Cybersecurity Essentials at Work: Rise 360 Storyboard

Instructional Designer: Ayoub Ibrahim Safi | Version 1.0 | 14 October 2026

Course Overview

Self-paced workplace course for non-technical employees, built in Articulate Rise 360. Six lessons: five content lessons and one graded quiz. Estimated seat time: 20 minutes.

Course Settings

What to include	Where in Rise	What to enter
Course title	Course overview page → title	Cybersecurity Essentials at Work
Course description	Course overview page → description	Learn four everyday habits that protect you and your organization: spotting phishing, securing your accounts, handling data safely, and reporting problems fast. About 15–20 minutes.
Cover image	Course overview page → cover image	The hero office image (see assets list)
Learning objectives	Lesson 0, as a Text block after the course map (optional)	1. Identify the warning signs of a phishing message. 2. Apply strong passphrases and MFA to work accounts. 3. Choose safe ways to store, share and work with company data. 4. Report a suspected security incident quickly and correctly.
5 Blocks lessons	Course outline → **Add lesson** → **Blocks**	Welcome: You're the First Line of Defense · Spot the Phish · Lock Down Your Accounts · Handle Data with Care · When Something Feels Wrong
1 Quiz lesson	Course outline → **Add lesson** → **Quiz** (last)	Final Quiz
Navigation	**Settings** → Navigation	Restricted

What to include	Where in Rise	What to enter
Look and feel	**Theme**	Brand colors and font applied in Theme settings
Quiz rules	Open the Quiz lesson → quiz settings	Passing score 80% · Unlimited retakes · Randomize answers on · Reveal answers on
Tracking and export	**Publish → LMS**	SCORM 2004 (SCORM 1.2 if required by the LMS) · Reporting: **Quiz result** → select Final Quiz

Lesson 0: Welcome: You're the First Line of Defense (1 min)

The welcome lesson starts with a short story and ends with the course map, so learners see why this matters to them before any rules.

#	Block	Content	Notes
1	Image – Hero	Overlay text: **Cybersecurity Essentials at Work**	Photo of an ordinary office desk or a laptop at a café. No hooded hackers.
2	Text – Paragraph	It's 8:55 on a Monday. Sara, a project coordinator, opens an email that says her mailbox is almost full. She clicks the link, types her password, and gets back to work. Nothing seems wrong. But someone else now has her password.	
3	Quote – Quote on image	Most attacks don't start with clever code. They start with one ordinary click.	Same office image, darkened
4	Text – Paragraph	You don't need to be a technical expert to stop attacks like this. You just need to know what	

#	Block	Content	Notes
		to look for and what to do. In this course, you'll learn four habits that protect you and your organization.	
5	List – Numbered list	1. **Spot the Phish** – recognize fake messages. 2. **Lock Down Your Accounts** – passphrases and MFA. 3. **Handle Data with Care** – store and share safely. 4. **When Something Feels Wrong** – report fast.	Bold the lesson names
6	Text – Paragraph	The course ends with a short quiz. You'll need 80% to pass.	
7	Continue	—	Default

Lesson 1: Spot the Phish (5 min)

Learners see the red flags on a real-looking email, then practice sorting messages. Objective 1.

#	Block	Content	Notes
1	Text – Heading + paragraph	**What is phishing?** Phishing is a message that pretends to come from someone you trust. The goal is to get you to click a link, open a file, share a password, or send money. It can arrive by email, text message, phone call, or chat app.	
2	Interactive – Labeled graphic	Intro: *Here's the email Sara received. Select each marker to see*	Image: mock email (fictional brand **"MailCloud IT Support"**). 5 markers

#	Block	Content	Notes
		what she missed.	below.
	↳ Marker 1 – Sender	**Check the sender.** The name says IT Support, but the address is it-support@mailc1oud-help.com. Look closely: a number 1 replaces the letter l.	On the sender line
	↳ Marker 2 – Subject	**Urgency is a red flag.** "Your mailbox will be deleted in 2 hours" is designed to make you act before you think.	On the subject line
	↳ Marker 3 – Greeting	**Generic greeting.** "Dear user" instead of your name can mean the message went to thousands of people.	On "Dear user"
	↳ Marker 4 – Link	**Hover before you click.** The button says "Verify mailbox," but the real address points to an unfamiliar site. On a phone, press and hold the link to preview it.	On the button
	↳ Marker 5 – Request	**Requests for passwords.** Real IT teams will never ask you to enter your password through an email link.	On the body text
3	Interactive – Accordion	Intro: *Phishing doesn't only arrive by email.*	4 items
	↳ Item 1: Email phishing	The most common type. Watch for fake senders, urgent requests, and unexpected links or	

#	Block	Content	Notes
		attachments.	
	↳ Item 2: Smishing (text messages)	Texts about a missed delivery, a bank problem, or a prize. They often include a short link. Don't tap it; go to the official app or website instead.	
	↳ Item 3: Vishing (phone calls)	A caller claims to be from IT, a bank, or a manager and asks for a code or password. Hang up and call back using a number you already know.	
	↳ Item 4: Fake payment requests	An email from a "manager" or "supplier" asks for an urgent payment or new bank details. Always confirm through a second channel, such as a phone call to a known number.	
4	Text – Paragraph	**Your rule of thumb:** If a message is unexpected, urgent, and asks you to do something, stop and check before you act.	Styled as a Statement (Note) for emphasis
5	Interactive – Sorting activity	Instructions: *Sort each message into the right pile.* Piles: **Suspicious** / **Looks safe**	6 cards below
	↳ Suspicious	"Your parcel couldn't be delivered. Pay a 1.99 fee here: bit.ly/…"	
	↳ Suspicious	"This is your CEO. I'm in	

#	Block	Content	Notes
		a meeting. Buy 5 gift cards and send me the codes."	
	↳ Suspicious	"Unusual sign-in detected. Enter your password here within 30 minutes."	
	↳ Looks safe	A meeting invite from a colleague you work with, for a meeting you discussed yesterday.	
	↳ Looks safe	A reminder from HR about a training you already registered for, with no links or attachments.	
	↳ Looks safe	A notification inside the company's official app that you opened yourself.	
6	Knowledge check – Multiple choice	**Question:** Sara gets an email from "Finance" asking her to approve an invoice today. The attachment is called Invoice.zip. What should she do first? A) Open the file to check the invoice amount. **B) Contact Finance using a known phone number or chat to confirm.** ✔ C) Reply to the email and ask if it's real. D) Forward it to her team to see if anyone else got it.	Correct: Right. Checking through a separate, known channel is the safest move. Incorrect: Not quite. Opening the file or replying to the sender could put you in contact with the attacker. Confirm through a channel you already trust.
7	Continue	—	Complete block above

Lesson 2: Lock Down Your Accounts (4 min)

Learners correct common password myths, then see step by step how MFA stops an attacker who already has a password. Objective 2.

#	Block	Content	Notes
1	Text – Paragraph	Remember Sara's password from the welcome story? The attacker has it now. Whether they get into her account depends on what she does next, and on the habits in this lesson.	
2	Interactive – Flashcard grid	Intro: *True or false? Flip each card to find out.*	4 cards, front = myth, back = fact
	↳ Card 1	Front: *A short password with symbols like P@ss1! is strong.* Back: **False.** Length matters more. A passphrase of 4 or more random words, like *river-lamp-orbit-jacket*, is much harder to guess and easier to remember.	
	↳ Card 2	Front: It's fine to reuse a strong password on a few sites. Back: **False.** If one site is breached, attackers try that password everywhere. Use a different password for every account.	
	↳ Card 3	Front: *Writing passwords in a notebook or file is the only way to remember them.* Back: **False.** Use	

#	Block	Content	Notes
		your organization's approved password manager. You remember one strong passphrase, and it stores the rest.	
	↳ Card 4	Front: *MFA is only for IT staff and managers.* Back: **False.** Everyone's account is a target. Turn on MFA for every work account that offers it.	
3	Text – Heading + paragraph	**What is MFA?** Multi-factor authentication (MFA) asks for a second proof that it's really you, usually a code or an app approval on your phone. Even if someone steals your password, they still can't sign in without that second step.	
4	Interactive – Process	Intro: *See how MFA protects Sara's account.*	4 steps + summary
	↳ Step 1: The attacker tries to sign in	The attacker enters Sara's email and the stolen password.	
	↳ Step 2: MFA asks for a second step	The system sends an approval request to Sara's phone. The attacker doesn't have her phone.	
	↳ Step 3: Sara gets a request she didn't	Sara wasn't signing in, so she selects **Deny**. She never approves a	

#	Block	Content	Notes
	expect	request she didn't start.	
	↳ Step 4: Sara reports it and changes her password	An unexpected MFA request means someone knows her password. She reports it and changes the password right away.	
	↳ Summary	The attack fails. One unexpected prompt became an early warning instead of a breach.	
5	Statement – Note	**Watch out for MFA fatigue.** Some attackers send request after request, hoping you'll approve one just to make them stop. If you get repeated prompts you didn't start, deny them all and report it.	
6	Knowledge check – Multiple response	**Question:** Which of these are good password habits? Select all that apply. **A) Using a long passphrase of random words** ✔ B) Using the same strong password for work and personal accounts **C) Storing passwords in the approved password manager** ✔ **D) Turning on MFA for every account that offers it** ✔ E) Approving an MFA	Correct: Exactly. Long, unique passphrases plus MFA are your strongest protection. Incorrect: Not quite. Never reuse passwords across accounts, and never approve an MFA request you didn't start.

#	Block	Content	Notes
		request to see who sent it	
7	Continue	—	Complete block above

Lesson 3: Handle Data with Care (4 min)

Learners compare safe habits in three work settings, then make a sharing decision in a short scenario. Objective 3.

#	Block	Content	Notes
1	Text – Heading + paragraph	**What counts as sensitive data?** Sensitive data is any information that could hurt people or the organization if the wrong person saw it. Examples include customer and employee personal details, financial records, contracts, passwords, and internal plans. If you're not sure, treat it as sensitive.	
2	Interactive – Tabs	Intro: *Safe habits depend on where you're working.*	3 tabs
	↳ Tab 1: In the office	Lock your screen every time you step away (**Windows + L** or **Ctrl + Cmd + Q** on Mac). Don't leave printed documents on desks or printers. Don't plug in USB drives you find or don't recognize.	
	↳ Tab 2: Working	Use the company VPN when it's required.	

#	Block	Content	Notes
	remotely	Keep work files on approved company storage, not on your personal laptop or personal cloud. Make sure family members can't see or use your work device.	
	↳ Tab 3: Traveling or in public	Avoid public Wi-Fi for work, or use the VPN or your phone's hotspot. Watch for people who can see your screen or hear your calls. Never leave your laptop or phone unattended.	
3	Interactive – Scenario	Character: **Sara**. Setting: office.	One scene, 3 choices
	↳ Scene	A client emails Sara: *"Our shared folder link isn't working. Can you just send the project file to my personal Gmail? I need it before my 3 pm meeting."* The file contains client contact details and pricing.	
	↳ Choice A	*Send it to the Gmail address. The client needs it urgently.* → **Feedback:** Sending sensitive data to a personal account takes it out of company control. Urgency is also a common pressure tactic. Try again.	Retry

#	Block	Content	Notes
	↳ Choice B ✔	*Re-share the file through the approved company tool to the client's work address, and let them know.* → **Feedback:** Well done. The client gets the file quickly, and the data stays protected and traceable.	Continue
	↳ Choice C	*Copy the file to a USB drive and courier it.* → **Feedback:** Physical copies are easy to lose and hard to track. There's a faster, safer option. Try again.	Retry
4	List – Checkbox list	**Before you share any file, check:** ☐ Am I using an approved company tool? ☐ Is it going to a work address, not a personal one? ☐ Does this person really need all of this data? ☐ Have I set the right access (view-only, expiry date) where possible?	Rise *Checklist* list style
5	Continue	—	Complete block above

Lesson 4: When Something Feels Wrong (3 min)

Learners learn the reporting steps and why reporting early matters, closing Sara's story. Objective 4.

#	Block	Content	Notes
1	Text – Paragraph	Back to Monday morning. Around 10:30, Sara realizes the mailbox email was	

#	Block	Content	Notes
		fake. She feels embarrassed and thinks about keeping quiet. What should she do?	
2	Quote – Quote A	Reporting quickly is never a mistake. Waiting is. The first minutes after an incident matter most.	
3	Text – Paragraph	You might need to report if you clicked a suspicious link, entered your password somewhere unusual, got an MFA request you didn't start, lost a device, or sent data to the wrong person. You'll never be blamed for reporting honestly.	
4	Interactive – Process	Intro: *If something feels wrong, follow these steps.*	4 steps + summary
	↳ Step 1: Stop	Don't click anything else, reply, or try to fix it yourself. Don't delete the suspicious message; the security team may need it.	
	↳ Step 2: Disconnect if needed	If you opened a suspicious file or your device is acting strangely, disconnect from Wi-Fi or unplug the network cable. Don't turn the device off.	

#	Block	Content	Notes
	↳ Step 3: Report it	Contact **[TBC: IT/security team name]** right away using **[TBC: email / phone / form / report button]**. Say what happened and when.	
	↳ Step 4: Follow instructions	The security team may ask you to change passwords or hand over the device. Do what they ask, even if it's inconvenient.	
	↳ Summary	Sara reported it within minutes. The team reset her password and blocked the attacker before any data was taken.	
5	Interactive – Button stack	Label: *How to report a security concern* → Button: **Report an incident**	Link to **[TBC: reporting URL]**. Remove block if no reporting URL is available.
6	Statement – Bold statement	**Pause. Check. Report.** Three habits that stop most attacks.	
7	Text – Paragraph	You're ready for the final quiz. You'll need 80% to pass, and you can retake it if needed.	
8	Continue	—	Default

Final Quiz (3 min, graded)

Eight scenario-based questions, two per objective. Passing score 80% (7 of 8 correct). The correct answer is marked ✔.

Quiz intro text: *Answer 8 questions to complete the course. You need 80% to pass, and you can retake the quiz as many times as you need.*

#	Type	Question	Options	Feedback	Obj.
1	Multiple choice	You get an email from "IT Helpdesk" saying your account will be locked in 1 hour unless you sign in through the link. What's the biggest red flag?	A) It mentions your account. **B) It creates urgency and asks you to sign in through a link.** ✔ C) It comes from IT. D) It's sent during work hours.	✔ Urgency plus a sign-in link is a classic phishing pattern. ✗ Look for pressure to act fast and requests for credentials.	1
2	Multiple response	A text says your package is delayed and asks you to pay a small fee through a link. Which actions are safe? Select all that apply.	**A) Delete the message and check the delivery in the official app.** ✔ B) Tap the link but don't enter card details. **C) Report it if your organization asks you to report smishing.** ✔ D) Reply STOP to unsubscribe.	✔ Go directly to the official source and never interact with the link. ✗ Tapping or replying confirms your number is active and can lead to harm.	1
3	Multiple choice	Which of these is the strongest password?	A) Summer2026! B) P@ssw0rd#1 **C) copper-tiger-window-sunrise** ✔ D) Your name plus your birth year	✔ A long passphrase of random words is strongest and easiest to remember. ✗ Short passwords and personal details are	2

#	Type	Question	Options	Feedback	Obj.
				easy to guess.	
4	Multiple choice	Your phone shows an MFA approval request, but you aren't signing in to anything. What should you do?	A) Approve it to see what happens. B) Ignore it; it's probably a glitch. **C) Deny it, change your password, and report it.** ✔ D) Turn off MFA so it stops.	✔ An unexpected request means someone may have your password. ✗ Never approve a request you didn't start, and always report it.	2
5	Multiple choice	A colleague asks you to email a file with customer details to their personal email so they can work from home. What should you do?	A) Send it; they're a colleague. B) Send it, but password-protect the file. **C) Share it through the approved company tool to their work account.** ✔ D) Print it for them to take home.	✔ Approved tools keep data protected and traceable. ✗ Personal accounts and printouts take data out of company control.	3
6	Multiple response	You're working from a café. Which habits keep company data safe? Select all that apply.	**A) Using the company VPN or your phone's hotspot** ✔ **B) Locking your screen when you get up** ✔ C) Asking a stranger to watch your	✔ Secure connection, locked screen, and privacy from onlookers all matter. ✗ Never leave your device with someone you don't	3

#	Type	Question	Options	Feedback	Obj.
			laptop **D) Sitting where others can't see your screen** ✔	know.	
7	Multiple choice	You realize you entered your password on a fake website 10 minutes ago. What's the best first step?	A) Wait to see if anything bad happens. **B) Report it to [TBC: IT/security team] right away.** ✔ C) Delete the email so no one else sees it. D) Tell a colleague and ask what they'd do.	✔ Reporting fast gives the security team time to stop the attacker. ✗ Waiting or deleting evidence makes it harder to contain the damage.	4
8	Multiple choice	You opened an attachment and your computer started acting strangely. Which action should you avoid?	A) Disconnecting from the network B) Reporting it immediately **C) Turning the computer off and on to fix it** ✔ D) Following the security team's instructions	✔ Correct, avoid restarting: it can erase information the security team needs. ✗ Disconnecting, reporting and following instructions are all the right moves.	4

Results messages

- Pass (80%+): *Well done! You've completed Cybersecurity Essentials at Work. Remember: Pause. Check. Report.*
- Fail (below 80%): *You're nearly there. Review the lessons you're unsure about, then retake the quiz.*

Build checklist and assets

Five image assets across six lessons. All other content uses native Rise blocks.

Assets

Asset	Used in	Notes
Hero office image	Lesson 0, blocks 1 and 3	Ordinary workplace, diverse people, no hackers
Mock phishing email	Lesson 1, labeled graphic	Custom graphic, exported as PNG (min. 1200 px wide). Fictional brand "MailCloud IT Support" and the address it-support@mailc1oud-help.com.
Sara character	Lesson 3 scenario	Rise built-in scenario character
Office background	Lesson 3 scenario	Rise scenario background library
Remote and travel photos (optional)	Lesson 3 tabs	Rise content library

Build steps

- ☐ Create the course and add the 5 lessons + 1 Quiz lesson in order.
- ☐ Set navigation to Restricted in course settings.
- ☐ Build each lesson from its table, top to bottom.
- ☐ Set every Continue block after an interaction to *Complete block above*.
- ☐ Build the quiz: passing score 80%, unlimited retakes, randomize answers on, reveal answers on.
- ☐ Results: pass and fail messages are displayed in a short Course Complete lesson after the quiz.
- ☐ Replace every **[TBC]** (Lesson 4 and Quiz Q7) or remove the reporting button.
- ☐ Preview on desktop and mobile; check every marker, card and scenario branch.
- ☐ Export as SCORM with tracking set to Quiz result, then test in SCORM Cloud before LMS upload.