# Network Security

1. Potential Security Issues
   1. **Customer Security Practices**

**Issue:**

One potential issue is with the customer’s personal security practices, i.e. does the customer use a passcode on their phone, is that the same passcode as is used in the mobile app (is there even a passcode on the mobile app). Similar concerns can be applied to access to the customer accessing the website on a personal computer at home where computers often do not have password protection and will save passwords to websites in the browser.

**Solution:**

A solution to these issues could be to both encourage proper password etiquette, such as using a secure password manager, as well as securing the app with a PIN, password, 2fa, biometrics, etc. (while encouraging it to be different than that of the mobile device).

* 1. **Public Wi-Fi and MITM**

**Issue:**

When users are accessing their accounts when away from home, there is often a desire to connect to public, often unsecured, Wi-Fi. This convenient source of internet can hide an attacker who can implement a man in the middle attack, and so would be able to intercept all communications between the customer’s browser and the bank.

**Solution:**

To help protect against these types of attacks, the bank could warn the user when they connect via an unsecured Wi-Fi connection or encourage the use of VPN’s when connecting to public or unsecured Wi-Fi.

* 1. **Employee Security Practices**

**Issue:**

Email security is a large concern in a corporate environment. Having worked in an IT environment for around five years, I have experienced even system security experts succumb to email sourced attacks. There have been breaches in my company from these kinds of attacks. Money has been transferred to a malicious third party while an attacker pretends to be an executive, emails have been used to infect the network with ransomware, and passwords have been guessed based on phishing and social engineering.

**Solution:**

As well as increased network security in general, implementing a system similar to that of IronPort provided by Cisco. These types of services provide anti spam, email reputation services, and other email security applications. Emails from external parties, regardless if they are trying to imitate local email addresses, can be filtered, and marked as such when arriving at the user’s inbox.

1. Bank employee modifies customer’s daily cash transfer limit.
   1. If the employee is away from the bank network, they need to connect to the bank servers via a secure connection.
   2. Bank Employee received the request and verifies the customer with some sort of identification. (Government issued ID, verbal password, SMS authentication, etc.)
   3. Once the customer is authenticated, employee logs into bank system via either desktop application or web browser.
   4. Bank employee makes the necessary changes to the customer’s account.
   5. A notification of the change is sent to the customer via email or SMS.
   6. Bank employee logs off.
2. Kerberos, SAML, and OAuth
3. IPSec, SSL/TLS, and SSH