# Security and Privacy Risks of Low-Cost Fitness Tracking Devices and Applications

*"Counting Steps, Losing Privacy"*

Project Proposal

by

Wiktor Knapik – C00283826

SETU Carlow Campus
BSc (Hons) IT Security & Cybercrime

## Executive Summary

This project focuses on the security and privacy risks that are associated with low-cost fitness tracking devices and the mobile application that comes with the device. These devices are specifically chosen from online shops such as Temu, AliExpress and Shein. These devices collect sensitive personal information, including health metrics and location data. Due to the cost of these devices ranging from as little as €5 - €20 compared to the reliable highly known brands which come at a cost of €100+, the cheap devices are often developed with limited regulations and minimal security safeguards.

## Project Background

Fitness tracking devices have become a major part of many people's everyday life. These devices help people monitor steps, heart rate and used within individuals to become motivated to reaching goals. While high established brands such as Fitbit, Garmin, and Apple typically invest heavily in security and are trusted by consumers, many low-cost alternatives are widely available online for under €20. These low prices are often attracted by new gym goers or people who never owned a high established device, but they have faced repeated criticism for poor build quality and a lack of transparency regarding data handling practices.

My personal interest in this project comes from two areas. Firstly, fitness and the gym are an important part of my weekly routine and life. While going to the gym and keeping on track with my health, I use well known tracking devices to monitor my improvements. I often see others using cheap alternative devices which raises the question on how safe these devices actually are when handling sensitive health and location data. I also have a strong interest in pen testing being the man-in-the-middle attacks which makes this project a great opportunity to learn extra skills in a real world environment.

## Objective

The primary objective of this project is to evaluate the security and privacy practices of low-cost fitness tracking devices and their associated applications. This will involve applying penetration testing and digital forensics techniques to uncover potential weaknesses and assess the risks they pose to consumers. Specifically, the project will:

- Analyse the permissions requested by companion applications and determine whether they are appropriate in relation to the advertised features.
- Capture and review network traffic, focusing on identifying unencrypted data transmissions or connections to untrusted or suspicious servers through man-in-the-middle inspection.
- Investigate device storage for forensic artefacts such as health metrics, GPS records, and cached application data that could be exposed or misused.
- Evaluate the applications against the OWASP Mobile Top 10 security risks to highlight common vulnerabilities.
- Provide practical recommendations for both end users and organisations regarding the risks of adopting low-cost fitness trackers in comparison to more secure, branded alternatives.

## Outcome

- A detailed written report documenting the security and privacy risks identified throughout the investigation.
- Evidence containing supporting material such as screenshots of app permissions, captured network traffic logs, and key forensic artefacts recovered during testing.
- Live demonstration showcasing the findings and their implications for consumers and organisations.

## Technologies

**Devices**

- Three low-cost fitness trackers sourced from Temu, AliExpress, and Shein.

**Mobile Platform**

- An Android phone to use as a consumer device of the low-cost device and application.

**Traffic Analysis Tools**

- Wireshark - Capturing and analysing network traffic.
- mitmproxy - Intercepting and inspecting HTTPs traffic.
- Burp Suite - Identifying insecure communications and vulnerable endpoints.

**Mobile Application Security**

- MobSF - Perform static and dynamic analysis of Android applications.

**Digital Forensics Tools**

- ADB (Android Debug Bridge) - Extract device files and application data.
- SQLite DB Browser - Examining and analysing local application databases.

## Conclusion

This project explores an important but often overlooked area of cybersecurity which are the risks of choosing a cheaper alternative fitness tracking device along with their application. As these devices become more commonly bought and used, the lack of effective security controls represents a growing threat to personal and health-related data.

By applying methods from penetration testing, digital forensics, and practical device analysis, the project will provide clear insights into the vulnerabilities of budget fitness trackers when compared to established known brands. The outcomes are expected not only to highlight technical flaws but also to increase awareness of the big privacy concerns associated with these devices.