Intrebări & răspunsuri
Vodafone Smart Protect/Vodafone Smart Protect Plus

1. *Cum se pot instala licenț ele pe alte dispozitive?*

În portalul de administrare Vodafone Smart Protect, puteți să adăugați noi computere (desktop, laptop), smartphone-uri şi tablete în contul pe care îl aveți şi să trimiteți programul de instalare pe noile dispozitive în limita numărului maxim de licenț e din pachet. Când instalați aplicaț ia pe noul dispozitiv, acesta va aparea ulterior în contul portalului de administrare.

Interfaț a este foarte intuitivă. Pentru a adăuga un nou dispozitiv este suficient să apăsaț i butonul „Adaugă dispozitiv" apoi sunteț i direcț ionat pas cu pas pentru a trimite licenț a către un alt dispozitiv sau pentru a îl instala pe dispozitivul de pe care aț i accesat portalul de administrare.

2. *Cum pot identifica pe câte dispozitive sunt instalate licenț ele din pachet?*

În portalul de administrare (https://safeavenue.f-secure.com/iframe/-sso/vodafoneromania) puteț i să vizualizaț i numărul de dispozitive pe care sunt instalate licenț ele incluse în pachet, utilizatorii ș i numărul de licenț e disponibile

3. *Cum procedez pentru a transfera o licenț ă de pe un dispozitiv pe altul?*

Pentru a transfera o licenț ă de pe un dispozitiv pe altul procedaț i astfel:

Pas 1: Eliberare licenț ă:

- Administratorul contului se loghează în portalul Vodafone Smart Protect
- Faceț i click pe iconiț a dispozitivului de pe care doriț i să eliberaț i licenț a (se va afisa o fereastră in care apar detalii de bază despre acest dispozitiv
- Faceț i click pe opț iunea "Eliberare licenț ă"
- Se va deschide o fereastra nouă pentru confirmarea acț iunii

Pas 2: Adăugare dispozitiv:

- Tot din portalul Vodafone Smart Protect faceț i click pe "Adăugare dispozitiv"
- Se deschide o fereastră nouă în care alegeț i al cui este dispozitivul.
- Se alege optiunea "Dispozitivul meu" si se deschide o nouă fereastră în care se alege tipul de dispozitiv
- După ce a fost ales tipul dispozitivului se deschide fereastra următoare in care alegeț i opț iunea dorită instalarea licenț ei pe dispozitivul de pe care aț i accesat portalul sau trimiterea prin mail sau SMS a link-ului pentru instalare

4. *Câte licenț e Vodafone Smart Protect trebuie să fie instalate pe un calculator dual-boot cu două sisteme de operare Windows sau MacOS?*

Este necesară o licenț ă pentru fiecare sistem de operare. Deci, pentru un calculator dual-boot sunt necesare doua licenț e.

5. Cum funcț ionează protecț ia la navigarea pe Internet?

Protecția la navigare vă ajută să navigați în siguranță pe Internet, furnizându-vă în browser evaluări de securitate pentru site-urile Web şi blocând accesul la site-urile Web care au fost evaluate ca dăunătoare de către F-Secure.

Uneori puteți naviga pe un site Web care are conținut suspect, contrafăcut sau interzis. De exemplu, site-ul Web poate fi un site falsificat, cunoscut pentru spam, poate conține programe potențial nedorite sau este ilegal indiferent în ce jurisdicție vă aflați.Puteți utiliza protecția la navigare pentru a evita accesarea accidentală a acestor site-uri Web.

Protecția la navigare utilizează extensii de browser pentru a vă oferi informații de securitate în timpul navigării.

De exemplu, dacă nu este instalată extensia pentru browser, veți vedea o pagină de eroare în browser în locul unei pagini de blocare, atunci când vizitați un site Web dăunător. De asemenea, este posibil ca rezultatele căutării să nu vă arate pictogramele de evaluare a siguranței.

Notă: Chiar dacă nu este instalată pe calculator extensia pentru browserul implicit, Vodafone Smart Protect vă protejează în continuare în timpul navigării, dar nu vedeți informațiile de securitate.

6. Cum funcț ionează protecț ia operaț iunilor bancare?

Protecția operațiunilor bancare adaugă încă un nivel de securitate, pentru a împiedica atacatorii să intervină în tranzacțiile dvs. confidențiale şi vă protejează împotriva activităților dăunătoare atunci când accesați online banca dvs. sau când efectuați tranzacții online.

Protecția operațiunilor bancare detectează în mod automat conexiunile securizate către site-urile bancare şi blochează orice conexiune care nu conduce către site-ul dorit. Când deschideți un site online al unei bănci, sunt permise numai conexiuni către site-uri bancare sau către site-uri Web care sunt considerate sigure pentru operațiunile bancare online.

Când protecția operațiunilor bancare este activată, ea detectează în mod automat momentul când accesați online site-ul Web al unei bănci. Când deschideți în browser un site Web de tranzacții bancare online, în partea de sus a ecranului apare notificarea **Protecție operațiuni bancare**. Cât timp protecția pentru operațiuni bancare este activă, toate celelalte conexiuni sunt blocate.

Notă: Pentru a profita de toate avantajele protecț iei bancare pe dispozitivele cu sistem de operare Android, vă rugăm să utilizaț i navigatorul Vodafone Smart Protect

7. De ce am nevoie de protecț ia tranzacț iilor bancare?

Serviciile bancare online au început să fie din ce în ce mai frecvent utilizate în societatea digitalizată contemporană. Băncile investesc masiv în vederea garantării protecț iei datelor dumneavoastră. Cu toate acestea, fără o vigilenț ă constantă, atacatorii cibernetici au mai multe modalităț i de a ajunge la datele dumneavoastră bancare sensibile. Aceș tia pot accesa datele în moduri ascunse, iar dumneavoastră să nu vă daț i seama de acest lucru decât în momentul în care este prea târziu.
Atunci când este activată pe dispozitivul dumneavoastră, protecț ia tranzacț iilor bancare permite combatarea tehnicilor utilizate de atacatori în vederea furtului de date personale. Câteva din aceste tehnici sunt:

- **Site-uri Web false** - Hackerii pot utiliza site-uri bancare false care par a fi veritabile. Astfel, autentificându-vă utilizând username-ul ș i parola, le daț i acces la toate datele dumneavoastră bancare.
- **Keylogger (program de înregistrare a tastelor)** - După cum sugerează ș i numele, un keylogger captează ș i înregistrează în secret combinaț iile de taste utilizate, apoi trimite acele informaț ii expeditorului programului. Este recomandat să vă scanaț i computerul în mod regulat pentru a elimina riscul de a avea instalate pe dispozitiv programe keylogger.

- **E-mailurile de phising și spam -** E-mailurile de phising sunt mesaje frauduloase care par să fi fost trimise de companii legitime. Conținutul lor vă redirecționează de obicei către site-uri web false sau vă păcălește astfel încât, în mod inconștient să divulgați informații personale care vor fi apoi utilizate pentru a accesa datele dvs. bancare.

8. Care sunt specificațiile tehnice minime pentru instalarea Vodafone Smart Protect?

Windows:

- Versiuni compatibile:
  - ✓ Windows 10
  - ✓ Windows 8.1
  - ✓ Windows 7 - Service Pack 1

  Notă: Tabletele ARM-based nu sunt compatibile)
- Procesor: Intel Pentium 4 sau superior
- Memorie: Minim 1 GB
- Spațiu liber pe disk: Minim 600 MB

Mac:

- Versiuni compatibile:
  - ✓ macOS version 11.0 (Big Sur);
  - ✓ macOS version 10.15 (Catalina);
  - ✓ macOS version 10.14 (Mojave)
- Procesor: Intel
- Memorie: Minim 1 GB
- Spațiu liber pe disk: Minim 250 MB

Android

- Versiuni compatibile: Android 6.0 sau mai recent
- Spațiu liber pe disk: Minim 70MB

iOS

- Versiuni compatibile: iOS13.0 sau mai recent
- Spațiu liber pe disk: Minim 10 MB

Important:

- ➢ Înainte de instalarea aplicației Vodafone Smart Protect pe computer sau laptop este recomandat să fie dezinstalate orice alte produse software antivirus instalate anterior pe acesta
- ➢ Pentru primirea actualizărilor automate este necesară conexiune la Internet
- ➢ Javascript trebuie să fie activat în setările browser-ului pentru a permite blocarea activă a paginilor web
- ➢ Browsere compatibile: Microsoft Edge (Chromium), Internet Explorer 11 (sau o versiune ulterioară), Mozilla Firefox, Google Chrome, Android browser (4.x sau mai recent), iOS Safari

9. Cum diferă funcționalitățile Vodafone Smart Protect în funcție de sistemul de operare al dispozitivului?

Soluția de securitate Vodafone Smart Protect oferă multiple funcționalități care asigură protecția dispozitivului împotriva amenințărilor de securitate online. Aceste funcționalități diferă în funcție de sistemul de operare al dispozitivului pe care este instalată aplicația software. În tabelul următor sunt prezentate funcționalitățile disponibile pentru fiecare tip de sistem de operare.

Functionalităț i	Windows	macOS	Android	iOS
Protecț ie navigare pe Internet Blochează paginile web dăunătoare ș i suspecte Nota: Pe dispozitivele mobile această funcț ionalitate este oferită prin Smart Protect Browser	√	√	√	√
Protecț ie tranzacț ii bancare Detectează în mod automat conexiunile securizate către site-urile bancare şi blochează imediat toate conexiunile către site-uri Web care sunt considerate nesigure pentru operațiunile bancare online. Nota: Pe dispozitivele mobile această funcț ionalitate este oferită prin Smart Protect Browser	√	√	√	√
Protecț ie antivirus Protecț ia automată a dispozitivelor împotriva viruș ilor, programelor de tip spyware ș i malware	√	√	√	
Protecț ia informaț iilor personale O combinaț ie de funcț ionalităț i: protecț ie antivirus, protecț ia tranzacț iilor bancare, protecț ie navigare Internet care asigură pretejarea informaț iilor personale ș i a activităț ii online	√	√	√	√
Protecț ie anti-ransomware Capabilitaț i de protecț ie bazate pe analiza comportamentului asigurată cu DeepGuard	√			
Reguli de Familie Protejaț i siguranț a online a copiilor prin blocarea conț inutului dăunător ș i setarea unor limite de utilizare a dispozitivelor	√	√	√	√
Finder Permite blocarea ș i/sau ș tergerea de la distanț ă a informaț iilor de pe dispozitivele Android			√	
Prevenirea furtului de identitate Reduceț i riscul de preluare a identităț ii dvs. online Nota: Doar in pachetele Vodafone Smart Protect Plus			√	√
Manager de parole Permite crearea unor parole puternice ș i stocarea lor în siguranț ă Nota: Doar in pachetele Vodafone Smart Protect Plus			√	√
Alerte privind breș e de securitate pe Android ș i iOS Sunteț i anunț aț i atunci când un serviciu popular a fost piratat Nota: Doar in pachetele Vodafone Smart Protect Plus			√	√
Portal web pentru managementul licenț elor Permite alocarea licenț elor incluse în pachet în funcț ie de preferinț e	√	√	√	√

10. Ce reprezintă DeepGuard?

DeepGuard monitorizează aplicațiile pentru a detecta modificări potențial dăunătoare ale sistemului de operare Windows. DeepGuard se asigură că utilizați numai aplicații sigure. Siguranța unei aplicații este verificată de F-

Secure prin serviciul Cloud Security. Dacă siguranța unei aplicații nu poate fi verificată, DeepGuard începe să monitorizeze comportamentul aplicației.

DeepGuard blochează troienii, viermii, programele exploit şi alte aplicații dăunătoare, noi sau nerecunoscute, care încearcă să facă modificări pe computer şi împiedică aplicațiile suspecte să acceseze Internetul.

Modificările potențial dăunătoare pe care DeepGuard le detectează includ:

- ✓ modificări de setare a sistemului (Windows registry)
- ✓ încercări de dezactivare a programelor de sistem importante, de exemplu a programelor de securitate
- ✓ încercări de editare a fişierelor de sistem importante

Pentru a vă asigura că DeepGuard este activ:

- Pe pagina Antivirus, selectați „Setări”
- Selectați „Viruşi şi amenințări”
- Selectați „Editare setări” Notă: Pentru a modifica setările, aveți nevoie de drepturi de administrator
- Activați „DeepGuard”

11. Ce este un program ransomware?

Un program ransomware este un software dăunător care criptează fişiere importante de pe computerul dumneavoastră, împiedicându-vă să le accesați. Infractorii cer o răscumpărare pentru a vă restabili fişierele, dar nu există nicio garanție că vă veți recăpăta vreodată datele personale, chiar dacă alegeți să plătiți.

12. Ce este un program backdoor?

Programele backdoor sunt funcții sau programe care pot fi utilizate pentru a eluda caracteristicile de securitate ale unui program, dispozitiv, portal sau serviciu.

O caracteristică dintr-un program, dispozitiv, portal sau serviciu poate fi considerată un program backdoor, în cazul în care concepția sau implementarea acesteia introduc un risc în privința securității. De exemplu, un acces pentru administrator, implementat prin cod (HTML, PHP etc.) la un portal online, poate fi utilizat ca program de tip backdoor.

De obicei, programele backdoor profită de lacunele din codul unui program, dispozitiv, portal sau serviciu. Lacunele pot fi erori de programare, vulnerabilități sau caracteristici care nu au fost documentate.

Atacatorii utilizează programe backdoor pentru a obține acces neautorizat sau pentru a efectua acțiuni dăunătoare, care să le permită să eludeze caracteristicile de securitate cum sunt restricționările accesului, autentificarea sau criptarea.

13. Ce sunt programele de tip exploit?

Rutinele de tip exploit sunt obiecte (de ex: un program elaborat special, o secvență de cod sau un şir de caractere) sau metode (de ex: o secvență specifică de comenzi) care profită de o lacună dintr-un program pentru a face ca acesta să se comporte într-un mod neprevăzut. Făcând acest lucru, se creează condițiile ca un atacator să poată efectua alte acțiuni dăunătoare.

O rutină de tip exploit este utilizată pentru a profita de o lacună sau breşă (vulnerabilitate) într-un program. Deoarece fiecare program este diferit, fiecare rutină de tip exploit trebuie să fie creată cu grijă, anume pentru acel program. Există mai multe modalități prin care un atacator poate livra o rutină de tip exploit, reuşind să fie în postura de a afecta un computer sau un dispozitiv:

- **Înglobarea într-un program piratat sau elaborat special** - când instalați şi lansați programul, se lansează şi rutina de tip exploit

- **Înglobarea într-un document ataşat la un mesaj de e-mail** - când deschideți fiș ierele ataș ate, se lansează şi rutina de tip exploit
- **Găzduirea pe un site Web piratat sau dăunător** - atunci când vizitați site-ul, se lansează şi rutina de tip exploit

Lansarea rutinei de tip exploit face ca programul să se comporte într-un mod neprevăzut, cum ar fi producerea unei erori fatale sau împiedicând accesul la spațiul de stocare şi la memoria sistemului. Acest fapt creează condițiile care permit unui atacator să efectueze şi alte acțiuni dăunătoare, cum ar fi furtul unor date sau câştigarea accesului la secțiuni restricționate ale sistemului de operare

14. Ce este un vierme?

Un vierme este un program care trimite propriile copii de la un dispozitiv la altul în cadrul unei rețele. De asemenea, unii viermi efectuează acțiuni dăunătoare pe un dispozitiv afectat.

Mulți viermi sunt concepuți să fie atractivi pentru utilizator. Ei pot lua forma unor imagini, clipuri video, aplicații sau orice alt tip de program sau fişier util. Obiectivul acțiunii frauduloase este să păcălească utilizatorul să instaleze viermele. Alți viermi sunt concepuți să fie total invizibili, întrucât ei exploatează lacunele dispozitivului (sau ale programelor instalate pe el) pentru a se instala singuri, fără a fi vreodată remarcați de către utilizator.

Odată instalat, viermele utilizează resursele fizice ale dispozitivului pentru a-şi crea copii şi pentru a trimite apoi acele copii către alte dispozitive la care poate ajunge într-o rețea. Dacă urmează să fie trimis un volum mare de copii ale viermelui, performanțele dispozitivului pot avea de suferit. Dacă sunt afectate mai multe dispozitive dintr-o rețea şi acestea trimit copii ale viermelui, rețeaua însăşi poate deveni nefuncțională. De asemenea, unii viermi pot face mai multe daune directe unui dispozitiv afectat, cum ar fi modificarea fişierelor stocate pe acesta, instalarea altor aplicații dăunătoare sau furtul de date.

Majoritatea viermilor se răspândesc numai pe un anumit tip de rețea. Unii viermi se pot răspândi pe două sau mai multe tipuri, cu toate că aceştia sunt relativ rari. De obicei, viermii vor încerca şi se vor răspândi pe una dintre următoarele rețele (deşi există şi cei care vizează canale mai puțin populare):

- Rețele locale
- Site-uri de socializare
- Conexiuni punct la punct (P2P)
- Mesaje SMS sau MMS

15. Ce este un cal troian („trojan”)?

Caii troieni sunt programe care oferă sau aparent oferă o funcție sau o caracteristică atractivă, dar apoi efectuează în tăcere acțiuni dăunătoare în fundal. Denumiți după legenda calului troian din Grecia, caii troieni sunt concepuți să pară atractivi pentru un utilizator. Ei pot lua aspectul unor jocuri, economizoare de ecran, actualizări de aplicații sau orice alt program sau fişier util. Unii cai troieni vor mima sau chiar vor copia programe populare sau bine cunoscute, pentru a părea mai convingători. Obiectivul acțiunii frauduloase este să păcălească utilizatorul să instaleze calul troian.

Odată instalați, caii troieni pot utiliza şi „capcane” pentru a menține iluzia că ei sunt legitimi. De exemplu, un cal troian deghizat într-o aplicație de economizor de ecran sau un fişier de tip document, va afişa o imagine sau un document. În timp ce utilizatorul este distras de aceste capcane, calul troian poate efectua pe tăcute alte acțiuni în fundal. De obicei, caii troieni fie vor efectua modificări dăunătoare asupra dispozitivului (cum ar fi ştergerea sau criptarea fişierelor ori modificarea setărilor programului), fie vor fura date confidențiale stocate pe acesta. Caii troieni se pot grupa după acțiunile pe care aceştia le efectuează:

- **Program de descărcare de tip cal troian**: se conectează la un site aflat la distanță, pentru a descărca şi instala alte programe

- **Program de instalare cai troieni**: conține unul sau mai multe programe în plus, pe care acesta le instalează
- **Hoț de parole de tip cal troian**: fură parolele stocate pe dispozitiv sau introduse într-un browser Web
- **Cal troian pentru operațiuni bancare**: un tip de cal troian specializat în furtul de parole, care caută în special nume de utilizator şi parole pentru portalurile de operațiuni bancare online
- **Spion de tip cal troian**: monitorizează activitatea pe dispozitiv şi redirecționează detaliile către un site aflat la distanță

Întrebări & răspunsuri utilizare aplicaț ie Vodafone Smart ID Protection

1. Ce se întâmplă atunci când adaug un nou element monitorizat?

Vodafone Smart ID Protection va verifica imediat încălcările existente ale securităț ii, pentru a vedea dacă adresa dumneavoastră de e-mail este menț ionată în oricare dintre ele. Nu este un lucru neobiș nuit ca timp de ani de zile să lucraț i fără să ș tiț i că datele dumneavoastră au fost piratate. De asemenea, F-Secure va începe să monitorizeze pe Web pentru a găsi orice menț ionări ale adresei de e-mail pe care aț i adăugat-o. Dacă adresa de e-mail apare într-o violare a securităț ii datelor, veț i fi anunț at ș i aceste încălcări vor fi afiș ate în lista din fila Monitorizare.

2. Ce înseamnă încălcarea securităț ii datelor?

O încălcare a securităț ii datelor are loc atunci când infractorii pătrund într-o companie sau serviciu ș i fură informaț iile private ale clienț ilor sau utilizatorilor acestora. Acestea pot merge de la informaț ii personale identificabile cum ar fi nume, numere ș i adrese de mail, până la informaț ii dăunătoare în mod direct cum sunt numerele cardurilor de credit.

3. Cum aflaț i de încălcările privind securitatea datelor?

F-Secure utilizeaza o combinaț ie de metode manuale ș i automate. Caută constant atât pe Web-ul normal cât ș i pe Dark Web, pentru a găsi menț ionări ale adresei dumneavoastră de e-mail personale, dar utilizează ș i expertiza F-Secure în domeniu pentru a accesa în mod legal liste cu date la care s-a încălcat securitatea, deseori înainte ca acestea să devină publice.

4. Cum puteț i găsi toate aceste informaț ii doar cu o adresă de e-mail?

În majoritatea cazurilor, o adresă de e-mail este utilizată pentru a crea un cont online ș i ca nume de utilizator pentru a vă conecta. Din acest motiv, o adresă de e-mail este aproape întotdeauna parte a unei încălcări a securităț ii datelor. Atunci când găsim adresa de e-mail, găsim ș i informaț iile ataș ate acesteia.

5. Ce ar trebui să fac în cazul în care informaț iile mele private au fost expuse?

Aplicaț ia Vodafone Smart ID Protection vă va oferi întotdeauna o listă cu acț iunile recomandate, care diferă în funcț ie de gravitatea încălcării securităț ii datelor ș i de informaț iile care au fost sparte. Găsiț i aceste acț iuni recomandate, dând click pe respectiva încălcare a securităț ii datelor.

6. Care sunt nivelurile de gravitate la încălcarea securităț ii datelor?

Încălcările securităț ii datelor sunt clasificate în funcț ie de gravitate, pe baza gradului de periculozitate adatelor expuse. Cele trei niveluri de gravitate sunt:

GRAVITATE RIDICATĂ

Încălcările de gravitate ridicată implică una dintre următoarele componente de informaț ii personale:

- Parolă în format uș or de citit (text simplu)
- Informaț ii despre cardul de credit
- Numărul paș aportului
- Numărul de asigurare socială

GRAVITATE MEDIE

Încălcările de gravitate medie implică una dintre următoarele componente de informaț ii personale:

- Numărul contului bancar
- Detalii despre paș aport, altele decât numărul acestuia
- Tipul cardului de credit
- Parolă într-un format amestecat (combinat)
- Mai multe tipuri de informaț ii expuse împreună (nume de utilizator, nume complet, data naș terii)

GRAVITATE SCĂZUTĂ

Încălcările de securitate cu gravitate scăzută implică una dintre următoarele componente de informaț ii personale:

- Nume de utilizator
- Nume complet
- Data naș terii
- Număr de telefon
- Adresă

7. Care sunt informaț iile mele de contact din aplicaț ia Vodafone Smart ID Protection?

Aceasta este adresa de e-mail la care se vor trimite notificările, atunci când informaț iile dumneavoastră apar într-o încălcare a securităț ii datelor. Prima adresă de e-mail pe care o adăugaț i la elementele monitorizate devine automat adresa dumneavoastră de contact. Puteț i modifica informaț iile dumneavoastră de contact în setări.

8. Alegerea parolei principale

Alegeț i-vă cu grijă Parola principală. Dacă o uitaț i, nu vă mai puteț i reseta parola principală.

Pentru a creș te securitatea, alegeț i o parolă puternică

- Includeț i atât litere mici, cât ș i MARI
- Includeț i cifre (1,2,3 etc) ș i caractere speciale (. , ! ; ,@ , * ,#)
- Evitaț i cuvinte obiș nuite

- Evitați secvențe de cifre (12345...) și litere (abcd, qwerty....)

Pentru a vă asigura securitatea, aplicația Vodafone Smart ID Protection nu va accepta o parolă principală slabă.

Dacă selectați „Să mi se memoreze parola principală pe acest dispozitiv", Vodafone Smart ID Protection nu vă va mai solicita parola principală pe respectivul dispozitiv , în afara cazului în care vă deconectați din meniu.

9. Cum se crează un cod de recuperare pentru parola principală?

Codul de recuperare pentru parola principală este un cod unic și personal, care reprezintă singura modalitate de a recâștiga accesul la Vodafone Smart ID Protection, în situația în care uitați parola principală.

Pentru siguranță, Smart ID Protection nu poate reseta parola principală, nici nu vă poate trimite un cod de recuperare atunci când uitați parola principală. De fiecare dată când modificați parola principală, Smart ID Protection afișează creare cod de recuperare. Vă recomandăm să salvați codul ca imagine și să imprimați o copie pe care să o păstrați în siguranță. Notă: Când modificați parola principală, veți primi un nou Cod de recuperare. Întotdeauna aveți nevoie de cel mai recent cod de recuperare pentru a recâștiga accesul la Smart ID Protection, atunci când uitați parola principală.

10. Utilizarea unui cod de recuperare pentru parola principală

Codul de recuperare pentru parola principală este un cod unic și personal, care reprezintă singura modalitate de a obține accesul la Smart ID Protection, în situația în care uitați parola principală.

Când începeți să utilizați Smart ID Protection și de fiecare dată când modificați parola principală, Smart ID Protection afișează opțiunea de creare cod de recuperare. Trebuie să salvați imaginea care conține codul.

O imagine salvată sau imprimată care conține codul, poate fi utilizată pentru a obține accesul la Smart ID Protection, atunci când uitați parola principală.

- ✓ În ecranul de conectare la Smart ID Protection selectați „Ați uitat parola principală?"
- ✓ Puteți să importați din dispozitivul dumneavoastră o imagine salvată a codului de recuperare sau să faceți o fotografie după un cod imprimat (valabil numai pentru smartphone si iphone)
- ✓ Dacă este corect codul, veți vedea parola principală și Smart ID Protection vă va conecta automat.

Notă: nu uitați să creați un alt cod de recuperare atunci când modificați parola principală.

11. Cum să rămâneți online în siguranță ?

Pentru a rămâne online în siguranță este recomandat să:

- ✓ Utilizați o parolă unică pentru fiecare serviciu online
- ✓ Utilizați o parolă puternică suficient de lungă și care conține litere mari și mici, cifre și caractere speciale
- ✓ Modificați regulat parolele, mai ales atunci când există o șansă ca parola dumneavoastră să fi fost compromisă

12. Conectarea dispozitivelor

Conectați dispozitivele pentru a vă vizualiza și gestiona parolele pe toate dispozitivele dumneavoastră. Prin conectare, parolele de pe toate dispozitivele se îmbină într-o singură listă și devin disponibile pe toate dispozitivele. Preferințele sunt specifice dispozitivului. Puteți alege separat preferințele pentru fiecare dispozitiv.

Vedeț i codul dumneavoastră de conectare scris cu galben. Deschideț i Smart ID Protection pe dispozitivul cu care doriț i să vă conectaț i, găsiț i ,,Conectare dispozitive", ș i introduceț i codul de la primul dispozitiv.

Important: Prin conectarea dispozitivelor se modifică parola principală pentru Smart ID Protection pe dispozitivele conectate. După conectare, toate dispozitivele vor avea aceeaș i parolă principală ca ș i dispozitivul care a furnizat codul de conectare.