XRT PATHFINDER / LEARNING ARENA

# AI Literacy & Social Cybersecurity 101

Build with AI. Protect your people. Six practical stations for a smarter, safer digital life.

Beginner friendly | 60-minute workshop | Solo or host-led teams | No account required

For community learners, families, creators, and small teams. You only need to read and make choices; an AI account is optional. Team play is facilitated in the room or on a call. This lesson does not connect multiplayer avatars, microphones, or a broadcast.

A1 / UNDERSTAND AI · 7 MINUTES

# A useful assistant. A human decision.

AI systems use patterns in data to make predictions or produce outputs. Generative AI makes new text, images, audio, or other content in response to your instructions.

Use it to draft an invitation, brainstorm a title, or explain a difficult paragraph. You still decide what is accurate, appropriate, and ready to share.

## Fluent does not mean factual

An AI can confidently invent a detail or a reference. This is often called a hallucination or confabulation. Outputs can also repeat unfair assumptions.

Reference: NIST Generative AI Profile.

**Practice / Sort the task**

Which task can start with an AI draft, followed by your review?

- Brainstorm five names for a neighborhood reading club.
- Decide someone’s medical treatment without a professional.
- Publish a claim about a neighbor without checking it.

**Expected result:** You identify a low-stakes drafting task and explain where human review is needed. **If unsure:** ask whether an error could harm someone or affect their rights, health, or money.

A2 / ASK BETTER · 8 MINUTES

# Give a clear task. Keep private details out.

A practical prompt has four parts: **task, context, constraints, and output format**. Give only the information needed. Use fictional names and details for practice.

```
Task: Draft a welcoming invitation to a community AI workshop.
Context: Adults who are curious but new to AI.
Constraints: Use plain language. Under 80 words. Do not invent a date,
venue, price, or registration link; use placeholders.
Format: One headline, one short paragraph, and one next step.
```

> **Data check before sending**
>
> Do not put passwords, verification codes, financial records, private messages, or identifiable participant information into this practice. Review an AI service's privacy settings and your organization's rules before using real work data.

▶ **See a sample draft — written for this lesson**

> **Practice / Rewrite a risky request**
>
> "Here are our members' names, phone numbers, and private messages. Write an event invite."
>
> Rewrite it aloud or on paper using a general audience description and placeholders. An optional AI tool can receive your fictional version.

**Expected result:** Your prompt includes all four parts without personal data. **If the draft invents details:** replace them with placeholders and clarify the constraint.

A3 / CHECK BEFORE SHARING · 8 MINUTES

# A claim needs evidence.

Use this workshop's **Claim** → **Source** → **Check** → **Decide** routine. Name the factual claim, open the original source, check its date and context, then decide whether to use it, correct it, or leave it out.

## Fictional AI answer

"Winter Blitz begins at 8 PM, admission is free, and every visitor gets a laptop."

None of those details is supplied in this exercise. A polished sentence does not establish an event fact.

> **Practice / Fact-check the invitation**
>
> 1. Identify the three claims.
> 2. Name the original source you would consult: the event organizer's current official event page or a verified organizer contact.
> 3. Replace unsupported details with [TIME], [COST], and [CONFIRMED BENEFITS].

**Media check:** A realistic face or voice is not proof of identity. Verify the source and the story before forwarding. Do not treat an AI detector's score as a verdict.

**Expected result:** You can explain what evidence is missing. **If a citation is broken or does not support the claim:** do not share the claim as verified.

References: NIST on unreliable generated content · FBI on verifying synthetic media.

B1 / DEFEND YOUR ACCOUNTS · 8 MINUTES

# Your social account is part of your identity.

Social cybersecurity means protecting your accounts, conversations, reputation, and the people connected to you.

## Protect the sign-in

- Use a unique password for each account; a password manager can help.
- Use a passkey where supported, or turn on multifactor authentication (MFA).
- Never send someone a one-time login code or approve a login you did not initiate.
- Keep devices and apps updated.

## Check what you share

- Review who can see posts, tag you, and send messages.
- Ask before posting another person's photo or story.
- Consider what a public post reveals about your location, routine, or family.
- Use the platform's own report and block tools for abuse or impersonation.

> **Practice / Private account check**
>
> On your own device, open your social app's official settings or help center. Locate its sign-in security and audience controls. You may only observe today; do not share your screen while entering passwords or recovery codes.

**Expected result:** Name one security setting and one sharing setting you want to review. **If the menu differs:** use that platform's current official help instructions. The instructor does not need your password.

Reference: FBI online safety guidance.

B2 / SPOT SOCIAL ENGINEERING · 10 MINUTES

# Slow the moment down.

Social engineering uses trust, fear, excitement, or urgency to pressure a person into taking an action. Phishing is a deceptive message that tries to get information, money, or a click.

## Scenario 1 / “Support” DM

Training example — no live link

“Your creator page closes in 10 minutes. Send us the six-digit code we just texted you to appeal.”

- Send the code because the message says support.
- Open the official app independently and check account notices.
- Reply with my password instead.

## Scenario 2 / Familiar voice

Someone sounding like a relative says, “I’m in trouble. Send money now. Don’t call anyone.”

- Pay because the voice sounds familiar.
- End the call and contact my relative using a number I already know.
- Use the new number the caller provides.

> **Pause → Verify → Protect → Report**
>
> Verify through a separate, known channel. If you cannot reach the person, try a trusted contact. Voice cloning can imitate someone you know; urgency is a reason to verify. Save relevant evidence and use the official reporting channel.

**Expected result:** Explain both the pressure tactic and your independent verification step. **If you are uncertain:** stop the requested action and ask a trusted person for help. A legitimate-looking logo alone is not evidence.

References: FTC voice-cloning scams · FBI phishing guidance.

B3 / RESPOND & RECOVER · 7 MINUTES

# Act calmly. Ask for help early.

Being targeted is not a personal failure. Match your next step to what happened.

## Account information exposed?

Go directly to the account provider's official recovery page. If you can sign in, change the compromised password, sign out other sessions, check recovery contacts, and enable MFA. Change reused passwords elsewhere. Tell contacts if your account sent scam messages.

## Money or identity involved?

Contact your payment provider promptly using a known channel and ask about reversing the transaction. Preserve messages and transaction details. In the US, report scams at ReportFraud.ftc.gov; use IdentityTheft.gov for a personal recovery plan. Recovery is not guaranteed.

> **Practice / A two-sentence response**
>
> A friend says, "I entered my social password on a link someone sent. What now?" Explain where they should go first and name one account-recovery action.

**If you only opened a link:** stop interacting; do not enter data or open downloads. If you downloaded or ran a file, or this is a work device, contact trusted technical support or your IT team. Use official support rather than a stranger offering paid recovery in your DMs.

**Expected result:** You have a next step without blaming the person. **If locked out:** follow the provider's official recovery process; this lesson cannot recover an account.

References: FTC account recovery · FTC after a scam.

FINAL CHALLENGE · 8 MINUTES + 4-MINUTE WELCOME = 60 MINUTES

# What would you do next?

Choose one answer per question. Aim for 6 of 8, then review any missed topics. You can retry. This is a practice check, not professional certification.

**Check my answers**

> **Your next 24 hours**
>
> Choose one action: improve a prompt, verify a claim before posting, review one social account's security, or agree on a family callback plan. Write it somewhere you will see it.

1. An AI answer sounds confident. What does that prove? A) It must be accurate. / B) Only that it was expressed confidently; the facts still need checking. / C) Its citations must exist.
2. What belongs in a practice prompt? A) A real customer's private messages. / B) Your one-time login code. / C) A fictional scenario with clear constraints.
3. AI invents a Winter Blitz start time. What next? A) Check the organizer's official information before publishing. / B) Post it because it sounds reasonable. / C) Ask AI to repeat it until it agrees.
4. A support DM asks for a six-digit sign-in code. A) Send it before the deadline. / B) Check the official app independently; do not share the code. / C) Post the code publicly to ask for help.
5. A relative's voice urgently asks for money. A) Trust the voice alone. / B) Call the new number in the message. / C) Verify through a number you already know.
6. Which habit helps protect accounts? A) Use the same strong password everywhere. / B) Use unique passwords and enable MFA or a supported passkey. / C) Turn off updates to avoid changes.
7. Your social account was taken over. Where do you start? A) The provider's official recovery process. / B) A stranger offering guaranteed recovery in DMs. / C) Send the attacker another password.
8. Before sharing a dramatic video, what is best? A) Trust it because it looks realistic. / B) Share it first and check later. / C) Verify its source and context through credible original information.

## Take-home card

**With AI:** Ask clearly. Keep private data out. Check facts. Review before sharing.

**With people online:** Pause. Verify independently. Protect your account. Report through official channels.

**If something went wrong:** You can ask for help. Use the provider's official recovery process and keep relevant evidence.

Progress is a self-check saved only in this browser when storage is available. No login, tracking, or information upload. External source links require internet access.

▶ **Sources & lesson notes**

AMX / LABS · XRT Pathfinder · Future Builders