Secure Start

Facilitator Guide · New-Hire Computer Onboarding

securibyte · IT ENABLEMENT · V1.0 · 2026

Every new hire's first act on a company machine sets their security posture for years. This 60-minute, instructor-led session teaches three habits: sign in cleanly, keep software patched, and recognize an attack. A new teammate leaves the room able to do all three, not just recall them.

COURSE AT A GLANCE

DURATION	FORMAT	GROUP SIZE
60 minutes	Instructor-led + hands-on	1–6 learners
AUDIENCE	**SETTING**	**PREREQUISITES**
Day-1 new hires	At each learner's device	Account + temp password

DESIGN NOTES

How this course was built: the ADDIE backbone

Analyze — New hires arrive with mixed tech confidence and no knowledge of securibyte's tools. The riskiest first-week gaps are weak sign-in habits, unpatched apps, and clicking malicious mail.

Design — Three short modules, each one terminal objective, sequenced login → update → defend. Performance-based, not lecture-based.

Develop — This guide, a one-page learner quick-reference, a 5-item knowledge check, and a live phishing-sample activity.

Implement — Delivered at the learner's own device on Day 1 so practice happens on the real environment.

Evaluate — Checks for understanding mid-module (formative); knowledge check + performance checklist at the end (summative); a 30-day behavior follow-up.

TERMINAL LEARNING OBJECTIVES

By the end of this session, the learner will be able to…

1. **Sign in independently** using their credentials, complete multi-factor authentication, and lock the device when stepping away.
2. **Keep software current** by installing application, browser, and operating-system updates through the approved channel and scheduling restarts.
3. **Defend against attacks** by identifying phishing red flags, responding safely, recognizing signs of malware, and reporting incidents correctly.

MATERIALS & SETUP CHECKLIST

- [ ] Provisioned account + single-use temporary password per learner
- [ ] Authenticator app installed on each learner's phone (or hardware token)
- [ ] Company Portal / Software Center available on each device
- [ ] Projector or screen-share for live demonstration
- [ ] Printed *Secure Start Quick Reference* handout per learner
- [ ] Two sample phishing emails staged for the spot-it activity

ACCESSIBILITY & ACCOMMODATIONS

- [ ] Speak each on-screen step aloud as you perform it
- [ ] Offer the quick-reference in large-print and screen-reader text
- [ ] Demonstrate keyboard-only paths, not just the mouse
- [ ] Allow extended hands-on time; never rush the MFA step
- [ ] Confirm captions are on for any recorded segment
- [ ] Don't rely on color alone when pointing at the screen

SESSION PLAN

Run of show

TIME	SEGMENT	MODE
0:00	Welcome, why this matters, objectives	Facilitator
0:05	Module 1: Logging in	Demo + practice
0:17	Module 2: Updating company apps	Demo + practice
0:29	Module 3: Malware & phishing	Demo + activity
0:47	Assessment: knowledge + performance	Individual
0:55	Wrap, evaluation, where to get help	Facilitator

OPEN THE SESSION: SAY THIS

"Welcome to securibyte. The computer in front of you is now part of how we protect every customer's data. In the next hour you'll do three things yourself: sign in securely, keep your software patched, and learn to spot an attack before it lands. You don't need to memorize anything, because you'll leave with a one-page reference. Let's start by signing in."

SESSION PLAN · MODULE 1 OF 3

01

MODULE 1 · ACCESS

Logging in to your company computer

12 min

Objective: Learner signs in with their own credentials, completes MFA, and locks the screen without help.

SAY THIS

"Your sign-in is the front door. A strong passphrase plus a second factor means that even if someone learns your password, they still can't get in. We'll set both up right now."

DO THIS: DEMONSTRATE, THEN HAVE THEM REPEAT

1. Power on and wait for the lock screen. On Windows, press **Ctrl + Alt + Delete** to reach sign-in.
2. Enter the company username (**first.last**) and the single-use temporary password.
3. When prompted, create a **passphrase** of at least 14 characters, ideally four unrelated words. Never reused from a personal account.
4. Enroll multi-factor authentication: approve the prompt in the authenticator app, or enter the 6-digit code.
5. Show how to lock instantly with **Windows + L**, and make it a habit whenever stepping away.

CHECK FOR UNDERSTANDING

- "Why isn't a strong password alone enough?" *(Looking for: MFA stops a stolen password from working.)*
- "Show me how you'd lock this screen right now." *(Performance check: they do it.)*

Common pitfalls: Caps Lock left on during the temp password; temp passwords expire quickly, so reset before the session if needed; reassure anyone uneasy about the authenticator app that it never reads personal phone data.

02

MODULE 2 · MAINTENANCE

Updating company applications

12 min

Objective: Learner installs app, browser, and OS updates through the approved channel and schedules a restart.

SAY THIS

"Most attacks don't break in. They walk through a hole that an update already fixed. Updating isn't busywork; it's how we close those holes. Everything you install comes from one trusted place: the Company Portal. Never from a search result or a pop-up."

DO THIS: DEMONSTRATE, THEN HAVE THEM REPEAT

1. Open **Company Portal** (or Software Center) and go to the **Updates** tab. Select **Update all** and let it run.
2. Check the operating system: **Settings → Windows Update → Check for updates**. Install anything pending.
3. Update the browser: open the menu → **Help → About**; it updates and prompts to relaunch.
4. Save open work, then **schedule the restart** for outside working hours if one is required.

CHECK FOR UNDERSTANDING

- "You need a new app for your role. Where do you get it?" *(Looking for: Company Portal, never the open web.)*
- "What do you do before a restart finishes installing updates?" *(Looking for: save your work.)*

Common pitfalls: Endlessly postponing the restart, since updates aren't applied until it completes; downloading software from the web instead of the Portal; forgetting that the OS and browser need updates too, not just apps.

03

MODULE 3 · DEFENSE

Staying safe from malware & phishing

18 min

Objective: Learner spots phishing red flags, responds safely, recognizes malware signs, and reports through the right channel.

SAY THIS

"Phishing is just a message engineered to make you act before you think, usually with urgency, fear, or a too-good offer. You don't have to be a security expert. You only need to slow down and check four things on anything that asks you to click, log in, or pay."

DO THIS: THE FOUR-POINT CHECK (WRITE IT UP WHERE EVERYONE CAN SEE)

- **Sender.** Is the address really who it claims? Hover to see the true domain; look for look-alikes.
- **Links.** Hover before clicking. Does the URL match the real site, or is it slightly off?
- **Ask.** Is it pushing urgency, secrecy, payment, gift cards, or your password? Real IT never asks for your password.
- **Attachments.** Unexpected file? Don't open it. Confirm with the sender through a known channel first.

ACTIVITY: SPOT THE PHISH (5 MIN)

Show two staged emails, one genuine and one phishing. In pairs, learners apply the four-point check and call out which is which and why. Then demonstrate the **Report Phishing** button (or forwarding to **phishing@securibyte.com**) and delete.

MALWARE: SAFE HABITS TO DEMONSTRATE

- Keep automatic updates and the company antivirus on; don't disable them.
- Only install from the Company Portal; never plug in an unknown USB drive.
- Lock your screen (Windows + L) every time you walk away; use the VPN on untrusted Wi-Fi.
- Watch for warning signs: sudden slowness, surprise pop-ups, unknown new programs, or antivirus alerts, and report these.

CHECK FOR UNDERSTANDING

- "An email says your account locks in 10 minutes and asks you to click to verify your password. What do you do?" *(Don't click; report it; urgency + password ask are red flags.)*
- "Where do you report a suspicious message?" *(Report Phishing button / phishing@securibyte.com / Help Desk.)*

Common pitfalls: Feeling embarrassed to report a click. Stress that fast reporting is always right and never punished; trusting a message just because it shows the securibyte logo; assuming antivirus catches everything.

Assessment: confirm they can do it

SUMMATIVE

Knowledge check (5 items)

Short multiple-choice covering one objective each, plus two scenarios. **Pass = 4 of 5 (80%).** Review any missed item before they leave.

PERFORMANCE

Can-do checklist

- [ ] Signs in + completes MFA unaided
- [ ] Runs updates via Company Portal
- [ ] Applies the four-point check to an email
- [ ] Reports a phishing sample correctly

Evaluation

Reaction One-minute exit survey: was it clear, useful, the right pace?

Learning Knowledge-check score (target ≥ 80%) and the completed can-do checklist.

Behavior At 30 days, IT confirms the learner's device is patched and reviews any phishing reports they filed. This is the real measure of transfer.

> **WRAP UP: SAY THIS**
>
> *"You just did all three: you signed in securely, you patched your machine, and you can spot an attack. Here's your one-page reference. Keep it by your desk. When in doubt about anything, the Help Desk would always rather hear from you early. Welcome aboard."*

FACILITATOR TIPS

- Do every step live before they copy it; never describe from memory.
- Let silence sit after a check question; give them time to answer.
- Hand out the quick-reference at the *start* so they can annotate.
- Normalize reporting mistakes; it's the single most protective habit.
- Note the Help Desk extension on the board and leave it up all session.
- If MFA enrollment stalls, move on and circle back; don't stall the room.