Tema 9

1. **Amenințări principale pentru dispozitivele mobile**

**Amenințări principale**

* **Malware** - programe malițioase care compromit funcționalitatea dispozitivului
* **Phishing** - atacuri care înșeală utilizatorii să dezvăluie informații confidențiale
* **Aplicații rău intenționate** - software legitim în aparență, dar cu funcții ascunse periculoase
* **Rețele Wi-Fi nesecurizate** - interceptarea comunicațiilor și datelor transmise
* **Exploatarea vulnerabilităților sistemului** - utilizarea defectelor din software pentru acces neautorizat
* **Furtul fizic** al dispozitivului
* **Atacuri de tip "Man-in-the-Middle"** - interceptarea comunicațiilor între dispozitiv și server

**Software pentru atacuri**

* **Spyware**: FlexiSpy, Pegasus, mSpy (monitorizează activitatea utilizatorului)
* **Ransomware**: WannaCry, Petya (criptează date și solicită răscumpărare)
* **Troiani**: Joker, EventBot, TeaBot (se ascund în aplicații legitime)
* **Rootkits**: Binder, Chrysaor (obțin acces la nivel de sistem)
* **Adware**: Shlayer, FakeAlert (afișează reclame intruzive și colectează date)
* **Keyloggers**: KeyDroid, Cerberus (înregistrează tastele apăsate)

**Modalități de compromitere a datelor private**

* **Permisiuni excesive** acordate aplicațiilor
* **Exfiltrarea datelor** prin aplicații malițioase
* **Inginerie socială** și atacuri de phishing (SMS, email, apeluri)
* **Interceptarea comunicațiilor** pe rețele nesecurizate
* **Backup-uri neparolate** în cloud
* **Exploatarea vulnerabilităților** din sistemul de operare
* **Furtul de credențiale** prin keylogging sau phishing
* **Accesul fizic neautorizat** la dispozitivul deblocat
* **Tehnici de fingerprinting** pentru urmărirea comportamentului utilizatorului
* **SIM swapping** - preluarea numărului de telefon pentru a depăși autentificarea în doi factori

# Măsuri de securitate pentru dispozitive mobile

## Măsuri principale de securitate

* **Actualizări sistem** - Instalați prompt toate actualizările sistemului de operare și aplicațiilor
* **Antivirus/Anti-malware** - Utilizați soluții dedicate dispozitivelor mobile
* **Gestionarea permisiunilor** - Acordați aplicațiilor doar permisiunile strict necesare
* **Descărcați aplicații doar din surse oficiale** - App Store, Google Play
* **Utilizați VPN** pentru conexiuni în rețele publice
* **Criptarea dispozitivului** - Activați criptarea completă a dispozitivului
* **Backup-uri securizate** și regulate
* **Soluție de localizare și ștergere la distanță** (Find My iPhone, Find My Device)
* **Dezactivați conectivitatea neutilizată** (Bluetooth, Wi-Fi, NFC)
* **Evitați root/jailbreak** deoarece eliminează protecțiile sistemului

## Parole sigure pentru dispozitive mobile

### Cele mai sigure tipuri:

* **Parole lungi și complexe** (minim 12 caractere) cu combinații de litere, cifre și simboluri
* **Modele complexe** pentru deblocare care utilizează cel puțin 7-9 puncte în configurații neobvie
* **Autentificare biometrică** (amprentă, recunoaștere facială) combinată cu o parolă puternică

### De ce sunt eficiente:

* **Complexitatea** crește exponențial timpul necesar atacurilor de forță brută
* **Unicitatea** previne atacurile bazate pe refolosirea parolelor compromise
* **Biometria** oferă un echilibru între securitate și ușurință în utilizare
* **Autentificarea multi-factor** asigură protecție chiar dacă un factor este compromis

# 3+4. Securitatea dispozitivului personal

Pentru dispozitivul meu Pixel 7 Pro am urmatoarele setari de securitate

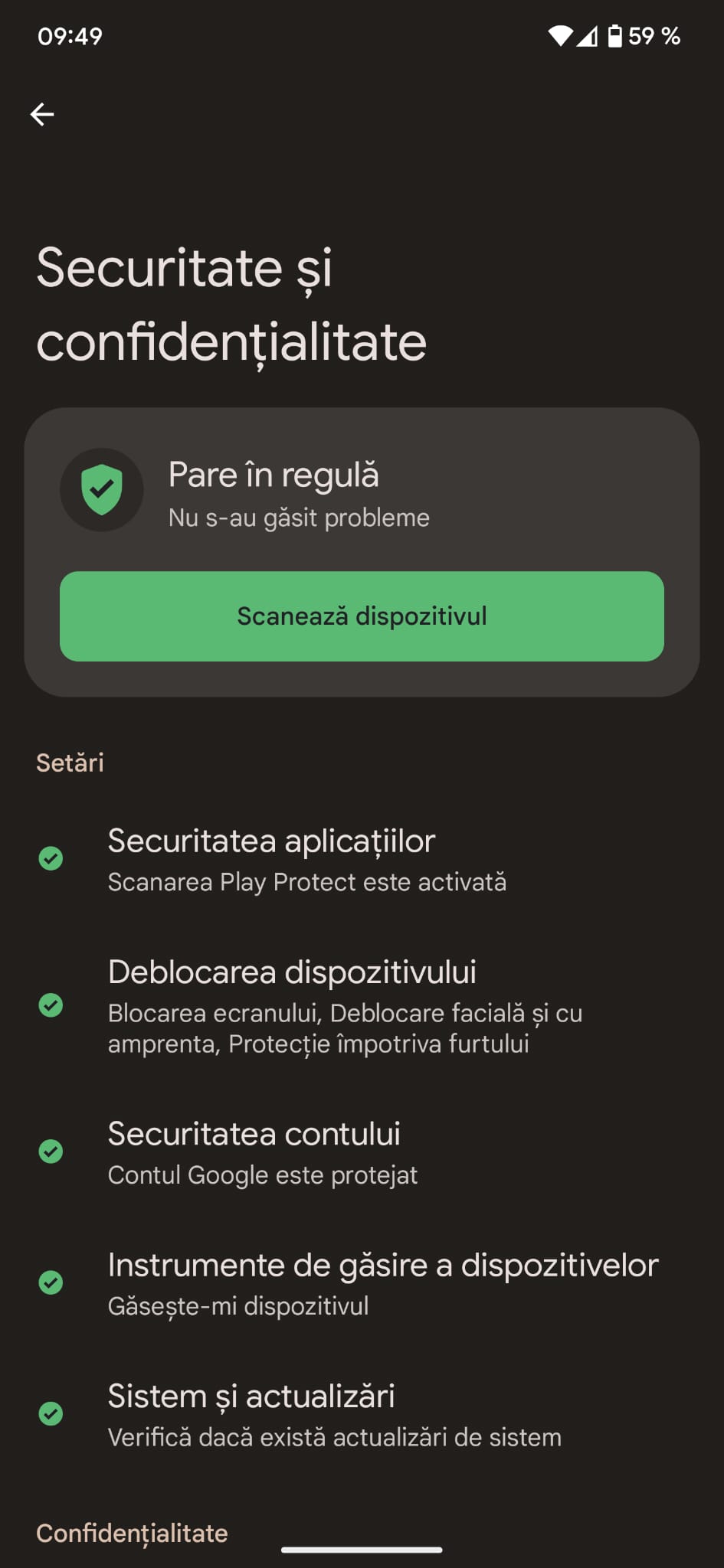
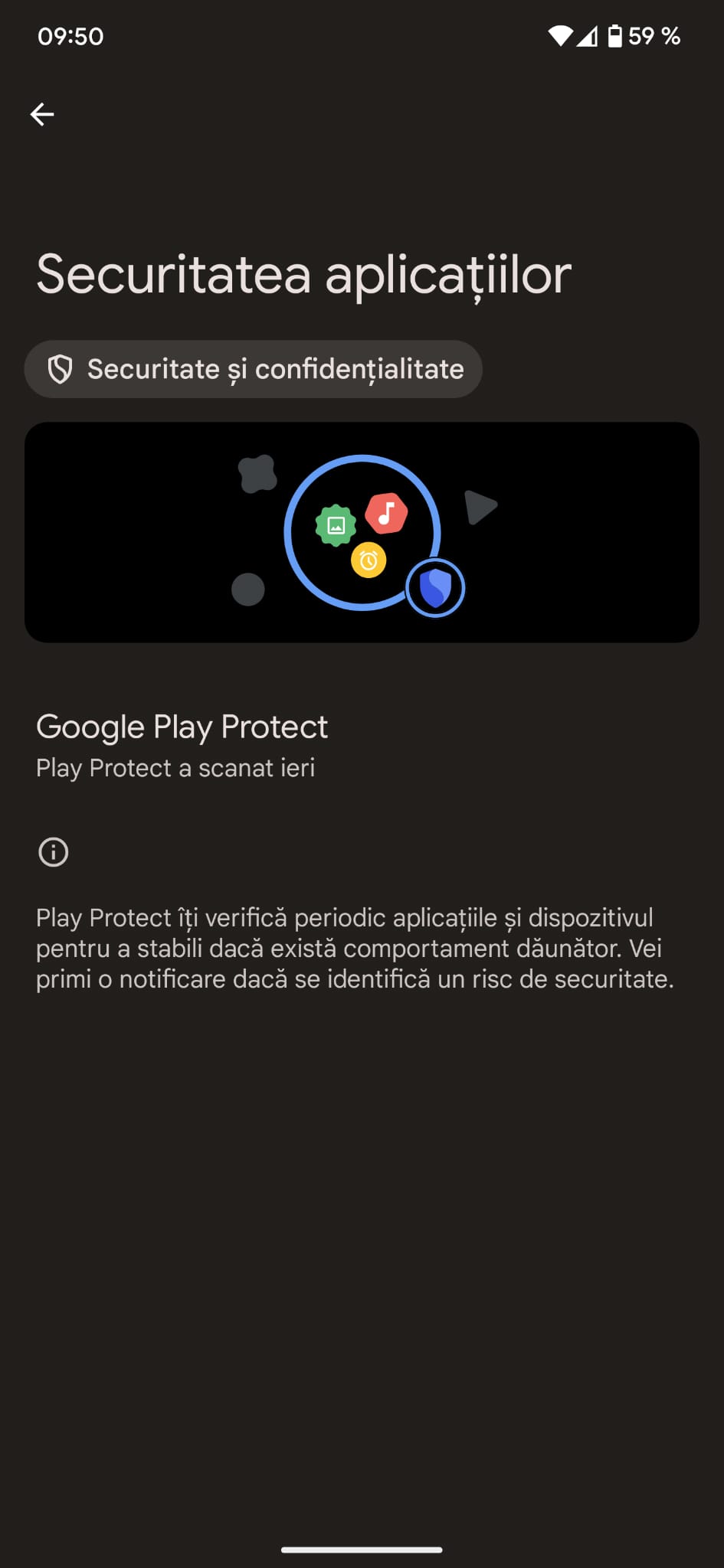
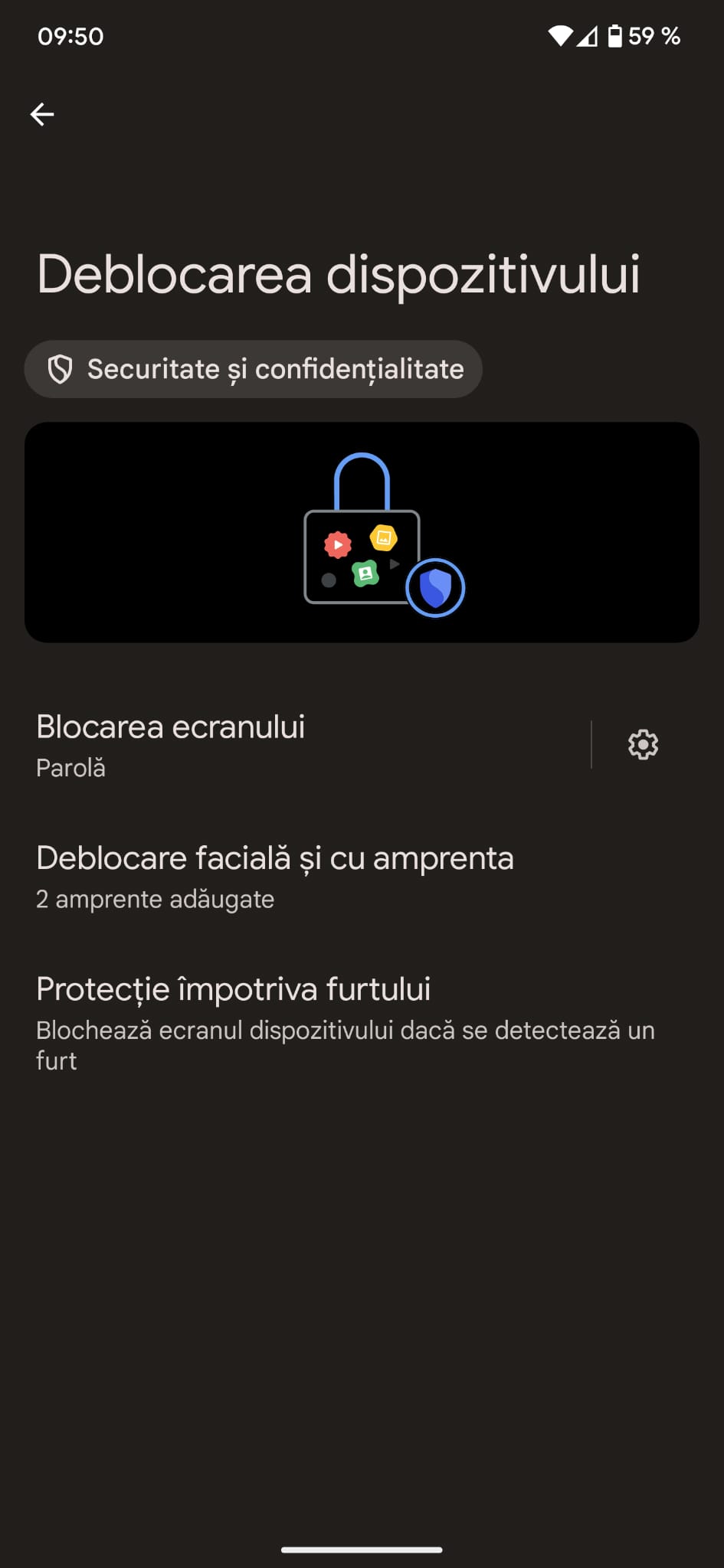
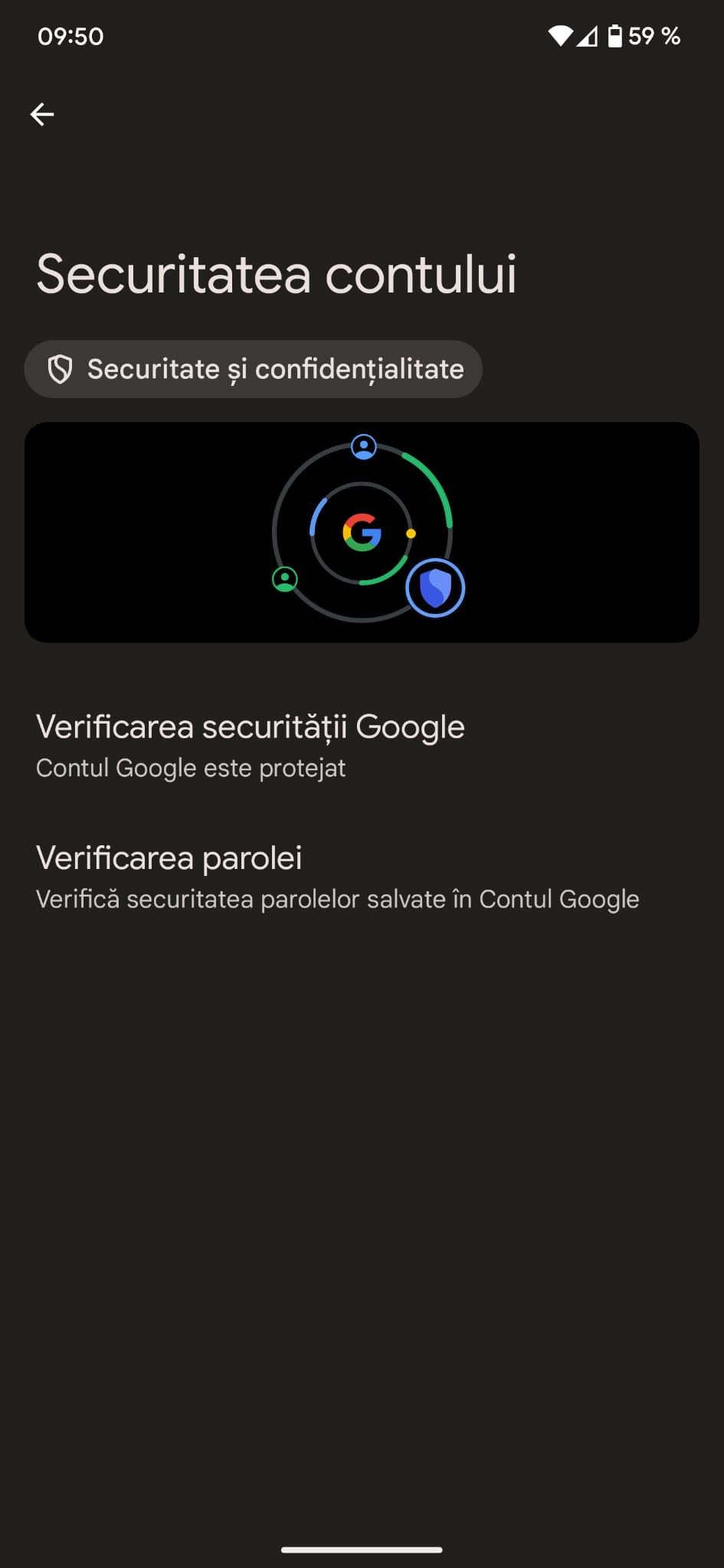
1. **Securitate generală** - "Pare în regulă" cu butonul "Scanează dispozitivul" pentru verificări manuale
2. **Securitatea aplicațiilor** - Play Protect activat, care scanează aplicațiile pentru comportament malițios
3. **Deblocarea dispozitivului** - Metode multiple configurate (blocarea ecranului, deblocare facială, amprentă) și protecție împotriva furtului
4. **Securitatea contului** - Contul Google este protejat, oferind funcții precum autentificare în doi factori
5. **Instrumente de găsire a dispozitivelor** - "Găsește-mi dispozitivul" activat pentru localizare, blocare sau ștergere la distanță
6. **Sistem și actualizări** - Verifică automat actualizările de securitate și pentru sistemul de operare

Aceste funcții reprezintă elemente cheie ale strategiei de securitate Google pentru dispozitivele Pixel, oferind protecție la mai multe niveluri: hardware, sistem de operare, aplicații și cont.

# Acțiuni de securitate întreprinse:

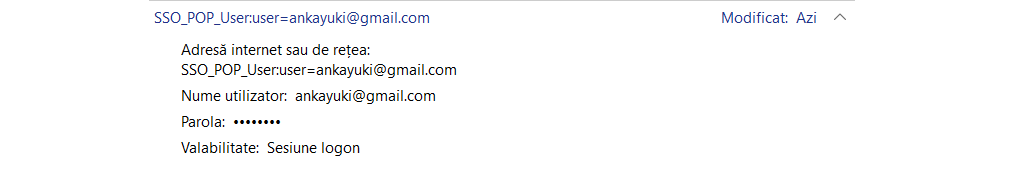
* Activare Play Protect pentru aplicații
* Folosire amprentă și parolă pentru deblocarea dispozitivului
* Activare Find My Device
* Actualizare la zi
* Aplicațiile au doar permisiunile necesare

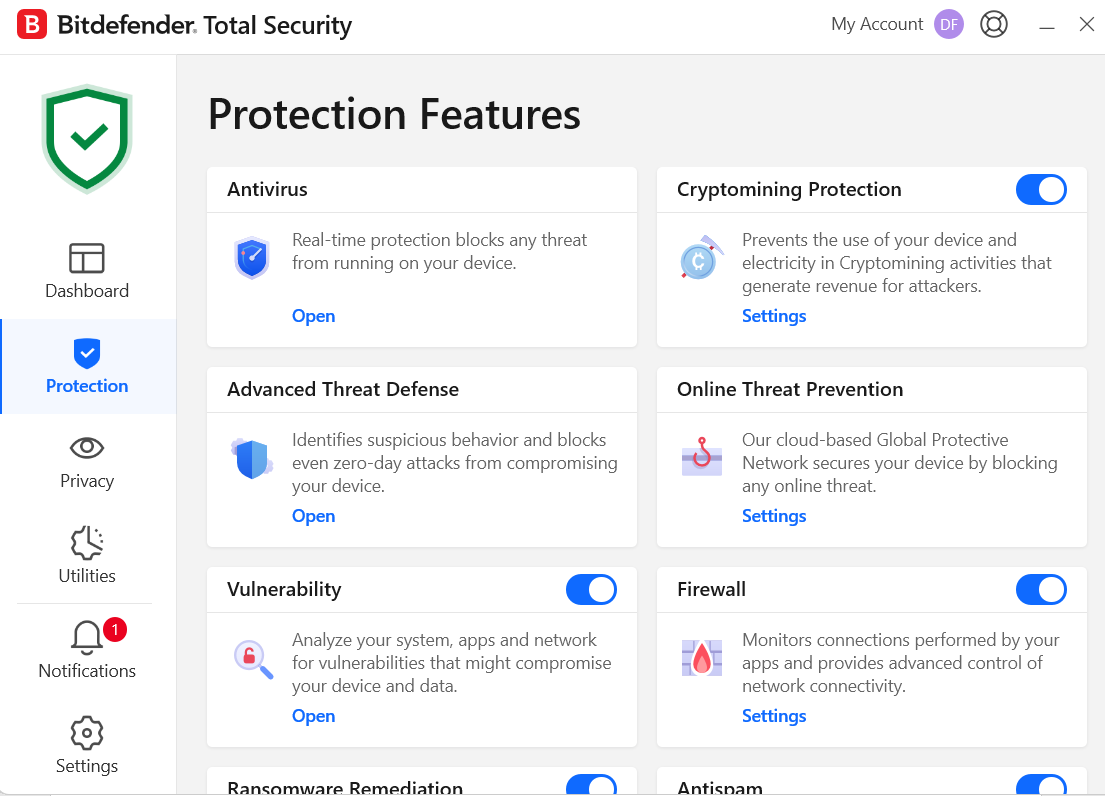
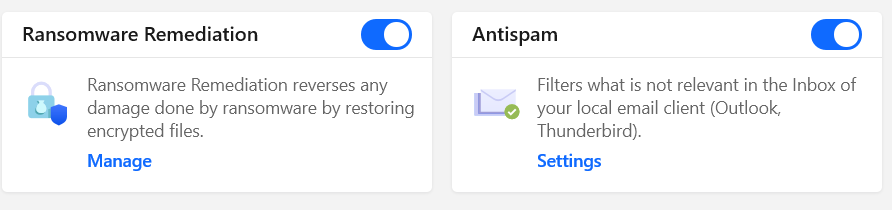
Un exemplu de acțiune ce nu am făcut-o încă este un backup al datelor personale în cloud-ul de la Google.



# Sarcina alternativa, securizare laptop

Utilizare cod pin de autentificare SSO



Utilizare Antivrus de la Bitdefender Total Security cu urmatoarele componente din imagine active  

De asemenea, utilizarea VPN Bitdefender, iar sistemul este actualizat la zi.

