Cybersecurity workshop for everyone: facilitator's guide

Everything you need to run a 45–60 minute workshop based on the book *A Hacker's Security Guide* by César Cerrudo. You don't need to be a security expert: the slide deck, this guide and the handouts do the heavy lifting.

01 Who this kit is for

HR and security teams at companies, teachers and school administrators, fraud-prevention teams at banks, libraries and community organizations. The workshop is designed for a **general adult audience with no technical background**; a variant for parents is available (see section 5).

02 What's in the kit

FILE	WHAT IT IS	USE
Slide deck (.pptx)	30 slides, each with speaker notes: what to say, where to pause, what to ask the room.	Project
Facilitator's guide	This document: agenda, tips and frequently asked questions.	Read beforehand
Activity sheet	2 printable pages: spotting red flags, a personal checklist and an action commitment.	Print 1 per attendee
8 infographics (.pdf)	Handouts by topic: phishing, passwords, phone, home, identity, family, response, travel.	Print or send afterwards
Hacker Academy	Interactive online lessons and quizzes to keep going after the workshop.	Share the link
Simulator and quiz	"Real or scam?" and "How hackable are you?": 2–10 minute online practice.	Share the link

03 Requirements and preparation

- **Room:** projector or screen, 45–60 minutes, groups of 5 to 60 people.
- **Printouts:** one activity sheet per attendee; optionally the infographics most relevant to your audience (companies: 01, 02, 03 and 07; schools: 06; banks: 01, 02 and 05).
- **Before the workshop:** go through the deck once reading the speaker notes (PowerPoint "Presenter" view). Each note explains the goal of the slide and how to work it.
- **The facilitator's golden rule:** the workshop alternates fear and solution. Never end a block on the threat: every section closes with concrete actions — respect that order.

04 Suggested agenda (50 minutes)

TIME	SLIDES	BLOCK	FACILITATION KEY
0–7 min	1–7	**Opening.** The value of your digital life, hackers vs. criminals, the map of the 5 doors.	On slide 2, ask everyone to take out their phone and look at it: the physical exercise hooks the room. Slide 7 is the map: announce it as a promise ("by the end you'll know how to close all five").
7–15 min	8–11	**Door 1: scams.** The trap email, the faceb00k test, how they manipulate you, the protocol.	On slide 9, ask out loud which address is the fake one and wait for answers before revealing. The pause that follows is the most important moment of the workshop.
15–21 min	12–14	**Door 2: passwords.** The domino effect and the ladder up to passkeys.	The question on slide 12 ("do you reuse the same password?") is rhetorical: don't ask for raised hands, the slide's humor does the work.
21–28 min	15–18	**Door 3: your phone.** The theft minute by minute, the 4 locks, USB and QR.	The timeline on slide 16 is read slowly, mark by mark. Slide 17 is actionable: suggest setting the SIM PIN that very afternoon.
28–34 min	19–21	**Door 4: your home.** Router, IoT and the two-places rule.	"The camera watching you" (20) tends to spark questions: the answers are in section 6 of this guide.
34–41 min	22–24	**Door 5: your family.** Grooming, sexting, guiding instead of forbidding.	Lower your voice on slide 22 and don't rush 23: it's the emotional peak. Move quickly on to 24 — never leave parents in fear without tools.
41–46 min	25–28	**Plan B + AI.** What to do if it already happened, the illegal mistake, deepfakes.	Slide 26 surprises people (hiring a "hacker" is a crime in itself): let it breathe.
46–50 min	29–30	**Closing + activity.** The full blueprint, "one door today", activity sheet.	Hand out the activity sheet and close with Activity 3 (the written commitment): asking for one single action multiplies follow-through.

SHORT VERSION (25 MINUTES)

Use slides 1–2, 7–11, 12–14, 22–24 and 29–30 (opening, scams, passwords, family and closing). They are the highest-impact-per-minute sections for general audiences.

05 The three activities on the sheet

Activity 1 — "Spot the red flags" (5 min, during or after Door 1)

Each attendee circles the scam signals in an email printed on the sheet. There are **five**: (1) the sender's domain is not the official one ("yourbank-alerts.net"), (2) the 24-hour urgency, (3) the request for username and password, (4) the shortened link, and (5) the unexpected prize at the bottom. Go over the answers out loud: every signal found as a group is worth more than ten explained.

Activity 2 — "My 10 locks" (3 min, towards the close)

A personal habits checklist. It is not handed in or shared: it's an individual mirror. Suggest that everyone count their empty boxes — that number is their task list for the week.

Activity 3 — "My first door" (2 min, workshop close)

Each attendee writes down **one single action** and **when** they will do it ("tonight I'll turn on my SIM PIN"). The evidence on implementation intentions is clear: writing down the when doubles the odds of follow-through. Close the workshop by reading two or three out loud, with permission.

06 Adaptations by audience

AUDIENCE	RECOMMENDED ADJUSTMENTS
Companies	Emphasize Doors 1 to 3 and Plan B. Connect with internal policies (incident reporting, corporate MFA). Hand out infographics 01, 02, 03 and 07.
Schools (for parents)	Double the time on Door 5 (slides 22–24) and hand out infographic 06. For classes WITH STUDENTS do not use this deck: the kit includes two dedicated school versions ("Internet Guardians" 8–12 and "Defense Mode" 12–15), each with its own teacher's guide and activity sheet.
Banks (for customers)	Emphasize Doors 1 and 2 plus infographic 05 (identity and money theft). Reinforce the message "the bank never asks for credentials by message" with your own official channels.
Older adults	Short version (25 min), at a slower pace. Insist on two rules: no personal data by message, and verify any request for money by calling a trusted family member.

07 Frequently asked questions from the audience (and how to answer)

"ARE PASSWORD MANAGERS SAFE? WHAT IF THE MANAGER GETS HACKED?"

No system is foolproof, but a manager with a strong master password and MFA is far better than the real-world alternative: reused or written-down passwords. The right comparison is not against perfection but against what the person does today.

"I HAVE NOTHING TO HIDE / NOBODY WOULD ATTACK ME."

Today's attacks are massive and automated: they don't pick victims, they sweep. And we all have something to lose: the money in our account, our identity (which can be used to take on debt or commit crimes in your name) and access to photos and conversations — our own and other people's.

"WHICH ANTIVIRUS / MANAGER / BRAND DO YOU RECOMMEND?"

The workshop recommends categories and habits, not brands: official stores, reviews, download counts and reasonable permissions are the criteria for choosing any product. Avoid endorsing specific brands unless your institution has its own policy.

"SOMETHING LIKE THIS HAPPENED TO ME — WHAT DO I DO ABOUT MY CASE?"

Don't analyze personal cases in public. Point to the general protocol (evidence, report to the police or prosecutor's office, password changes, official channels) and refer them to a private conversation or a specialist.

"DOESN'T AI MAKE ALL OF THIS USELESS?"

Quite the opposite: AI makes scams more convincing, but the workshop's defenses don't rely on spotting sloppy writing — they rely on structural habits: verifying through another channel, never handing over data by message, MFA. Those survive deepfakes.

08 Facilitator's checklist

- [ ] I went through the full deck reading the speaker notes.
- [ ] I printed one activity sheet per attendee (and the chosen infographics).
- [ ] I tested the projector and the presenter view.
- [ ] I have the links to the Hacker Academy, the simulator and the quiz at hand to share at the close.
- [ ] I know which version I'm running (full 50 min / short 25 min) and my audience adaptation.