**1) My Services, Devices, Accounts, and Their Security**

* **Email (Personal and Professional)**:
  + **Security Measures**: Strong, unique passwords; two-factor authentication (2FA); regular password updates.
  + **Loopholes**: Limited use of encrypted communication.
* **Banking and Financial Apps**:
  + **Security Measures**: Complex passwords; biometric authentication; regular account monitoring.
  + **Loopholes**: Infrequent updates to account information.
* **Social Media (Facebook, Twitter, LinkedIn)**:
  + **Security Measures**: Strong passwords; 2FA; limited sharing of personal information.
  + **Loopholes**: Potential oversharing of information.
* **Laptop and Smartphone**:
  + **Security Measures**: Full disk encryption; strong device passwords; regular software updates.
  + **Loopholes**: Public Wi-Fi usage without VPN; infrequent backups.
* **Online Shopping Accounts (Amazon, eBay…)**:
  + **Security Measures**: Strong, unique passwords; 2FA; secure payment methods.
  + **Loopholes**: Occasional use of unsecured public Wi-Fi networks for transactions.

**2) Possible Threats Relating to the Used Services/Devices/Accounts**

* **Phishing Attacks**:
  + **Targets**: Email, Social Media, Online Shopping Accounts.
  + **Risks**: Unauthorized access, identity theft, financial loss.
* **Malware Infections**:
  + **Targets**: Laptop, Smartphone.
  + **Risks**: Data loss, compromised privacy, financial loss.
* **Unauthorized Access to Financial Accounts**:
  + **Targets**: Banking and Financial Apps.
  + **Risks**: Financial loss, identity theft.
* **Data Breaches on Social Media**:
  + **Targets**: Social Media Accounts.
  + **Risks**: Privacy invasion, potential identity theft.

**3) Detailed Plan on Addressing These Threats**

* **Phishing Attacks**:
  + **Mitigation**: Regularly review and verify sender information. Educate myself and stay vigilant against suspicious emails.
* **Malware Infections**:
  + **Mitigation**: Install reputable antivirus software. Avoid downloading from unknown sources. Regularly scan devices for malware.
* **Unauthorized Access to Financial Accounts**:
  + **Mitigation**: Enable strong, unique passwords and 2FA. Monitor accounts for suspicious activity and update login information regularly.
* **Data Breaches on Social Media**:
  + **Mitigation**: Review privacy settings and limit the information shared publicly. Regularly update passwords and review account activity.
* **Overall Improvements**:
  + Regularly update all passwords and enable 2FA wherever possible. Use secure, private networks for sensitive transactions. Regularly back up important data.

This plan will be reviewed and updated on a quarterly basis, or as new services/devices/accounts are added. Continuous education and staying informed about emerging threats will also be a priority. For further information, I'll refer to the provided course materials and Digital Scam Recognition resources from the [Finnish consumer union.](https://www.kuluttajaliitto.fi/en/materials/recognize-a-digital-scam-training-material/?fbclid=IwAR2F_8lt7c52Eq3BtgR_Rcg25cr5woy1T_FoOAb0erFzUqz-ec2PTaehDco)