Design Document

Cyber Security in the Wild

Luis Joann Alvarado

Cybersecurity in the Wild

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

1. Project Overview

Business Problem: Remote employees are increasingly working from home, cafes, and airports. IT has identified a rise in preventable security incidents related to remote work, including unsecured WiFi use, shoulder surfing, and unsafe charging practices.

Business Impact: These incidents increase the risk of data exposure, compliance issues, and reputational damage. Many incidents occur due to poor decisions made under time pressure rather than lack of awareness.

Proposed Solution: A short, scenario based web based training that allows employees to practice making secure decisions in realistic remote work situations. The training focuses on high risk moments where mistakes are most likely to occur.

2. Target Audience

Primary Audience: Remote and hybrid employees who regularly work outside of corporate offices.

Secondary Audience: Employees who travel for business and work from public locations such as airports, hotels, and cafes.

Learning Context: Learners often work under time pressure, in distracting environments, and may prioritize convenience over security.

3. Learning Goals and Success Measures

Primary Goal: Reduce preventable remote work security incidents by 25% within the first quarter after training deployment.

Success Measures:

- Decrease in IT reported remote work related incidents
- Post training knowledge checks
- Employee confidence survey on secure remote work practices

4. Required Behavior Changes

After completing the training, employees will be able to:

- Use a VPN whenever connected to public WiFi
- Lock devices when unattended, even briefly
- Avoid public USB charging ports
- Avoid forwarding work documents to personal email accounts

These behaviors directly address the most common remote work security failures identified by IT.

5. Learning Strategy

Instructional Approach

The training uses short, realistic scenarios that mirror common remote work environments. Learners make decisions under time pressure and receive immediate feedback that shows the consequences of their choices.

Design Methodology

The design is informed by SME interviews and established instructional design practices, including ADDIE and action mapping, with a focus on real world decision making rather than policy recall.

6. Content Scope and High Level Outline

Module 1: Securing the Home Workspace

- Risks of shared home networks
- Device and router security basics

Module 2: Working Safely in Public Spaces

- Physical security and shoulder surfing
- Safe use of public WiFi

Module 3: Travel and Charging Risks

- USB charging risks
- Safe alternatives when device power is low

7. Project Deliverables

1. Web based training developed in Articulate Storyline
2. Text based storyboard for design and stakeholder review
3. Downloadable job aid in infographic format for performance support

8. Assumptions and Constraints

- Learners have access to a company issued device
- VPN access is already provisioned
- Training length target is 15 to 20 minutes
- Training materials will be available via the corporate LMS

9. Stakeholders and Review

Primary Stakeholders

- IT Security
- Learning and Development Team
- Legal or Compliance Teams, if required

Review Checkpoints

- Design document review and approval
- Text storyboard review and approval
- 1 review cycle for the final learning assets
- Final course sign off