

CyberMo's Pocket Guide

Small lessons. Watchful instincts.



Pause. Review. Verify.

QR codes + suspicious emails

blackpanthercybersecurity.com

MO'S RULE

Before you follow the invitation.

A familiar name, a pretty logo, or a sense of urgency can catch your attention. They do not establish who sent the message.

1

PAUSE

Take a breath. Do not let a message rush you into clicking, scanning, paying, or sharing information.

2

REVIEW

Look at the full sender address and the actual destination. A familiar-looking word is only a clue.

3

VERIFY

Open the official app, use a trusted bookmark, or type the known website address yourself.

Mo says: When you are unsure, use a trusted route you already know.

LESSON 01

The QR Trap

An unexpected code in an email or text? Do not scan it. Check the request through the company's official app, website, or a phone number you already trust.

1

Expected does not mean verified

At a location where you expect a QR code, check for stickers or signs of tampering.

2

Inspect before opening

Use a camera or reader that shows the destination without automatically opening it. Check the full address.

3

Choose a trusted route

If the address is unfamiliar, shortened, or unclear, stop and use the known official site instead.

Previewing an address is a screening step, not a guarantee. Avoid entering passwords or payment details through an unverified code.

LESSON 02

The Email Lure

An unexpected delivery problem or urgent account warning deserves a closer look.

1

Pause before interacting

Do not click links, open attachments, or reply to a suspicious message.

2

Review the real destination

Check the complete sender address. On desktop, hover to inspect a link without clicking. Sender addresses can also be spoofed.

3

Verify independently

Use the official app, a known bookmark, or a website address you already trust. Do not use contact details supplied by the suspicious message.

At work? Use your organization's phishing-reporting process. Report the message to IT/security before deleting it, according to your policy.

LOOK CLOSER

A familiar name can hide the real domain.

Suppose the known official address is:

`riverbank.example`

A suspicious address might be:

`riverbank.example.`

`account-check.example/login`

The controlling domain in this example is `account-check.example`. The words `riverbank.example` at the front do not make it Riverbank's website.

All addresses above are fictional. The `.example` ending is reserved for documentation and training.

HTTPS encrypts the connection. A padlock does not prove that a site or its operator is trustworthy.

OPTIONAL CLUES

Helpful tools. Limited answers.

1

ICANN Lookup (RDAP)

Shows available domain-registration details. Registration dates and registrar information are clues; they do not prove legitimacy.

2

Google Safe Browsing

Checks whether a website is flagged for known threats. A new phishing page may not have been detected yet.

3

.gov domain lookup

The get.gov lookup identifies who manages a .gov domain. It is not a general website-safety scanner.

Keep private links private. Do not submit password-reset links, credentials, private tokens, or confidential work links to public checking tools.

IF YOU ALREADY INTERACTED

Stop. Then take the next useful step.

1

At work: report it promptly

Tell IT/security what you clicked, downloaded, or entered, and when. Follow their instructions.

2

If you entered a password

Change it through the known official app or site. Change it anywhere you reused it. Review recovery and MFA settings.

3

If you shared payment details

Contact your bank or card provider through its official app or a trusted number, such as the number on your card.

4

If a file downloaded or ran

Do not reopen it. On a personal device, update your security software and run a scan. At work, follow IT/security guidance.

KEEP LEARNING WITH MO

Your next safe step.

Find Mo's posters, videos, and adventures:

CyberMo on Black Panther Cybersecurity

OFFICIAL GUIDANCE

FTC: QR-code scams

FTC: Recognize and avoid phishing

FBI: HTTPS does not prove trust

ICANN Lookup (RDAP)

Google Safe Browsing site status

.gov domain lookup

IANA: Reserved example domains

Educational guidance. Follow your organization's reporting process for work-related concerns.

Edition: October 24, 2026

Black Panther Cybersecurity

Pause. Review. Verify.