After completing the Digital Defense Personal Security Checklist, I reviewed my overall score: 190 out of 256 items, with 93% Essential, 75% Optional, and 45% Advanced practices completed. The results give a clear picture of my current digital security habits and highlight where improvements are needed.

1. Safest Segments

The categories where I performed best were:

- Physical Security (15/16) – good habits in device protection and real-world security.
- Web Browsing (34/39) – strong privacy practices, safe browsing behavior, and use of privacy tools.
- Personal Computers (29/35) – solid operating system security, updates, and local protection.
- Human Aspect (19/21) – good awareness of social engineering risks.

These results show that my general security awareness and device management are at a good level.

2. Biggest Weaknesses

The weakest areas were:

- Personal Finance (4/10) – lack of security measures for online banking and financial accounts.
- Smart Home (8/13) – some IoT devices are not fully secured or configured with best-practice settings.
- Networks (14/25) – room for improvement in network segmentation, VPN usage, and router configuration.

- Email (14/21) – several best practices still missing, such as additional hardening measures and advanced settings.

These areas represent the main attack surface where improvements would have the highest impact.

3. What Surprised Me

I was surprised by how many smaller, easy-to-overlook habits affect the total score—especially in categories like personal finance and IoT devices. Despite feeling generally secure, the checklist revealed more gaps than expected in areas I normally don't think about.

4. What I Will Change

Based on the results, I plan to:

- Improve security of financial accounts (stronger authentication, reduced exposure, better monitoring).
- Reconfigure my home network and secure IoT devices with stronger defaults.
- Strengthen email security settings and add missing protections.
- Regularly review account permissions and reduce unnecessary data sharing.

5. Reflection

How important is awareness of digital exposure?

Awareness is essential, many vulnerabilities come not from complicated attacks but from simple habits users tend to ignore. Understanding my digital exposure helps me prioritize which risks actually matter.

Would you recommend this tool to others?

Yes. It's simple, visual, and gives immediate insight into personal security. It would be especially useful for people who are not aware of how exposed they are online.

How would you adapt the checklist for schools or businesses?

For schools: simplify technical sections, focus on social media safety, password habits, and device protection.

For businesses: add sections on work accounts, phishing training, data handling policies, and company device security.