovery phone number and recovery email are current.

! **Good to know:** Protect email first, then work outward to financial, health, shopping, and social accounts.

Take care: Never use an email account you cannot reliably access as the only recovery route.

TALE

PASSWORD PROOF STORY

A familiar moment

Lena had twelve accounts but one email address. Securing that inbox made the rest of the cleanup much easier.

UNDERSTAND THE LOCKS

Password, PIN, and passcode

These secrets look similar, but they may protect different doors.

Phone PIN › Email password › Vault password

1. Use an account password to sign in to an online service.
2. Use a device PIN or passcode to unlock a phone or computer locally.
3. Use a password-manager primary password to open your password vault.
4. Do not assume changing one automatically changes the others.

! **Good to know:** Label instructions by door: “phone PIN,” “email password,” or “vault password.”

Take care: Never reveal any of these secrets to an unsolicited caller.

TALE

PASSWORD PROOF STORY

A familiar moment

Arthur changed his email password three times while trying to fix his phone PIN. Both devices remained politely unconvinced.

UNDERSTAND THE LOCKS

How passwords are stolen

Most criminals do not sit guessing one character at a time like a movie villain.

Old breach › Reused password › New account

1. Expect reused passwords from old breaches to be tried on new accounts.
2. Expect fake messages and copied sign-in pages designed to collect what you type.
3. Expect convincing calls that ask for a code or remote access.
4. Reduce the risk with unique passwords, updates, careful sign-ins, and MFA.

! **Good to know:** A strong password cannot protect you if you type it into a fake page.

Take care: If a message scares you into immediate action, stop and open the official app yourself.

TALE

PASSWORD PROOF STORY

A familiar moment

The villain does not need a dark room and six monitors. Sometimes all it takes is a rushed click before breakfast.

UNDERSTAND THE LOCKS

Three rules beat twenty tricks

A good password is long, unique, and secret.

LONG › UNIQUE › SECRET

1. Make it long enough for the account's rules; 15 or more characters is a strong target when possible.
2. Use it for one account only.
3. Keep it out of email, text messages, and unlocked notes.
4. Let a password manager create random passwords when possible.

! **Good to know:** Length and uniqueness matter more than decorating one familiar word with predictable symbols.

Take care: Do not use examples printed in any book, including this one.

TALE

PASSWORD PROOF STORY

A familiar moment

"Garden1!" may satisfy a form, but a criminal has seen that gardening trick before.

UNDERSTAND THE LOCKS

Build a memorable passphrase

A passphrase joins several unrelated words into one long password you can remember.

Unrelated word › Unrelated word › Unrelated word › Unrelated word

1. Choose four to seven unrelated words that do not form a famous quotation.
2. Avoid names, birthdays, addresses, teams, pets, and facts visible online.
3. Add spaces or punctuation only if the account allows them.
4. Practise typing the phrase accurately before saving it.

! **Good to know:** Use a passphrase for the one or two secrets you must remember, especially your password-manager primary password.

Take care: Never use the sample structure itself as your password. Make your own words.

TALE

PASSWORD PROOF STORY

A familiar moment

Ruth chose words from four unrelated objects in imaginary rooms. Odd? Yes. Memorable? Also yes.

UNDERSTAND THE LOCKS

Let randomness do the work

Randomly generated passwords are ideal for accounts because you do not need to remember them.

Email login

Bank login

Shopping login

1. Open the password generator in your manager.
2. Choose a long password; 16 or more characters is a practical default when the site accepts it.
3. Include letters, numbers, and symbols if the site requires them.
4. Save it in the manager before leaving the change- password screen.

! **Good to know:** When a website rejects a generated password, adjust only what the site requires.

Take care: Do not shorten a random password just to make it easier to type; use autofill instead.

TALE

PASSWORD PROOF STORY

A familiar moment

A generated password may look like a cat walked across the keyboard. That is the cat's finest security work.

UNDERSTAND THE LOCKS

Keep personal clues out

Information that feels private may already be visible in public records or social posts.

Public clue › Easy guess › Account entry

1. Leave out birth dates, anniversaries, street names, and telephone digits.
2. Leave out names of children, grandchildren, pets, schools, and favourite teams.
3. Avoid keyboard patterns and simple substitutions such as changing an A to @.
4. Use unrelated words or a generated password instead.

! **Good to know:** Ask the “twenty guesses” question: could someone who knows you guess it quickly?

Take care: Security questions should get unique, stored answers when the service permits; truthful answers may be easy to research.

TALE

PASSWORD PROOF STORY

A familiar moment

Murray’s dog was loyal, lovable, and featured in 214 public photos. The dog was not a secret ingredient.

UNDERSTAND THE LOCKS

Stop password reuse

One stolen password should not open several accounts.

One old password › Many accounts › Change each one

1. Choose the account you care about most. Give it a new unique password.
2. Search your manager or records for other accounts using the old password.
3. Change those one at a time, starting with email and financial accounts.
4. Mark each completed account on your inventory without writing the password.

! **Good to know:** Do not try to fix everything in one sitting. Five accounts per session is excellent progress.

Take care: If a reused password appears in a breach warning, change every account that used it.

TALE

PASSWORD PROOF STORY

A familiar moment

Edna reused one excellent password everywhere. The problem was not excellence; it was everywhere.

BUILD YOUR PLAN

Make an account inventory

A list of account names and usernames reveals what needs protection without exposing passwords.

Service › Username › Unique? › MFA?

1. Write categories: email, money, health, shopping, social, government, travel, and home devices.
2. Under each category, list the service and sign-in email or username.
3. Mark whether the account has a unique password, MFA, and current recovery details.
4. Store the inventory securely; do not put passwords on this list.

! **Good to know:** An inventory is a map of doors, not a ring of keys.

Take care: Do not include full account numbers, security answers, or one-time codes.

TALE

PASSWORD PROOF STORY

A familiar moment

Walter discovered three streaming accounts and one mystery newsletter. Password cleanup can also be spring cleaning.

Enjoyed this sample?

Get the full book, and more free sample chapters, at
www.buyproof.ca

Join our email list and be the first to hear about
new Proof-series releases for Canadians.

We email only about new books.
Unsubscribe anytime.

