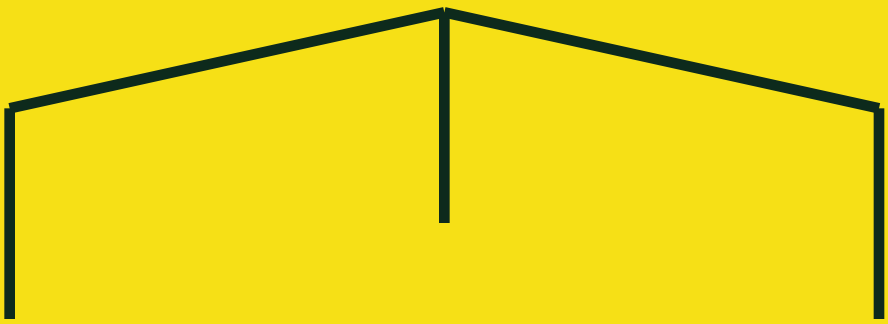
NONPROFIT DIGITAL MENTOR INC.

DIGITAL BOOK SERIES

Safer Online Every Day

Simple habits for passwords, messages, privacy, and scams



A practical guide to learn at your own pace

Start where you are.

Online safety is a set of everyday decisions, not a perfect score. These pages show how to slow down, check a claim, and protect the accounts you rely on.

Inside this guide

Make stronger sign-ins 3

Spot a suspicious message 4

Protect your privacy 5

Shop and pay carefully 6

What to do when something feels wrong 7

Your quick checklist 8

Make stronger sign-ins

Use unique passwords

Give important accounts different passwords. If one website has a breach, a reused password can put other accounts at risk.

Try a password manager

A trusted password manager can create and store long passwords. Protect it with one strong master password you can remember.

Turn on a second check

Enable multi-factor authentication for email, banking, and other important accounts. An authenticator app or security key is preferable when available.

TRY IT

Practice: Check whether your main email account offers multi-factor authentication and enable it.

Spot a suspicious message

Notice pressure

Scam messages often demand immediate action, threaten a penalty, or promise a prize. Urgency is a reason to pause.

Check outside the message

Do not use the message's link or phone number to verify it. Open the company's app or type its known website yourself.

Look at the sender

A familiar display name can hide an unfamiliar address. Check the full address, but remember that a plausible address alone is not proof.

TRY IT

Practice: Take a recent promotional message and identify its sender, link destination, and requested action.

Protect your privacy

Share less by default

A website does not always need your birthday, contact list, or location. Give only what is needed for the task.

Review app permissions

Open privacy settings and check which apps can use your camera, microphone, photos, and location. Remove access you do not need.

Lock your device

Use a PIN, passphrase, or biometric lock. Set the screen to lock automatically after a short period.

TRY IT

Practice: Review one app's permissions and turn off any access that is not necessary.

Shop and pay carefully

Start from a trusted route

Type a retailer's known address or use its official app. Be wary of ads that imitate a familiar store.

Review the details

Before paying, check the total, delivery terms, refund policy, and merchant name. Save the receipt and order number.

Use a protected payment method

Avoid sending gift cards, cryptocurrency, or wire transfers to a seller you do not know. These are difficult to recover.

TRY IT

Practice: Before your next purchase, find the seller's return policy and total charge.

What to do when something feels wrong

Stop interacting

Close the message or page. Do not send more information while you decide what to do.

Secure the account

From a trusted device or official app, change the password and sign out other sessions if possible. Turn on a second sign-in check.

Get help promptly

Contact your bank or service provider through its official number if money or account access may be affected. Report suspicious messages using the service's report feature.

TRY IT

Practice: Write down the official support route for one account you depend on.

Keep what works.

You can return to any chapter when you need it. Notice what you can do now, then choose one small skill to practice next.

- [ ] I use a different password for each important account.
- [ ] I pause when a message creates urgency.
- [ ] I verify requests through an official app or website.
- [ ] I know where to get help if an account may be compromised.

Your next small step

Write one task you will practice this week. Keep it specific and make time to try it twice.