Text Based Storyboard

Cybersecurity in the Wild

Luis Joann Alvarado

Course Title: Digital Nomad or Digital Victim? Securing Your Remote Workspace

1. Global Introduction

Logic behind this web based training

You can complete the modules in any order. Each module places you in a high risk remote work situation. You will make decisions under time pressure. You can ask for help if you are unsure. If you select an incorrect answer you will get additional information and will be prompted to try again. Complete a module to earn a security badge.

Collect all badges to complete the training.

On screen text

You are no longer protected by office walls.

Remote work gives flexibility, but it also creates new risks. Cyber incidents often happen in ordinary moments. A quick coffee break. A low battery. A shared home network.

In this training, you will step into real world remote work situations. Each decision you make has consequences. Some are small. Some expose company data.

Your goal is simple
Work securely, wherever you are.

2. Module Selection Screen

Learners will be prompted to choose their module or mission. Each mission displays an empty badge icon. Completed modules show a filled badge.

There will be 3 different modules or missions to choose from:

a. Securing the Home Workspace
b. Working Safely in Public Spaces
c. Travel and Charging Risks

On screen text

Choose Your Mission

3. Module: Securing the Home Workspace

Badge Earned: Home Network Defender

On Screen Text

Home networks are one of the most common entry points for security incidents.

Shared WiFi, smart devices, and family activity increase risk. Attackers look for weak passwords, outdated routers, and unsecured devices.

Best practices you will apply in this module:

- Secure your home WiFi
- Recognize suspicious network activity
- Protect your device during virtual meetings

Scenario: The Hacker House

Scene Setup

You are working from home on a confidential project. A family member is gaming online. A video meeting is about to start.

Your laptop connects to your home WiFi.

A notification appears: New device connected to network
Unknown_User

Decision Point: What do you do next?

- Option A: Ignore the alert and join the meeting
- Option B: Change your WiFi password after the meeting
- Option C: Pause work and secure the network now

Help Option Text

Look for actions that reduce risk immediately. Delaying security actions often increases exposure.

Feedback and Consequences

- Option A: You proceed with the meeting. The unknown device remains connected. Risk increases due to potential unauthorized access.
- Option B: You delay action. Sensitive data remains exposed during the meeting.
- Option C: Correct choice. You secure the network before continuing work.

Key Takeaway

- Secure home networks before handling sensitive work.
- Use strong encryption, updated routers, and unique passwords.
- If something looks wrong, act immediately.

4. Module: Working Safely in Public Spaces

Badge Earned: Public Space Protector

On Screen Text

Public spaces create both physical and digital risks.

Open WiFi networks, close seating, and shared spaces increase the chance of data exposure. Attackers often rely on visibility and convenience rather than technical skill.

Best practices you will apply in this module

- Protect your screen from others

- Lock devices when unattended
- Use VPNs on public networks

Scenario: The Coffee Shop Caper

Scene Setup

You are working in a busy cafe. Your laptop is open with work documents visible. A stranger sits behind you.

You need to use the restroom.

Decision Point: What do you do?

- Option A: Leave the laptop open to save your seat
- Option B: Lock the screen and leave the laptop on the table
- Option C: Take the laptop with you

Help Option Text

Think beyond theft. Consider what others can see or capture when you are away.

Feedback and Consequences

- Option A: High risk. Anyone can view or access your data.
- Option B: The screen is locked, but exposure remains. A short video shows the stranger photographing the screen before it locked.
- Option C: Correct choice. You remove both physical and visual risk.

Key Takeaway

- Physical security matters as much as digital security.
- If you are more than a few feet away, take the device with you.

5. Module: Travel and Charging Risks

Badge Earned: Travel Security Pro

On Screen Text

Travel creates pressure to stay connected.
Low battery and limited outlets lead to risky decisions.

Public charging stations and personal workarounds are common sources of data exposure.

Best practices you will apply in this module

- Avoid public USB charging ports
- Use approved power sources
- Protect work data during travel

Scenario: The Airport Juice Jack

Scene Setup

You are at an airport gate. Your laptop battery is at 2 percent. A presentation starts in 30 minutes.

You see a free USB charging station nearby.

Decision Point: What do you do?

- Option A: Use the USB charging port
- Option B: Use your own wall charger and outlet
- Option C: Forward the file to personal email and use a kiosk

Help Option Text

Convenience often hides risk. Look for options that keep company data under control.

Feedback and Consequences

- Option A: High risk. USB ports can transmit malware or extract data.
- Option B: Correct choice. Power without data connection.
- Option C: High risk. Personal email breaks data security controls.

Key Takeaway

- Never use public USB ports.
- Avoid personal email for work files.
- Protect the chain of custody for company data.

6. Final Completion Screen

All Badges Earned

On Screen Text

You have completed all missions.

Secure work habits reduce risk everywhere. At home. In public. While traveling.

Training Complete.