# CYB 250 Stepping Stone Two Template

| Howard Threat Model | | |
| --- | --- | --- |
| Incident | Bank Attacks | Bluetooth Bug |
| Attackers | Attackers are said to be Nigerian, Cameroon, and Spanish | Attackers are unknown |
| Tools | Malware and Social Engineering Tools | Bluetooth Sniffer Tool |
| Vulnerability | The HTML from the official site was used to create a man-in-the-middle site for users so they can get sensitive information. | Since the devices were using Secure Simple Pairing and Low Energy (LE) Secure Connections venders were able to opt out of implementing the public key authentication. |
| Action | Monitoring communications for the payment requests and establishing access connections | Send forged pairing messages between two vulnerable Bluetooth devices, intercepting traffic, and any attacker within 30 meters can gain unauthorized access via any adjacent network. |
| Target | Large and Medium European Companies are Targeted | Any Bluetooth device was Targeted |
| Unauthorized Result | Attackers use a sophisticated network of money laundering transactions that transferred the money they stole from the European Companies. | The attackers intercepted and decrypted all device messages and forged and injected messages |
| Objective | Financial Gain | Various Objectives |

The incident that I will talk about is the Bank Attacks where 49 suspects that were spread throughout Europe were arrested on suspicion of man-in-the-middle (MiTM) attacks. What the MiTM managed to do is taking the HTML from the official website and made their own. This means that they then can get sensitive information from the customers from these banks. In doing this they were able to gain access to several accounts by sending them the web address they made and asking to put in there information. Since they had the HTML from the official web page the people didn’t know it was a scam.

The attackers where able to access the HTML because it wasn’t secure. Then they were monitoring communication requests for payments and establishing access connections for the accounts. That then allowed them to access what they needed to get the information on making the fake web page and making people believe that they are on the real web page.

The techniques that could have been used to prevent the MiTM attack where that they needed to secure the HTML better. If this was more secure they would not have been able to steal it and put it on a fake web page. Also, they would need to monitor the communication and the connections for the accounts so that no one else can monitor them as well. All that is really needed to prevent these attacks and to prevent any future attacks is to pay attention and make sure every part of the website is secure.

**References**

June 11, 2015/[49 busted in Europe for Man-in-the-Middle bank attacks – Naked Security (sophos.com)](https://nakedsecurity.sophos.com/2015/06/11/49-busted-in-europe-for-man-in-the-middle-bank-attacks/)

Seals, T./July 24, 2018/[Bluetooth Bug Allows Man-in-the-Middle Attacks on Phones, Laptops | Threatpost](https://threatpost.com/bluetooth-bug-allows-man-in-the-middle-attacks-on-phones-laptops/134332/)