Internet zaštita

za Mac

Jedan za sve.

Sadržaj

1 Uvod u aplikaciju A1 Sigurniji internet 6
1.1 Sistemski preduvjeti 7
1.2 Gdje mogu kupiti A1 Sigurniji internet? 7
2 Početak rada 8
2.1 Instalacija proizvoda na vaš prvi uređaj 8
2.1.1 Deinstaliranje proizvoda 9
2.2 Prikaz podataka o vašem računu 10
2.3 Obavijesti o potrebnim i preporučenim zadacima 10
2.4 Upravljanje postavkama proizvoda 11
2.5 Prikaz statusa vašeg proizvoda 12
2.5.1 Ikone stanja zaštite 12
2.5.2 Prikaz nedavnih događaja za proizvod 12
2.5.3 Prikaz najnovijih ažuriranja 13
2.6 Odjava iz aplikacije 13
3 Osobe i uređaji 14
3.1 Zaštita vlastitih uređaja 14
3.2 Ograničavanje internetskog sadržaja za djecu 15
3.2.1 Postavljanje filtriranja sadržaja za dijete 15
3.2.2 Kategorije sadržaja 16
3.3 Dijeljenje zaštite s članom obitelji ili prijateljem 18
3.3.1 Jeste li dobili poziv da zaštitite svoje uređaje? 19
3.3.2 Prestanite dijeliti zaštitu s članom obitelji ili prijateljem 19
3.4 Oslobađanje licence s uređaja 20
3.5 Premještanje aplikacije A1 Sigurniji internet sa vašeg starog uređaja na novi 21
4 Zaštita uređaja 22
4.1 Korištenje automatskog skeniranja 22

4.1.1 Kako funkcionira automatsko skeniranje 22
4.1.2 Privremeno isključivanje automatskog traženja 23
4.2 Pokretanje pregledavanja zlonamjernog softvera 24
4.3 Izuzimanje datoteka ili mapa iz skeniranja 24
4.4 Što je DeepGuard? 25
4.4.1 Odabir razine zaštite rješenja DeepGuard 26
4.4.2 Optimizacija rješenja DeepGuard za vaš sustav 26
4.4.3 Omogućivanje aplikacija koje je DeepGuard blokirao 27
4.5 Što radi štetan sadržaj 28
4.5.1 Potencijalno neželjene aplikacije (PUA, Potentially unwanted applications) i neželjene aplikacije (UA, Unwanted applications) 28
4.5.2 Crvi 28
4.5.3 Trojanci 29
4.5.4 Programi za neovlašten ulazak u sustav 30
4.5.5 Kodovi koji se koriste slabim točkama 30
4.5.6 Paketi kodova koji se koriste slabim točkama 31
4.6 Slanje uzorka 31
5 Zaštita od prijevara 32
5.1 Ikone ocjene ugleda u rezultatima pretraživanja 32
5.2 Blokiranje štetnih web-mjesta 33
5.2.1 Dopuštanje blokiranih web-mjesta 33
5.2.2 Ručno dopuštanje blokiranih web-mjesta 34
5.3 Uključivanje zaštite bankarstva 34
5.4 Sigurna online kupnja 35
5.5 Blokiranje oglasa na web-mjestima 36
5.6 Odbijanje nepotrebnih kolačića 36
5.7 Provjera koriste li se proširenja preglednika 37
5.7.1 Instaliranje i omogućavanje proširenja preglednika za Safari 37
5.7.2 Instaliranje i omogućavanje proširenja preglednika za Chrome 38

5.7.3 Instaliranje i omogućavanje proširenja preglednika za Firefox 38
5.7.4 Instaliranje i omogućavanje proširenja preglednika za Edge 39
6 Spremište za lozinke 40
6.1 Početak rada sa Spremištem za lozinke 40
6.2 Korištenje trezora lozinki.....41
6.2.1 Prijava na internetsku uslugu sa Spremištem za lozinku 41
6.2.2 Pohranjivanje nove lozinke u Spremište za lozinke 43
6.2.3 Pohranjivanje podataka vaše platne kartice u Spremište za lozinke...44
6.2.4 Uređivanje postojećih podataka.....44
6.2.5 Brisanje unosa.....45
6.2.6 Dopuštanje aplikaciji da generira novu lozinku za postojeći unos.....45
6.2.7 Pristup vašim starim lozinkama 46
6.2.8 Provjerite jesu li vaše lozinke jake.....46
6.3 Povezivanje uređaja za sinkronizaciju vaših podataka iz Spremišta za lozinke na svim vašim uređajima 47
6.4 Postavljanje automatske ispune za brži pristup uslugama na mreži 48
6.5 Uvoz lozinki iz drugih upravitelja lozinki.....49
6.6 Izvoz podataka iz trezora lozinki.....50
6.7 Promjena glavne lozinke.....51
6.8 Stvaranje QR koda za oporavak za glavnu lozinku 51
6.9 Upotreba QR koda za oporavak u svrhu oporavka vaše zaboravljene glavne lozinke 52
6.10 Otključavanje i zaključavanje Spremišta za lozinke 53
7 Nadzor ID-a 54
7.1 Dodavanje stavki za praćenje 54
7.2 Brisanje nadziranih stavki.....55
7.3 Promjena adrese e-pošte za kontakt 56
8 Zaštita privatnosti 57
8.1 Sigurnosni podaci 57

8.2 Poboljšanje proizvoda 58
9 Tehnička podrška 59
9.1 Gdje pronaći ID računa? 59
9.2 Gdje mogu pronaći informacije o verziji proizvoda? 59
9.3 Korištenje alata za podršku 59
9.4 Problemi otklanjanja pogrešaka proizvoda 60
9.5 Ponovno postavljanje predmemorije reputacije 61
9.6 Telefonske prijevare i što učiniti ako mislite da ste meta 62

1 Uvod u aplikaciju A1 Sigurniji internet

Aplikacija A1 Sigurniji internet pokriva sve vaše potrebe za sigurnošću i zaštitom privatnosti.

Aplikacija A1 Sigurniji internet uključuje sve zaštitne značajke koje su vam potrebne u samo jednoj aplikaciji.

Izrađena je na temelju nagrađivane tehnologije zaštite od virusa tvrtke F-Secure.

Ovaj korisnički priručnik odnosi se na sljedeće pretplate na A1 Sigurniji internet:

- A1 Sigurniji internet

A1 Sigurniji internet pruža vam sveobuhvatnu zaštitu kako za sigurnost vaših uređaja, tako i za vašu privatnost. Također vam pomaže u izbjegavanju krađe identiteta. Kako danas sve više i više podataka o privatnom životu dijelimo na internetu, ne samo da moramo zaštititi svoje uređaje, već i svoje osobne podatke.

Internet je važan dio našeg svakodnevnog života. Želimo ostati povezani sa svojim voljenima, obavljati bankarstvo, kupovati na mreži i pretraživati informacije na internetu postavljajući pitanja tražilicama.

Uz količinu osobnih podataka s kojima svakodnevno upravljamo na svojim pametnim telefonima, tabletima i računalima, važno je da svi naši uređaji ostanu zaštićeni, naši podaci privatni, a naši osobni podaci sigurni.

Uz A1 Sigurniji internet možete:

- Zaštititi sebe i cijelu svoju obitelj i prijatelje na mreži
- Zaštititi svoje pregledavanje, internetsko bankarstvo i kupovinu
- Zaštititi vezu s bežičnim mrežama
- Zaštititi sebe i svoje uređaje od zlonamjernog softvera i drugih prijetnji na mreži

1.1 Sistemski preduvjeti

Ova tema navodi verzije operacijskog sustava koje podržava aplikacija A1 Sigurniji internet.

Aplikacija A1 Sigurniji internet podržava sljedeće operacijske sustave:

Za računala sa sustavom Windows:

- Windows 11
- Verzija 21H2 sustava Windows 10 s najnovijim instaliranim ažuriranjima (sva 64-bitna izdanja; 32-bitna izdanja nisu podržana)
- Windows 11 na ARM64 verziji 24H2 ili novijoj

Za Mac računala:

- macOS 26 (Tahoe)
- macOS 15 (Sequoia)
- macOS 14 (Sonoma)
- macOS 13 (Ventura)
- Podržani su procesori Intel i Apple Silicon

Za pametne telefone i tablete:

- Android 11.0 ili novija verzija
- iOS 18.0 ili noviji

Bilješka: Proizvod podržava širok raspon Android uređaja, uključujući punu podršku za Samsung uređaje. Međutim, zbog raznolikosti hardverskih i softverskih konfiguracija među proizvođačima, neki uređaji mogu imati ograničenu funkcionalnost. Chromebook i Doro uređaji trenutno nisu podržani.

1.2 Gdje mogu kupiti A1 Sigurniji internet?

A1 Sigurniji internet možete kupiti na svim A1 prodajnim mjestima, kao i preko Moj A1 aplikacije i portala te pozivom u Službu za korisnike na 0800 091 091.

2 Početak rada

Ovaj odjeljak opisuje kako instalirati proizvod na vaš prvi uređaj, kako pristupiti alatima i značajkama proizvoda te kako promijeniti postavke proizvoda.

2.1 Instalacija proizvoda na vaš prvi uređaj

Nakon što aktivirate svoj račun za A1 Sigurniji internet, možete preuzeti i instalirati proizvod na svoj prvi uređaj putem poruke za dovršetak registracije koja će Vam biti poslana.

Instalaciju možete napraviti i direktno putem App Storea, a za dovršetak registracije potrebno je pričekati poruku koju će Vam poslati A1.

Ako ste koristili stariju verziju aplikacije (A1 Internet zaštita), ne morate deinstalirati prijašnju verziju, ali morate istu osvježiti preko App Storea te nakon toga ponovno postaviti postavke aplikacije.

Da biste instalirali proizvod na svoj mobilni uređaj:

Instaliraj iz trgovine aplikacija da biste pristupili trgovini aplikacija i pokrenuli instalaciju.

Da biste instalirali proizvod na nekom drugom uređaju, učinite sljedeće:

a) U aplikaciji pod Osobe i Uređaji odaberite Dodaj uređaj, vrstu uređaja koji želite dodati (Moj uređaj, Uređaj mog djeteta, Uređaj neke druge osobe), a zatim **Nastavi**.
b) Unesite Ime i Prezime osobe te potom i **Pozovi putem SMS poruke** i unesite telefonski broj uređaja.
Ako uređaj nema telefonski broj, odaberite **Pozovi putem poruke e-pošte** i unesite adresu e-pošte uređaja.
c) Odaberite **Pošalji pozivnicu**.
d) Odaberite **Ovo računalo** da biste instalirali proizvod na svoj trenutačni uređaj. Pratite upute za instalaciju poslane na uređaj.

5. Pokrenite preuzeti instalacijski paket. Otvara se stranica za postavljanje proizvoda A1 Sigurniji internet.
Proizvod automatski otkriva unaprijed odabrani jezik koji se koristi na računalu te u proizvodu Kada instalacija završi, otvorite aplikaciju.

6. Proizvod automatski otkriva unaprijed odabrani jezik koji se koristi na računalu te u proizvodu postavlja isti taj jezik. Ako želite promijeniti jezik proizvoda, odaberite jezik s padajućeg izbornika u gornjem lijevom kutu stranice za postavljanje.
Ako naknadno želite promijeniti jezik proizvoda, morat ćete iznova instalirati proizvod te odabrati željeni jezik tijekom postavljanja.

7. Pročitajte uvjete licence za krajnjeg korisnika te, ako se s njima slažete, odaberite **Prihvaćam i nastavi**. Dok instalacijski paket instalira proizvod na uređaj slijedite upute prikazane na zaslonu.
Kad se instalacija završi, može proći nekoliko minuta prije nego što proizvod primi najnovija ažuriranja. Svoj status zaštite možete vidjeti na glavnoj stranici proizvoda.

8. Proizvod zahtijeva puni pristup disku da bi mogao otkriti i blokirati prijetnje na osjetljivim lokacijama vašeg računala Mac.
Da biste omogućili puni pristup disku:
a. Na računalu Mac idite na **Postavke sustava** > **Privatnost i sigurnost** > **Privatnost**.
b. Odaberite **Potpuni pristup disku**.
c. Da biste mogli promijeniti postavke zaštite privatnosti, kliknite ikonu lokota u donjem lijevom kutu prozora i s popisa odaberite aplikaciju **A1 Sigurniji internet**.
d. Da bi nove postavke stupile na snagu, najprije morate zatvoriti proizvod A1 Sigurniji internet. Odaberite **Zatvori odmah**.

9. Proizvod vas obavještava ako proširenje vašeg preglednika još nije u upotrebi. Da biste dodali proširenje preglednika, odaberite **Postavi** na obavijesti prikazanoj na glavnoj stranici proizvoda i pratite upute na zaslonu.

Bilješka: Ako ne vidite obavijest o proširenju za preglednik, proširenje je već u upotrebi.

Ako ste prilikom instaliranja aplikacije koristili pogrešan profil i želite se prebaciti na drugi:

1. Na glavnom prikazu odaberite  u gornjem desnom kutu, a zatim odaberite **Promijeni korisnika**.

2. Prijavite se u svoj račun za A1 Sigurniji internet.

3. Odaberite profil koji želite koristiti, a zatim odaberite **Nastavi**.

2.1.1 Deinstaliranje proizvoda

Proizvod se ne može deinstalirati premještanjem aplikacije u smeće. Morate upotrijebiti program za deinstalaciju proizvoda da biste ga uklonili s računala.

Da biste deinstalirali proizvod, morate imati prava za administraciju računala.

Slijedite ove upute:

1. Otvorite mapu u koju ste instalirali proizvod. Proizvod se prema zadanim postavkama nalazi u mapi Aplikacije.

2. Dvaput kliknite ikonu proizvoda Deinstaliraj.
Otvorit će se deinstalacijski program.

3. Odaberite **Deinstaliraj**.
Da biste mogli deinstalirati proizvod, morate unijeti administratorsku lozinku.

4. Unesite svoje administratorsko korisničko ime i lozinku te odaberite **U redu**.

Bilješka: Nakon unosa vjerodajnica deinstalacija može malo potrajati.

Proizvod je uklonjen s vašeg računala. Kada deinstalirate proizvod sa svog računala, ne zaboravite također poništiti njegovu licencu u aplikaciji A1 Sigurniji internet. Tek tada možete ponovno upotrebljavati izdanu licencu na drugom računalu.

2.2 Prikaz podataka o vašem računu

Svoj status pretplate, podatke o računu i trenutačni naziv uređaja možete jednostavno pronaći na glavnoj stranici proizvoda.

Ako želite provjeriti pojedinosti svojeg računa, kao što je ime vlasnika računa, adresa e-pošte koja se upotrebljava za prijavu na račun i naziv uređaja koji trenutačno upotrebljavate, učinite sljedeće:

1. Otvorite aplikaciju A1 Sigurniji internet.
Možete vidjeti koga proizvod štiti u gornjem desnom kutu glavne stranice proizvoda.

2. Odaberite ikonu profila  .
Ovdje će se prikazati Vaše Ime i prezime te broj/e-mail uz koji je usluga vezana.

Za podatke o iskorištenim licencama:
1. Odaberite ikonu profila u gornjem desnom kutu zaslona.
2. Pod stavkom Račun odaberite Pretplata.

Za podešavanje funkcionalnosti koje se koriste:
1. U gornjem desnom kutu portala odaberite glavni izbornik , a zatim odaberite **Postavke** iz kontekstnog izbornika. Otvara se prikaz **Postavke računa**.
2. Ako promijenite postavke, odaberite **Spremi**.

2.3 Obavijesti o potrebnim i preporučenim zadacima

Putem zadataka obavještavamo vas kad god postoji potreba za vašom pažnjom u aplikaciji A1 Sigurniji internet.

Aplikacija vam prikazuje zadatke koje morate izvršiti da biste održali potpunu zaštitu. Dok neki zadaci zahtijevaju brzu radnju, drugi vam omogućuju dodatno vrijeme za razmišljanje o zadatku prije nego što ga dovršite.

U glavnom prikazu aplikacija prikazuje zadatke koje je pokrenula aplikacija na temelju trenutačnog statusa. Prioriteti su raspoređeni prema težini zadatka.

Možete pristupiti svim zadacima na čekanju i odbačenim zadacima iz glavnog prikaza aplikacije tako da odaberete  u gornjem desnom kutu.

Aplikacija pruža zadatke u sljedećim kategorijama:

Vrsta zadatka	Opis
Kritično	Kritičan zadatak označava pojavu greške koja zahtijeva hitno rješavanje, ne ostavljajući mjesta za kašnjenje ili propust.
Potrebna radnja	Ova vrsta zadatka zahtijeva rješavanje, ali ga imate opciju odgoditi ili, u određenim situacijama, čak i zaobići.
Prijedlog	Ova vrsta zadatka može istaknuti značajku koja ne utječe uvelike na pruženu zaštitu, ali služi kao vrijedan dodatak za korisnika. Ova određena vrsta zadatka možda se neće automatski prikazati u glavnom prikazu aplikacije. To je, međutim, vidljivo na opsežnom popisu zadataka dostupnih na kartici Svi zadaci.
Uvođenje / uvodne napomene	Ova kategorija zadataka pruža vam kratki uvod u novu značajku i pomaže vam razumjeti njezine prednosti. Zadatak vam pruža jednostavan način početka upotrebe značajke.

2.4 Upravljanje postavkama proizvoda

Možete upravljati ponašanjem proizvoda putem postavki proizvoda.

Možete brzo pristupiti postavkama proizvoda putem ikone proizvoda na traci izbornika.

Kada instalirate proizvod na svoj uređaj, sve osnovne značajke zaštite automatski se uključuju i sve su postavke proizvoda podešene tako da vaš uređaj bude u potpunosti zaštićen.

Međutim, ako želite, možete napraviti vlastite prilagodbe postavki.

Za promjenu nekih postavki proizvoda potrebna su vam administratorska prava.

2.5 Prikaz statusa vašeg proizvoda

Postoje različiti načini na koje možete provjeriti radi li sve kako je predviđeno u proizvodu i jesu li vaš uređaj i pregledavanje mreže zaštićeni.

2.5.1 Ikone stanja zaštite

Ikone stanja zaštite prikazuju vam ukupno stanje proizvoda i njegovih značajki.

Ikone stanja zaštite:

Ikona stanja	Naziv stanja	Opis
	**U redu**	Vaš je uređaj zaštićen. Značajke su uključene i pravilno funkcioniraju.
	**Upozorenje**	Vaš uređaj nije u potpunosti zaštićen. Proizvod traži vašu pažnju, na primjer zato što dugo nije ažuriran ili je neka sigurnosna značajka isključena.
	**Opasnost**	Vaš uređaj nije zaštićen. Ovaj proizvod zahtijeva trenutačnu akciju, na primjer zato što je kritična značajka onemogućena ili je pretplata istekla.

Primjeri poruka o stanju koje biste mogli vidjeti:

- **Ne koristi se proširenje za preglednik Google Chrome**
- **Ne koristi se proširenje za preglednik Mozilla Firefox**
- **Proširenje preglednika Safari nije u upotrebi**
- **Pretplata je istekla**

2.5.2 Prikaz nedavnih događaja za proizvod

Možete vidjeti što je proizvod učinio i kako je zaštitio vaše računalo na stranici **Zaraze**.

Izvješće o zarazi prikazuje različite događaje za instalirani proizvod i detalje zaštitnih mjera koje je proizvod poduzeo. Na primjer, prikazuje vam sve štetne stavke koje su otkrivene i izbrisane.

Da biste prikazali cijelu povijest događaja za proizvod:

1. Odaberite ikonu proizvoda na traci izbornika.

2. Odaberite **Izvješće o zarazi**.
Ovo otvara prikaz **Zaraze** koji vam pokazuje vrijeme i opis svakog događaja, kao i radnje koje su poduzete.

2.5.3 Prikaz najnovijih ažuriranja

Proizvod automatski dohvaća najnovija ažuriranja na vaše računalo kada ste spojeni na internet.

Da biste vidjeli detalje o najnovijim ažuriranjima za instalirani proizvod:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu odaberite gornji lijevi gumb izbornika .

3. Odaberite **Postavke**.

4. U odjeljku **Postavke** odaberite **Ažuriranja**.

U ovom prikazu možete vidjeti vrijeme posljednje provjere ažuriranja i njegov status.

5. Da biste ručno potražili najnovija ažuriranja, odaberite **Provjeri odmah**.
Ova provjera također nadograđuje najnoviju verziju sigurnosnog proizvoda na vaš uređaj ako je izdana, ali još nije instalirana na vašem uređaju.

U odjeljku **Povijest ažuriranja** možete vidjeti najnovija instalirana ažuriranja. Imajte na umu da paket ažuriranja s najvećim brojem verzije nije nužno najnovije ažuriranje koje je preuzeto.

2.6 Odjava iz aplikacije

Ako imate drugu pretplatu na ovu aplikaciju s drugačijim korisničkim imenom, kako biste mogli početi upotrebljavati njezinu licencu na ovom uređaju, prvo se morate odjaviti iz aplikacije.

Upozorenje: Kada se odjavite iz aplikacije, također će se zaustaviti zaštita svih korisnika na uređaju.

Sve postavke Pravila za obitelj, ako su postavljene, prestat će raditi. Također, više nećete moći pristupiti svojim podacima Spremišta za lozinke.

Za odjavu iz aplikacije:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu odaberite u gornjem desnom kutu, a zatim odaberite **Odjavi se**.

Bilješka: Za odjavu iz aplikacije potrebna su vam administratorska prava.

Kada se odjavite iz aplikacije na svom uređaju, ne zaboravite također osloboditi njezinu licencu s mrežnog portala za upravljanje. Tek tada možete ponovno upotrebljavati izdanu licencu na drugom uređaju.

3 Osobe i uređaji

Ovaj odjeljak pruža informacije o tome kako koristiti proizvod za zaštitu vlastitih uređaja, kao i uređaja svoje obitelji i prijatelja.

Nakon što ste izradili svoj A1 Sigurniji internet račun i zaštitili svoj prvi uređaj, možete nastaviti sa zaštitom svojih uređaja putem instaliranog sigurnosnog proizvoda.

Prikaz **Osobe i uređaji** vam daje pregled osoba i njihovih uređaja koje ste vi, kao vlasnik pretplate, zaštitili svojom pretplatom. Da biste vidjeli detaljne informacije o korisniku, samo odaberite korisnika i otvorit će se prikaz specifičan za korisnika koji vam daje pregled zaštite korisnika.

U prikazu **Osobe i uređaji** možete dodati više korisnika i uređaja u svoju grupu slanjem poveznice za instalaciju proizvoda na korisnikov uređaj e-poštom ili SMS porukom.

Korisnici koje pozovete u svoju grupu imat će vlastiti korisnički račun. Svim dječjim profilima upravlja se pomoću vašeg računa.

Bilješka: Alternativno, možete upotrebljavati portal za upravljanje na mreži za upravljanje zaštitom uređaja u vašoj grupi.

3.1 Zaštita vlastitih uređaja

Ova tema opisuje kako početi štititi svoje druge uređaje.

Nakon što ste kreirali svoj My A1 Sigurniji internet račun i zaštitili svoj prvi uređaj, možete nastaviti štititi svoje ostale uređaje putem portala My A1 Sigurniji internet ili putem instalirane sigurnosne aplikacije.

Da biste počeli štititi svoje druge uređaje putem aplikacije:

1. U glavnom prikazu odaberite **Osobe i uređaji**

2. U prikazu **Osobe i uređaji** odaberite **+ Dodaj uređaj ili korisnika**.

3. Odaberi **Moj uređaj** > **Nastaviti**.

4. Odaberite kako želite dostaviti instalacijsku vezu na uređaj koji želite zaštititi, a zatim odaberite **Pošalji vezu**.

5. Otvorite poruku s uređajem koji želite zaštititi i slijedite upute za instalaciju.
Otvara se vaš web-preglednik, prema zadanim postavkama prikazuje gumb za instalaciju za vaš trenutni uređaj.

6. Preuzmite odgovarajući instalacijski paket za uređaj i pokrenite instalacijski program.

7. Nakon što se prikaže prozor za postavljanje proizvoda, odaberite **Prihvati i nastavi** ako se slažete s Uvjetima licence za krajnjeg korisnika.

8. Kada instalacija završi, prijavite se na svoj račun, ako se to od vas zatraži, i odaberite **Nastaviti** kako biste dovršili zaštitu uređaja.

Važno: Za zaštitu pregledavanja obavezno je proširenje za preglednik da bi vaše pregledavanje mreže, internetsko bankarstvo i kupovina bili zaštićeni te da bi se mogli prikazivati podaci o sigurnosti dok pregledavate internet. Stoga se uvjerite da su proširenja za preglednik u upotrebi.

Sada ste postavili zaštitu za svoj uređaj. Za pregled i upravljanje zaštitom gore navedenog uređaja idite na proizvod **Osobe i uređaji** pregledajte ili se prijavite na svoj račun kako biste pristupili mrežnom portalu za upravljanje.

3.2 Ograničavanje internetskog sadržaja za djecu

Obiteljska zaštita omogućava vam da djeci ograničite pristup neprimjerenom sadržaju da biste ih zaštitili od izlaganja neželjenom materijalu na internetu.

Bilješka: Ta značajka nije dostupna u svim verzijama aplikacije.

Internet je pun zanimljivih web-mjesta, no neka su od njih neželjenog ili neprimjerenog sadržaja, posebice za djecu. Filtriranje sadržaja omogućava vam da ograničenjem pristupa određenim web stranicama svojoj djeci na uređajima omogućite samo primjeren sadržaj.

Bilješka: Uređivanje postavki Obiteljske zaštite zahtijeva administratorske ovlasti. Postavke možete uređivati zasebno za svaki korisnički račun na računalu.

3.2.1 Postavljanje filtriranja sadržaja za dijete

Filtriranjem sadržaja možete ograničiti vrste online sadržaja kojima vaše dijete može pristupiti.

Bilješka: Postavke filtriranja sadržaja možete urediti zasebno za svaki korisnički račun na računalu.

Za postavljanje zaštite za vaše dijete:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu odaberite **Obiteljska zaštita**.
Ovim se otvaraju postavke **Obiteljske zaštite**.

3. Odaberite ikonu zaključavanja u donjem lijevom kutu.
Za promjenu ovih postavki potrebna su vam administrativna prava.

4. Odaberite korisnički račun koji želite urediti.

5. Uključite **filtriranje sadržaja**.

6. Odaberite profil filtriranja sadržaja.
Možete odabrati **Strogo**, **Umjereno** ili **Osnovno**. Svaki profil blokira drugačiji skup vrsta sadržaja
Ako ne vidite popis vrsta sadržaja, pomaknite se prema dolje da biste vidjeli koje su blokirane.

Također možete dopustiti određene web-stranice, čak i ako bi ih filtriranje sadržaja blokiralo na temelju vrste sadržaja:
a) Odaberite **Prikaži iznimke web-mjesta**.
Ovo otvara novi prikaz koji navodi web-lokacije koje želite dopustiti.
b) Unesite adresu web-stranice koju želite dopustiti.
c) Odaberite **+**.
d) Odaberite **Gotovo** za zatvaranje prikaza.

7. Dopustite VPN konfiguracije.
Sada ste postavili filtriranje sadržaja za svoje dijete. Da biste kasnije promijenili bilo koju od ovih postavki, odaberite **Obiteljska zaštita** u glavnom prikazu aplikacije.

Važno: Zaštita pregledavanja koristi proširenja preglednika za zaštitu vašeg pregledavanja weba, online bankarstva i kupovine te za prikaz sigurnosnih informacija dok pregledavate internet. Stoga provjerite jesu li proširenja preglednika uključena.

3.2.2 Kategorije sadržaja

Možete blokirati pristup nekoliko vrsta sadržaja.

Ikona	Kategorija	Opis
	Sadržaj za odrasle	Web-mjesta namijenjena odraslim publikama na kojima se nalazi jasno seksualan sadržaj ili sadržaj seksualnih konotacija. To su, primjerice, web-mjesta sex-shopova ili seksualno orijentirana golotinja.
	Uznemirujući sadržaj	Web-mjesta koja sadrže slike, objašnjenja ili videoigre koje bi mogle biti uznemirujuće. U toj se kategoriji nalaze informacije, slike i videozapisi odvratnog, jezovitog ili stravičnog sadržaja koji bi mogao uznemiriti malu djecu.
	Narkotici	Web-mjesta koja promiču upotrebu droga. Primjerice, web-mjesta koja sadrže informacije za kupnju, uzgoj ili prodaju neke od tih supstanci.
	Nezakonito	Web-mjesta koja sadrže zakonom zabranjene slike ili informacije.
	Nasilje	Web-mjesta koja mogu poticati na nasilje ili sadrže krvave i nasilne slike ili videozapise. Primjer su web-mjesta s

		informacijama o silovanju, zlostavljanju, snuff sadržaju, bombama, napadima, ubojstvima i samoubojstvima.
	Mržnja	Web-mjesta koja potiču predrasude prema određenoj religiji, rasi, nacionalnosti, spolu, dobi, invaliditetu ili seksualnoj orijentaciji. To su, primjerice, web-mjesta koja promiču nanošenje boli odnosno štete ljudima, životinjama ili ustanovama ili pak sadrže opise ili slike fizičkih napada na neku od tih kategorija.
	Oružje	Web-mjesta koja sadrže informacije, slike ili videozapise o oružju ili bilo čemu što se može koristiti kao oružje za nanošenje ozljeda ljudima ili životinjama. To obuhvaća organizacije koje promiču takva oružja, kao što su lovački i streljački klubovi. Kategorija obuhvaća i igračke u obliku oružja, kao što su puške za paintball, zračne puške i zračni pištolji.
	Kockanje	Web-mjesta na kojima se korisnici mogu kladiti za novac ili neku vrstu kredita putem mreže. To su, primjerice, web-mjesta internetskih kockarnica i igara na sreću te blogovi i forumi koji sadrže informacije o internetskom ili stvarnom kockanju.
	Alkohol i duhan	Web-mjesta na kojima se prikazuju ili promiču alkoholna pića ili pušenje i duhanski proizvodi, uključujući proizvođače kao što su destilerije, vinogradi i pivovare. To su, primjerice, web-mjesta koja promiču pivske festivale i web-mjesta barova i noćnih klubova.
	Nezakonita preuzimanja	Web-mjesta za neovlašteno dijeljenje datoteka ili za piratski softver. To su, primjerice, web-mjesta koja omogućuju nezakonit ili zakonski upitan pristup softveru te ona koja razvijaju i distribuiraju programe koji bi mogli ugroziti mreže i sustave.
	Upoznavanje	Web-mjesta koja služe kao portal za pronalaženje ljubavnih partnera ili partnera za seks. To su, primjerice, web-mjesta za upoznavanje ili ona za naručivanje mladenki.
	Anonimizatori	Web-mjesta koja omogućuju zaobilaženje mrežnih filtara ili sadrže upute za to, uključujući web-mjesta za prijevod koja to omogućuju korisnicima. To su, primjerice, web-mjesta s popisima javnih proxya koji se mogu koristiti za zaobilaženje eventualnih mrežnih filtara.
	Kupovina i dražbe	Web-mjesta na kojima se mogu kupovati proizvodi ili usluge, uključujući ona koja sadrže kataloge artikala koji olakšavaju naručivanje i kupnju putem interneta te web-mjesta koja

		sadrže informacije o naručivanju i kupovanju artikala putem mreže.
	Medijski sadržaji za streaming	Web mjesta i usluge koje korisnicima omogućuju prijenos raznih vrsta videozapisa, često bez dobnih ograničenja.
	Društvene mreže	Portali za umrežavanje koji služe za općenito povezivanje ljudi ili povezivanje s određenim skupinama ljudi radi druženja, poslovne interakcije i dr. To su, primjerice, web-mjesta na kojima možete stvoriti članski profil radi dijeljenja osobnih i profesionalnih interesa. Obuhvaća web-mjesta društvenih mreža kao što je X, Facebook, i sl.
	Nepoznato	Web mjesta koja su nova ili nepoznata našim web filtrima. Sadržaj ovih web mjesta ne može se potvrditi.

3.3 Dijeljenje zaštite s članom obitelji ili prijateljem

Ova tema opisuje kako podijeliti zaštitu s članom obitelji ili prijateljem.

Kada pozovete članove obitelji ili prijatelje u svoju grupu, pozvane osobe dobivaju vlastiti korisnički račun koji im omogućuje zaštitu svojih uređaja pomoću vaših licenci.

Bilješka: Imajte na umu da ako je osoba koju želite pozvati u svoju grupu već dodana u vašu grupu ili pripada nekoj drugoj A1 Sigurniji internet grupi, vidjet ćete poruku u dijaloškom okviru pozivnice koja kaže da ta osoba već pripada vašoj grupi ili drugu grupu. To znači da je adresa e-pošte korištena u pozivnici već aktivirana za A1 Sigurniji internet račun. To možete riješiti korištenjem druge adrese e-pošte, ako postoji, da pozovete korisnika u svoju grupu ili možete zatražiti od ovog korisnika da izbriše postojeći A1 Sigurniji internet račun nakon čega možete koristiti adresu e-pošte u pozivnici.

Za dijeljenje zaštite s nekim drugim:

1. U glavnom prikazu odaberite **Osobe i uređaji**

2. U prikazu **Osobe i uređaji** odaberite **+ Dodaj uređaj ili korisnika**.

3. Odaberi **Tuđi uređaj** > **Nastaviti**.

4. Da biste pozvali korisnika u svoju grupu:
a) Unesite ime korisnika.
b) Unesite prezime korisnika.
c) Unesite email adresu korisnika.
d) Odaberi **Poslati pozivnicu**.

Ova osoba prima e-poštu s pozivnicom i sada ima račun koji joj omogućuje zaštitu svojih uređaja pomoću vaših licenci. Korisnici u vašoj grupi neće vidjeti uređaje ili druge pojedinosti drugih korisnika ili profila u grupi.

3.3.1 Jeste li dobili poziv da zaštitite svoje uređaje?

Ova tema opisuje kako početi štititi svoje uređaje ako ste primili pozivnicu od prijatelja.

Kada vaš prijatelj podijeli zaštitu s vama, primit ćete e-poruku u kojoj ste pozvani da besplatno upotrijebite njihove licence kako biste zaštitili svoj PC, Mac, pametni telefon i tablet. Već smo napravili račun za vas, a podatke o računu možete pronaći u poruci.

Za početak zaštite svojih uređaja:

1. Otvorite e-poštu s pozivnicom i pažljivo je pročitajte. Zabilježite podatke o svom računu.

2. Odaberite **Započni sada**.
Otvara se stranica za prijavu na vaš račun.

3. Unesite vjerodajnice za prijavu na svoj račun koje ste dobili u e-poruci s pozivnicom i odaberite **Prijava**.
Otvara se prikaz **Promjena lozinke**.

4. Stvorite novu jaku lozinku za svoj račun, odaberite **Promijeniti**, a zatim odaberite **Nastaviti**.
Otvara se vaš mrežni portal za upravljanje. Počnite štititi svoje uređaje odabirom **Dodaj uređaj** za instaliranje proizvoda na jedan od vaših uređaja.

Sada možete upravljati vlastitim uređajima i njihovom zaštitom putem online portala za upravljanje ili putem prikaza proizvoda **Osobe i uređaji**. Kao pozvani korisnik, možete upravljati svojim računom na sljedeći način:

▪ Zaštitite više vlastitih uređaja ako to pretplata omogućuje.

▪ Možete promijeniti naziv zaštićenog uređaja.

▪ Možete osloboditi licencu koja se koristi. Imajte na umu da vlasnik pretplate ili osoba koja vas je pozvala na dijeljenje zaštite može ukloniti vaše licence u bilo kojem trenutku.

▪ Grupu možete napustiti u bilo kojem trenutku.

▪ Možete mijenjati postavke svog računa, kao što je promjena lozinke računa i korištenje dvostruke provjere.

3.3.2 Prestanite dijeliti zaštitu s članom obitelji ili prijateljem

Ova tema opisuje kako prestati dijeliti zaštitu s članom obitelji ili prijateljem.

Ako želite prestati dijeliti zaštitu s članom obitelji ili prijateljem, možete ukloniti podkorisnika iz svoje grupe A1 Sigurniji internet.

Za uklanjanje podkorisnika:

1. U glavnom prikazu odaberite **Osobe i uređaji**

2. Odaberite podkorisnika s kojim želite prestati dijeliti zaštitu.

3. Izaberite **Ukloni iz grupe**.

4. Za potvrdu uklanjanja morate se prijaviti na svoj A1 Sigurniji internet račun. Odaberite **Prijava**, unesite vjerodajnice računa, a zatim odaberite **Prijava**.
Otvara se prozor **Ukloni iz grupe**,

5. Odaberite **Ukloni**.

Podkorisnik je uklonjen iz vaše A1 Sigurniji internet grupe i više nije zaštićen vašom pretplatom.

3.4 Oslobađanje licence s uređaja

Ova tema opisuje kako osloboditi licencu koja više nije potrebna za uređaj.

Ako imate uređaj za koji više nije potrebna licenca, preporučujemo da oslobodite licencu. Tek se tada licenca može upotrebljavati na drugom uređaju. Na primjer, ako kupite novo računalo, telefon ili tablet, a stari se više ne upotrebljava, trebate osloboditi licencu koju je upotrebljavao stari uređaj prije nego što se licenca može dodijeliti novom uređaju.

Za oslobađanje licence s uređaja:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. U glavnom prikazu odaberite **Osobe i uređaji**

3. Odaberite korisnika s čijeg uređaja želite osloboditi licencu.
Prikazuje se popis zaštićenih uređaja korisnika.

4. Odaberite uređaj s kojeg želite osloboditi licencu.
Prikazuju se osnovne pojedinosti o uređaju.

5. Izaberite **Oslobodi licencu**.

Bilješka: Da biste potvrdili oslobađanje licence, možda ćete se morati prijaviti na svoj račun. Izaberite **Prijava**, unesite vjerodajnice računa i zatim odaberite **Prijava**.

Otvara se prozor **Oslobodi licencu**.

6. Izaberite **Oslobodi licencu**.
Ovo oslobađa licencu koju sada možete upotrebljavati na drugom uređaju.

Bilješka: Oslobađanje licence s uređaja ne deinstalira sigurnosnu aplikaciju s uređaja. Da biste deinstalirali aplikaciju, morate to učiniti ručno na uređaju.

3.5 Premještanje aplikacije A1 Sigurniji internet sa vašeg starog uređaja na novi

Ova tema objašnjava što učiniti ako ste kupili novi uređaj i želite prenijeti aplikaciju A1 Sigurniji internet na taj novi uređaj.

S vremena na vrijeme možda ćete morati kupiti novo računalo, tablet ili pametni telefon. Možda ste slučajno razbili svoj telefon, ili je završio izgubljen ili ukraden, pa vam treba novi. Važno je osigurati da se licenca vezana za stari uređaj oslobodi prije nego što se može prenijeti i aktivirati na novom uređaju.

Ako još uvijek imate neiskorištenih licenci u svojoj pretplati, instalirajte aplikaciju na novi uređaj na isti način kao što ste to učinili na starom uređaju. Međutim, ako ste potrošili sve svoje dostupne licence, morate osloboditi licencu koja je bila povezana s vašim starim uređajem prije nego što instalirate aplikaciju A1 Sigurniji internet na svoj novi uređaj.

Savjet: Uvijek je dobra ideja osloboditi licencu vezanu uz uređaj koji u potpunosti prestajete koristiti.
Na ovaj način licenca je dostupna za korištenje drugom uređaju kad god je to potrebno.

Dovršite dolje navedene korake u prozoru **Povezane teme** ako trebate prenijeti licencu s jednog uređaja na drugi.

4 Zaštita uređaja

Proizvod štiti računalo od programa koji mogu ukrasti osobne podatke, oštetiti računalo ili pak ga koristiti u nezakonite svrhe.

Bilješka: Ta značajka nije dostupna u svim verzijama aplikacije.

Zaštita od virusa prema zadanim postavkama obrađuje sve štetne datoteke čim ih pronađe da bi spriječila štetu.

Proizvod automatski pregledava lokalne tvrde diskove, uklonjive medije (kao što su prijenosni pogoni ili DVD-ovi) i sav sadržaj koji preuzmete.

DeepGuard daje dodatan sloj sigurnosti radi zaštite osobnih podataka od brisanja, otimanja i krađe putem zlonamjernih aplikacija.

4.1 Korištenje automatskog skeniranja

Automatsko skeniranje štiti vaše računalo u stvarnom vremenu uklanjanjem štetnih datoteka s vašeg računala prije nego što ga mogu oštetiti.

Preporučujemo da automatsko skeniranje stalno bude uključeno. Datoteke možete skenirati i ručno i postaviti zakazana skeniranja ako želite biti sigurni da na vašem računalu nema štetnih datoteka ili skenirati datoteke koje ste isključili iz automatskog skeniranja.

Prema zadanim postavkama, automatsko skeniranje je uključeno kada instalirate sigurnosni proizvod na svoje računalo.

Kako biste bili sigurni da je automatsko skeniranje uključeno:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Ako glavni prikaz proizvoda prikazuje obavijest da je automatsko skeniranje isključeno, odaberite **Upaliti**.
Za detaljne informacije o ovom kritičnom problemu odaberite **Više detalja...**

4.1.1 Kako funkcionira automatsko skeniranje

Automatsko skeniranje štiti računalo skeniranjem svih datoteka kada im se pristupi i blokiranjem pristupa onim datotekama koje sadrže *malware*.

Kada vaše računalo pokuša pristupiti datoteci, automatsko skeniranje skenira datoteku u potrazi za zlonamjernim softverom prije nego što vašem računalu omogući pristup datoteci.

Ako automatsko skeniranje pronađe bilo kakav štetan sadržaj, stavlja datoteku u smeće prije nego što prouzroči bilo kakvu štetu.

Utječe li automatsko skeniranje na performanse mog računala?

Obično ne primjećujete proces skeniranja jer oduzima malo vremena i resursa sustava. Količina vremena i sistemskih resursa potrebnih za automatsko skeniranje ovise o, primjerice, sadržaju, lokaciji i vrsti datoteke.

Za skeniranje datoteka na prijenosnim pogonima, kao što su CD-ovi, DVD-ovi i prijenosni USB pogoni, potrebno je dulje vrijeme.

Bilješka: Komprimirane datoteke, kao što su *.zip* datoteke, ne skeniraju se automatskim skeniranjem.

Ako želite pratiti aktivnost skeniranja na vašem računalu, možete odabrati prikaz indikatora aktivnosti skeniranja na traci izbornika na sljedeći način:

1. Kliknite ikonu proizvoda na traci izbornika i odaberite **Postavke**.

2. Da biste mogli mijenjati postavke, potrebna su vam administratorska prava: odaberite ikonu lokota u donjem lijevom kutu.

3. u **Zaštita uređaja** kartici, odaberite **Prikaži indikator aktivnosti automatskog skeniranja na traci izbornika**.

Automatsko skeniranje može usporiti vaše računalo ako:
▪ imate računalo koje ne zadovoljava sistemske preduvjete
▪ odjednom pristupate velikoj količini datoteka. Primjerice, kada otvorite direktorij s puno datoteka koje je potrebno pregledati.

4.1.2 Privremeno isključivanje automatskog traženja

Ova tema opisuje kako privremeno isključiti automatsko skeniranje.

Upozorenje: Onemogućavanje automatskog skeniranja može učiniti vaše računalo osjetljivim na pohranjivanje štetnog softvera na vaš tvrdi disk i dopuštanje njegovog rada.

Da biste isključili automatsko skeniranje:

1. Na glavnom prikazu aplikacije odaberite **Zaštita uređaja**.

2. Odaberite **Postavke**.

3. Odaberite ikonu zaključavanja u donjem lijevom kutu.
Za promjenu ovih postavki potrebna su vam administrativna prava.

4. u **Zaštita uređaja** kartici, odaberite vrijeme kada želite ponovno automatski uključiti skeniranje i zatim odaberite **Onemogući**.

Čim isključite automatsko skeniranje, obavijest o kritičnom zadatku pojavljuje se na glavnom prikazu proizvoda. Automatsko traženje možete ponovno uključiti u bilo kojem trenutku odabirom **Upaliti** iz zadatka i zatim odabirom **Ponovno uključi** u postavkama proizvoda.

4.2 Pokretanje pregledavanja zlonamjernog softvera

Možete skenirati svoje računalo kako biste bili potpuno sigurni da nema štetnih datoteka ili neželjenih aplikacija.

Pregledavanjem cijelog računala na unutarnjim se i vanjskih tvrdim diskovima traže virusi, špijunski softver i potencijalno neželjene aplikacije. Osim toga, provjerava se i ima li stavki koje su možda skrivene alatom za prikrivanje prisutnosti napadača. Pregledavanje cijelog računala može dugo trajati.

Da biste učinkovitije uklonili neželjene aplikacije i štetne stavke s računala, pregledati možete i dijelove sustava koji sadrže instalirane aplikacije.

Ako su vam određene datoteke na računalu sumnjive, možete skenirati samo te datoteke ili mape.

Ova će skeniranja završiti puno brže nego skeniranje cijelog računala. Na primjer, kada na računalo povežete vanjski tvrdi disk ili USB izbrisivi memorijski pogon, možete ih skenirati kako biste bili sigurni da ne sadrže štetne datoteke.

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu aplikacije odaberite **Zaštita uređaja**.

3. Izaberi **Antivirusno skeniranje**.

4. Odaberite što želite skenirati.
Za skeniranje cijelog računala odaberite **Skeniranje virusa i špijunskog softvera** > **Započni skeniranje**.

Za skeniranje određenih datoteka ili mapa:
a) Izaberi **Odaberite što želite skenirati** > **Odaberite**.
Otvara se prozor u kojem možete odabrati što skenirati.
b) Odaberite datoteke ili mape koje želite skenirati, a zatim odaberite **Otvorena**.
Skeniranje počinje. Kada skeniranje završi, možete vidjeti rezultat skeniranja u prozoru skeniranja.

4.3 Izuzimanje datoteka ili mapa iz skeniranja

Kada izuzmete datoteke ili mape iz pregleda, u njima se neće tražiti štetan sadržaj.

Da biste izostavili datoteke ili mape iz automatskog i ručnog skeniranja:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu aplikacije odaberite **Zaštita uređaja**.

3. U prikazu **Zaštita uređaja** odaberite **Upravljanje izuzecima skeniranja**.
Ovo otvara postavke.

4. Odaberite ikonu lokota da biste dopustili promjene, a zatim odaberite **Postavite izuzetke skeniranja**.
Ovo otvara popis izuzetih datoteka i mapa.

5. Odaberi **+** a zatim odaberite datoteku ili mapu koju želite izuzeti iz skeniranja.
Odabrane datoteke ili mape izuzete su iz budućih pregledavanja.

4.4 Što je DeepGuard?

DeepGuard daje dodatan sloj sigurnosti radi zaštite osobnih podataka od brisanja, otimanja i krađe putem zlonamjernih aplikacija.

DeepGuard omogućuje upotrebu samo sigurnih aplikacija. Sigurnost aplikacija provjerava putem pouzdanog servisa u oblaku. Ako nema informacija, DeepGuard prikazuje dijaloški okvir u kojem odbijate ili prihvaćate aplikaciju.

Provjerom reputacije datoteke DeepGuard poboljšava otkrivanje kompromitacija za sustav.

Aplikacijama koje ne poštuju privatnost, k tome, onemogućuje se korištenje web-kamera, instaliranje novih programa za pokretanje, preuzimanje kontrole nad drugim programima, prisluškivanje internetske veze i druge aktivnosti koje mogu utjecati na vašu privatnost.

Da biste bili sigurni da je DeepGuard aktivan:

1. Kliknite ikonu proizvoda na traci izbornika i odaberite **Postavke**.

2. Odaberite karticu **DeepGuard**.

3. Odaberite ikonu zaključavanja u donjem lijevom kutu.
Za promjenu ovih postavki potrebna su vam administrativna prava.

4. Možete birati između sljedećih opcija:
▪ Prema zadanim postavkama **Pratite aplikacije** je omogućeno. DeepGuard prati aplikacije za potencijalno štetne promjene sustava.
▪ Odaberite **Omogući spremanje novih pravila i korisnicima koji nisu administratori** ako nova pravila za DeepGuard želite primijeniti bez administratorskog računa.

▪ Odaberi **Koristite napredni način rada za upite** ako želite više opcija kada vas DeepGuard pita kako postupati s novim aplikacijama. To vam omogućuje stvaranje detaljnijih pravila za rukovanje određenim aplikacijama ili njihov pristup određenim datotekama i mapama na vašem računalu. Kada DeepGuard otkrije prethodno blokiranu ili nepoznatu aplikaciju u naprednom načinu rada, odaberite **pojedinosti** u dijaloškom okviru dopuštenja za izmjenu ili prilagodbu pravila za aplikaciju.

Bilješka: Sva DeepGuard pravila vidljiva su svim korisnicima. Pravila mogu uključivati nazive datoteka i mapa s osobnim podacima. Stoga imajte na umu da drugi korisnici istog računala mogu vidjeti staze i nazive datoteka uključene u DeepGuard pravila.

4.4.1 Odabir razine zaštite rješenja DeepGuard

DeepGuard ima tri razine zaštite ili skupova pravila koja možete odabrati, ovisno o opsegu u kojem želite pratiti aktivnost na računalu.

Da biste promijenili skup pravila, učinite sljedeće:

1. Kliknite ikonu proizvoda na traci izbornika i odaberite **Postavke**.

2. Odaberite karticu **DeepGuard**.

3. Odaberite ikonu zaključavanja u donjem lijevom kutu.
Za promjenu ovih postavki potrebna su vam administrativna prava.

4. Odaberite **Konfiguriraj DeepGuard**.
Otvorit će se aplikacija **Konfiguracija rješenja DeepGuard**.

5. Odaberite ikonu zaključavanja u donjem lijevom kutu.
Za promjenu ovih postavki potrebna su vam administrativna prava.

6. U aplikaciji **Konfiguracija rješenja DeepGuard** na padajućem izborniku **Skup pravila** odaberite razinu zaštite.

Bilješka: Za promjenu postavke potrebna su vam administratorska prava.

▪ Zadano: ta razina omogućuje većinu ugrađenih aplikacija za macOS i postupaka za normalan rad. Ne omogućuje praćenje operacija samo za čitanje na računalu, ali provjerava pokušaje zapisivanja u datoteke ili njihova pokretanja.
▪ Klasično: ta razina omogućuje većinu ugrađenih aplikacija za macOS i postupaka za normalan rad. Omogućuje praćenje operacija čitanja, zapisivanja i pokretanja datoteka na računalu.
▪ Strogo: ta razina omogućuje pristup samo osnovnim procesima. Daje precizniju kontrolu nad procesima i ugrađenim aplikacijama.

4.4.2 Optimizacija rješenja DeepGuard za vaš sustav

Možete koristiti način za učenje rješenja DeepGuard i stvoriti pravila koja omogućuju aplikacije i operacije koje se pojavljuju prilikom standardne upotrebe računala.

Kada uđete u način za učenje, računalo koristite normalno te otvorite sve aplikacije za koje želite da ih DeepGuard omogući. DeepGuard omogućuje sve pokušaje pristupa datotekama te stvara prilagođena pravila za računalo koja možete uvesti nakon izlaska iz načina za učenje.

Način rada za učenje najkorisniji za **Klasični** i **Strogi** skup pravila. Ako koristite **Zadani** skup pravila, vjerojatno vam nije potreban način rada za učenje.

Upozorenje: DeepGuard ne štiti računalo dok koristite način za učenje.

Da biste koristili način za učenje, učinite sljedeće:

1. Kliknite ikonu proizvoda na traci izbornika i odaberite **Postavke**.

2. Odaberite karticu **DeepGuard**.

3. Odaberite ikonu zaključavanja u donjem lijevom kutu.
Za promjenu ovih postavki potrebna su vam administrativna prava.

4. Odaberite **Konfiguriraj DeepGuard**.
Otvorit će se aplikacija **Konfiguracija rješenja DeepGuard**.

5. u **DeepGuard konfiguracija** aplikacija, odaberite **Datoteka** > **Način učenja**, a kada se to od vas zatraži, unesite svoje administratorske vjerodajnice.

6. Odaberi **U redu** za pokretanje načina učenja.

7. Pokrenite aplikacije koje inače koristite na računalu.

8. Vratite se u aplikaciju **Konfiguracija rješenja DeepGuard** te opet odaberite **Datoteka** > **Način za učenje** da biste izašli iz načina za učenje.
DeepGuard otvara popis aplikacija koje možete uvesti kao pravila, koja omogućuju odabranim aplikacijama da pristupe datotekama na računalu.

9. Odaberite aplikacije koje želite dopustiti, a zatim odaberite **Uvoz**.
Uvezena pravila poslije možete urediti u aplikaciji **Konfiguracija rješenja DeepGuard**.

4.4.3 Omogućivanje aplikacija koje je DeepGuard blokirao

Ako je DeepGuard blokirao aplikaciju koju smatrate pouzdanom i želite omogućiti njen rad, uredite pravilo za tu aplikaciju u aplikaciji **Konfiguracija rješenja DeepGuard**.

Bilješka: Pravila koja stvara DeepGuard nisu specifična za korisnika, pa ih može vidjeti svatko tko koristi isto računalo. Primjerice, većina aplikacija u sustavu macOS instalira se u mapu / Applications (Aplikacije), pa su time dostupne svim korisnicima računala. To znači da pravila koje DeepGuard primjenjuje na takve aplikacije imaju učinak u cijelom sustavu.

Omogućivanje aplikacija koje je DeepGuard blokirao:

1. Kliknite ikonu proizvoda na traci izbornika i odaberite **Postavke**.

2. Odaberite karticu **DeepGuard**.

3. Odaberite ikonu zaključavanja u donjem lijevom kutu.
Za promjenu ovih postavki potrebna su vam administrativna prava.

4. Odaberite **Konfiguriraj DeepGuard**.
Otvorit će se aplikacija **Konfiguracija rješenja DeepGuard**.

5. U aplikaciji **Konfiguracija rješenja DeepGuard** desnom tipkom miša kliknite pravilo za aplikaciju koju želite omogućiti te odaberite **Uredi**.

6. Odaberite **Omogući** kao **Pravilnik** za tu aplikaciju.

7. Odaberite dozvole koje želite omogućiti za tu aplikaciju.

8. Odaberite **Spremi**.

4.5 Što radi štetan sadržaj

Štetne aplikacije i datoteke mogu pokušati oštetiti podatke ili ostvariti neovlašten pristup računalnom sustavu da bi vam ukrale osobne podatke.

4.5.1 Potencijalno neželjene aplikacije (PUA, Potentially unwanted applications) i neželjene aplikacije (UA, Unwanted applications)

"Potencijalno neželjene aplikacije" imaju ponašanja ili obilježja koja možete smatrati neželjenim.
"Neželjene aplikacije" imaju ponašanja i obilježja s ozbiljnijim utjecajem na uređaj ili podatke.

Aplikacija je "potencijalno neželjena" (PUA) ako:
▪ **utječe na vašu privatnost ili produktivnost** – primjerice, otkriva osobne podatke ili izvodi neovlaštene radnje
▪ **nepotrebno opterećuje resurse vašeg računala** – primjerice, koristi prekomjernu količinu prostora za pohranu ili memorije
▪ **ugrožava sigurnost vašeg uređaja i podataka koji su na njemu pohranjeni** – primjerice, izlaže vas neočekivanom sadržaju ili aplikacijama

Učinak takvih ponašanja i obilježja na uređaj ili podatke u rasponu je od blagog do ozbiljnog. No ona nisu dovoljno štetna za klasifikaciju aplikacije kao zlonamjernog softvera.

Ako aplikacija ima ponašanja ili obilježja s ozbiljnim učinkom, smatra se "neželjenom aplikacijom" (UA).
Proizvod će takve aplikacije tretirati s više opreza.

Način na koji proizvod tretira aplikaciju ovisi o tome je li to PUA ili UA:
▪ **Potencijalno neželjena aplikacija** – proizvod će automatski blokirati izvođenje aplikacije. Ako ste sigurni da je aplikacija pouzdana, morate uputiti proizvod tvrtke A1 Sigurniji internet da je izuzme iz pregleda.
Da biste blokiranu datoteku izuzeli od pregledavanja, morate imati administrativne ovlasti.
▪ **Neželjena aplikacija** – proizvod će automatski blokirati izvođenje aplikacije.

4.5.2 Crvi

Crvi su programi koji šalju svoje kopije s jednoga na drugi uređaj putem mreže. Neki crvi, k tome, izvode štetne akcije na zahvaćenom uređaju.

Dosta crva dizajnirano je tako da korisniku djeluju atraktivno. Mogu izgledati poput slika, videozapisa, aplikacija i drugih korisnih programa ili datoteka. Cilj je varke namamiti korisnika da instalira crva.

Drugi su crvi dizajnirani tako da budu posve nevidljivi i da se koriste nedostacima na uređaju (ili u programima instaliranim na njemu) kako bi se neprimjetno instalirali.

Nakon instalacije crv koristi fizičke resurse uređaja da bi stvorio svoje kopije, a zatim šalje te kopije na neke druge uređaje s kojima se može povezati putem mreže. Ako se šalje veliki broj kopija crva, performanse uređaja slabe. Ako je mnogo uređaja na mreži zahvaćeno te šalju kopije crva, mogu se pojaviti smetnje u radu same mreže Neki crvi mogu i napraviti izravnije štete na uređaju, npr. mijenjati datoteke pohranjene na njemu, instalirati druge štetne aplikacije ili krasti podatke.

Većina crva širi se samo putem neke određene vrste mreže. Neki se crvi mogu širiti putem dviju ili više vrsta mreža, ali takvi su razmjerno rijetki. Crvi se obično pokušavaju širiti putem jedne od sljedećih mreža (iako ima i onih napadaju manje popularne kanale):
- Lokalne mreže
- mreže za e-poštu
- web-mjesta društvenih mreža
- P2P veze
- SMS ili MMS poruke

4.5.3 Trojanci

Trojanci su programi koji nude ili se čine da nude neku atraktivnu funkciju ili značajku, ali u tišini izvode štetne akcije u pozadini.

Nazvani prema grčkoj legendi o Trojanskom konju, trojanci su dizajnirani tako da korisniku djeluju atraktivno. Mogu izgledati poput igara, čuvara zaslona, ažuriranja aplikacija ili nekog drugog korisnog programa ili datoteke. Neki trojanci oponašat će ili čak kopirati popularne ili dobro poznate programe da bi izgledali pouzdano. Cilj je prijevare namamiti korisnika da instalira trojanca.

Trojanci nakon instalacije znaju koristiti "varke" da bi održavali iluziju da su legitimni. Trojanac koji se, primjerice, izdaje za čuvara zaslona ili datoteku dokumenta prikazivat će sliku ili dokument. Dok te varke korisniku odvlače pozornost, trojanac može tiho izvoditi druge akcije u pozadini.

Trojanci obično unose štetne promjene na uređaj (npr. brišu ili šifriraju datoteke ili pak mijenjaju programske postavke) ili kradu povjerljive podatke pohranjene na njemu. Trojance je moguće grupirati po akcijama koje izvode:
- **Trojanac preuzimatelj**: povezuje se s udaljenim web-mjestom da bi preuzeo i instalirao druge programe.
- **Trojanac utovarivač**: sadrži dodatne programe, koje instalira.
- **Trojanac za lozinke**: krade lozinke pohranjene na uređaju ili unesene u web-preglednik.
- **Bankovni trojanac**: specijalizirani trojanac za lozinke koji traži korisnička imena i lozinke za portale za internetsko bankarstvo.
- **Špijunski trojanac**: prati aktivnost uređaja i prosljeđuje detalje na udaljeno web-mjesto.

4.5.4 Programi za neovlašten ulazak u sustav

Programi za neovlašteni pristup značajke su ili programi putem kojih se mogu izbjeći sigurnosne značajke programa, uređaja, portala ili usluge.

Značajka programa, uređaja, portala ili usluge može se smatrati programom za neovlašteni ulazak u sustav ako njezin dizajn ili implementacija predstavljaju sigurnosni rizik. Primjerice, programom za neovlašteni ulazak u sustav može se smatrati administratorska pristupna točka na internetskom portalu s kodiranom lozinkom.

Programi za neovlašten ulazak u sustav obično iskorištavaju nedostatke u kodu programa, uređaja, portala ili usluge. Nedostaci mogu biti programske pogreške, slabe točke ili nedokumentirane značajke.

Putem programa za neovlašteni pristup napadači obično ostvaraju neovlašten pristup i izvode štetne akcije koje im omogućuju izbjegavanje sigurnosnih značajki, kao što su ograničenja pristupa, provjera autentičnosti i šifriranje.

4.5.5 Kodovi koji se koriste slabim točkama

Kodovi koji se koriste slabim točkama objekti su ili metode koje iskorištavaju nedostatak programa tako da u njemu izazovu neočekivano ponašanje. Time se stvaraju uvjeti pomoću kojih napadač može izvoditi druge štetne akcije.

Kod koji se koristi slabim točkama možete biti objekt ili metoda. Objekti su, primjerice, i posebno dizajniran program, i dio koda, i niz znakova, a metoda je poseban niz naredbi.

Kod koji se koristi slabim točkama služi za iskorištavanje nedostatka ili rupe (što nazivamo i ranjivost) u nekom programu. Budući da je svaki program različit, svaki kod koji se koristi slabim točkama mora biti pažljivo prilagođen tom konkretnom programu.

Nekoliko je načina na koje napadač može dostaviti kod koji se koristi slabim točkama i utjecati na računalo ili uređaj:
- **ugradnja u hakiran ili posebno dizajniran program** – kod koji se koristi slabim točkama pokreće se kada instalirate i pokrenete taj program
- **ugradnja u dokument priložen poruci e-pošte** – kod koji se koristi slabim točkama pokreće se kada otvorite privitak
- **hostiranje na hakiranom ili štetnom web-mjestu** – kod koji se koristi slabim točkama pokreće se kada posjetite to web-mjesto

Pokretanje koda koji se koristi slabim točkama uzrokuje neočekivano ponašanje programa, npr. rušenje programa ili pak unos promjena u pohranu ili memoriju sustava. To može stvoriti uvjete koji dopuštaju napadaču izvođenje drugih štetnih akcija, kao što su krađa podataka ili ostvarivanje pristupa ograničenim dijelovima operacijskog sustava.

4.5.6 Paketi kodova koji se koriste slabim točkama

Paketi kodova koji se koriste slabim točkama napadačima služe za upravljanje tim kodovima i uvođenje štetnih programa na ranjivo računalo ili uređaj.

Paket kodova koji se koriste slabim točkama sadrže inventar tih kodova koji se koriste slabim točkama od kojih svaki može iskoristiti nedostatak (ranjivost) programa, računala ili uređaja. Sam paket obično je hostiran na štetnom ili hakiranom web-mjestu, pa su sva računala ili uređaji koji posjete to web-mjesto izloženi njegovim efektima.

Kada se novo računalo ili uređaj poveže s miniranim web-mjestom, paket s kodovima koji se koriste slabim točkama traži na njemu sve nedostatke koje bi mogao iskoristiti neki kod u njegovom inventaru.

Ako se neki pronađe, paket pokreće kod koji iskorištava tu ranjivost.

Nakon ugrožavanja računala ili uređaja kod koji se koristi slabim točkama može na njega postaviti korisne podatke. To je obično neki drugi program koji se instalirana i pokreće na računalu ili uređaju, a zatim izvodi neke druge neovlaštene akcije.

Kodovi koji se koriste slabim točkama dizajnirani su tako da budu modularni i jednostavni za upotrebu, pa njihovi kontrolori mogu jednostavno dodavati ili uklanjati kodove i korisne podatke u paket.

4.6 Slanje uzorka

Da biste nam pomogli u poboljšanju zaštite, možete nam poslati sumnjive aplikacije i web-mjesta na analizu.

Kada proizvod blokira aplikaciju, na primjer zato što je mogući sigurnosni rizik za vaše računalo ili je aplikacija pokušala učiniti nešto potencijalno štetno, možete nam poslati uzorak aplikacije u svrhu sigurnosnog istraživanja. To možete učiniti ako znate da je aplikacija koju je proizvod neispravno blokirao sigurna ili ako sumnjate da bi aplikacija mogla biti štetna.

Također, ako sumnjate da web stranica nije sigurna, možete nam poslati njen URL na analizu.

Da biste poslali uzorak na analizu:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu aplikacije odaberite **Zaštita uređaja**.

3. Na **Zaštita uređaja** pogled, odabir **Predajte uzorak**.
Ovo otvara **Predajte uzorak** web stranicu u vašem zadanom web pregledniku gdje možete poslati ili datoteku ili uzorak URL-a na analizu.

4. Da biste poslali uzorak, popunite obrazac na web-mjestu.

5 Zaštita od prijevara

Ovaj odjeljak objašnjava kako aplikacija može osigurati sigurno pregledavanje interneta, kao i sigurno internetsko bankarstvo. Aplikacija vas također štiti od drugih uobičajenih prijevara.

Bilješka: Ta značajka nije dostupna u svim verzijama aplikacije.

Zaštita pregledavanja prikazuje sigurnosne ocjene za web-mjesta navedene u rezultatima tražilice.

Prepoznavanjem web-mjesta koja sadrže sigurnosne prijetnje, kao što su zlonamjerni softver (virusi, crvi, trojanski programi) i krađa identiteta, sigurnosne ocjene zaštite pregledavanja pomažu vam da izbjegnete najnovije internetske prijetnje koje tradicionalni antivirusni programi još ne prepoznaju.

Ocjene sigurnosti web-mjesta temelje se na analizi našeg reputacijskog servisa za web-mjesta.

Zaštita pregledavanja kompatibilna je s web-preglednicima Safari, Microsoft Edge, Mozilla Firefox i Google Chrome.

5.1 Ikone ocjene ugleda u rezultatima pretraživanja

Zaštita pregledavanja prikazuje ocjene sigurnosti za web-mjesta na stranici s rezultatima pretraživanja kada koristite Google, Bing, Yahoo ili DuckDuckGo.

Ikone različitih boja označavaju ocjenu sigurnosti trenutnog web-mjesta. Istim se ikonama prikazuje i sigurnosna ocjena svake veze na stranici:

Koliko znamo, ovo je web-mjesto sigurno. Nismo na njemu pronašli ništa sumnjivo.

Web-mjesto je sumnjivo i preporučujemo da budete oprezni kad ga posjećujete. Izbjegavajte preuzimanje datoteka i navođenje osobnih podataka.

Web-mjesto je štetno. Preporučujemo da izbjegavate posjećivanje ovog web-mjesta.

Alternativno, administrator je blokirao ovo web-mjesto i ne možete ga posjetiti.

Još nismo analizirali to web-mjesto ili trenutno nema dostupnih informacija za njega.

Pristup ovom web-mjestu nikad nije blokiran.

Ako smatrate da je blokirana stranica sigurna i da je uopće ne treba blokirati, možete je poslati na analizu ovdje ili je prijavite izravno pomoću ikone proširenja za zaštitu pregledavanja na alatnoj traci preglednika.

Ako ne vidite nijednu ikonu ocjene reputacije na stranici rezultata pretraživanja, provjerite je li postavka uključena:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu aplikacije odaberite **Zaštita od prijevara**.

3. Odaberite **Postavke**.

4. Odaberite ikonu zaključavanja u donjem lijevom kutu.
Za promjenu ovih postavki potrebna su vam administrativna prava.

5. Provjerite je li uključena **Zaštita pregledavanja**.

6. Odaberite **Prikaži ocjenu ugleda za web stranice u rezultatima pretraživanja**.

7. Ako je preglednik otvoren, ponovno ga pokrenite da biste primijenili promijenjene postavke.

Bilješka: Da biste koristili zaštitu pregledavanja, u web-pregledniku koji koristite proširenje Zaštita pregledavanja mora biti uključeno.

5.2 Blokiranje štetnih web-mjesta

Zaštita pregledavanja blokira pristup štetnim web-mjestima kada je uključena.

Zaštita pregledavanja automatski se uključuje kada počnete koristiti proizvod.

Da biste provjerili je li Zaštita pregledavanja uključena:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu aplikacije odaberite **Zaštita od prijevara**.

3. Odaberite **Postavke**.

4. Uvjerite se da je **Zaštita pregledavanja** odabrana.

Bilješka: Zaštita pregledavanja zahtijeva da instalirate i omogućite proširenje za web preglednik koji koristite. Proizvod podržava preglednike Safari, Microsoft Edge, Mozilla Firefox i Google Chrome.

5.2.1 Dopuštanje blokiranih web-mjesta

Ako ste uvjereni da su sigurna, možete ručno dopustiti web-mjesta koja je proizvod blokirao.

Da biste dopustili blokirano web-mjesto:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu aplikacije odaberite **Zaštita od prijevara**.

3. Odaberite **Upravljanje dopuštenim i blokiranim web-mjestima**.

4. Odaberite ikonu zaključavanja u donjem lijevom kutu.
Za promjenu ovih postavki potrebna su vam administrativna prava.

5. U odjeljku **Dopuštena web-mjesta** odaberite opciju **Postavite dopuštena web-mjesta**.
Otvorit će se prozor **Dodajte web-mjesta koja želite dopustiti**.

6. Za dodavanje web-mjesta na popis dopuštenih web-mjesta odaberite **+** u donjem lijevom uglu prozora, unesite adresu web-mjesta koje želite dopustiti i pritisnite **Unesi**.
Web-mjesto je sada navedeno kao dopušteno.

7. Da biste uklonili web-mjesto s popisa dopuštenih web-mjesta, odaberite adresu web-mjesta, a zatim odaberite **-** u donjem lijevom uglu prozora.

8. Za zatvaranje prozora odaberite **Gotovo**.

5.2.2 Ručno dopuštanje blokiranih web-mjesta

Kad pokušate pristupiti web-mjestu koje je ocijenjeno kao štetno, prikazat će se stranica blokiranja zaštite pregledavanja.

Kada se pojavi stranica blokirana zaštitom pregledavanja, a još uvijek želite ući na web-mjesto:

1. Ako želite ući na web-mjesto, odaberite **Dopusti web-mjesto na ovom računalu** > **Dopusti**.

2. Unesite svoju administratorsku lozinku i odaberite **u redu**.
Otvorit će se blokirano web-mjesto. Uz to, proizvod će web-mjesto dodati na popis dopuštenih web mjesta.

Ako mislite da je blokirano web-mjesto sigurno i da ga nije potrebno blokirati, možete ga poslati na analizu ovdje.

5.3 Uključivanje zaštite bankarstva

Sigurno online plaćanje štiti vas od štetnih aktivnosti prilikom pristupa internetskim bankama ili obavljanja transakcija na internetu.

Zaštita bankarstva automatski otkriva sigurne veze s priznatim internetskim bankovnim web-mjestima i obavještava vas kada posjetite bilo koje takvo mjesto.

Zaštita bankarstva trenutačno podržava sljedeće preglednike:
- Safari
- Mozilla Firefox
- Google Chrome
- Microsoft Edge

Bilješka: Zaštita bankarstva zahtijeva upotrebu proširenja preglednika.

Zaštita bankarstva uključena je prema zadanim postavkama. Ako nije uključena, uključite je na sljedeći način:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu aplikacije odaberite **Zaštita od prijevara**.

3. Odaberite **Postavke**.

4. Odaberite ikonu zaključavanja u donjem lijevom kutu.
Za promjenu ovih postavki potrebna su vam administrativna prava.

5. Odaberite **Sigurno online plaćanje**.
Čim vaša sesija bankarenja završi, međuspremnik će se automatski izbrisati. Ako želite, možete promijeniti ovu postavku u postavkama Sigurnog pregledavanja.

5.4 Sigurna online kupnja

Zaštita kupnje čini vaše online kupnje sigurnijima obavještavajući vas o lažnim i nepouzdanim web stranicama.

Bilješka: Zaštita kupnje zahtijeva da je proširenje Zaštita pregledavanja omogućeno u web pregledniku koji koristite.

Zaštita kupnje je prema zadanim postavkama uključena kako bi se poboljšala sigurnost vaše online kupnje. Nakon ulaska na web mjesto za kupnju, skočni prozor s ocjenom sigurnosti prikazuje se u donjem desnom kutu stranice kako bi se pokazalo koliko je web mjesto pouzdano. Ako je mjesto za kupnju sigurno, skočni prozor nestaje nakon nekoliko sekundi i više se neće prikazati na toj stranici tijekom sesije kupnje. Međutim, ako web mjesto nije sigurno, skočno upozorenje ostat će na stranici dok ne napustite web mjesto.

Možete prilagoditi kada se obavijesti prikazuju u postavkama proizvoda, na primjer ako ne želite vidjeti obavijesti za web stranice za sigurnu kupnju.

Skočni prozor s ocjenom sigurnosti prikazuje se i kada uđete na mjesto za kupnju klikom na vezu, na primjer u poruci e-pošte ili tekstualnoj poruci.

Ocjene sigurnosti također su predstavljene kao informativne ikone na stranicama s rezultatima pretraživanja kada koristite popularne tražilice kao što su Google, Bing, Yahoo ili DuckDuckGo. Kada prijeđete mišem iznad ikone ocjene, vidjet ćete detalje o sigurnosti web stranice.

Tim je informacijama također moguće pristupiti putem ikone proširenja preglednika na alatnoj traci preglednika.

Za promjenu postavki za Zaštitu kupovine:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu aplikacije odaberite **Zaštita od prijevara**.

3. Odaberite **Postavke**.

4. Odaberite ikonu zaključavanja u donjem lijevom kutu.
Za promjenu ovih postavki potrebna su vam administrativna prava.

5. Uključite ili isključite **Zaštitu kupnje**.

6. Odaberite ili poništite **Prikaži obavijesti za web stranice za sigurnu kupnju** i **Prikaži obavijesti za sumnjive web stranice za kupnju** prema tome koje obavijesti želite vidjeti.

5.5 Blokiranje oglasa na web-mjestima

Blokiranje oglasa blokira oglašivački sadržaj na web-mjestima koja posjećujete i tako otežava da vas se prati te poboljšava vaše iskustvo pregledavanja.

Blokiranje oglasa je prema zadanim postavkama uključeno kako bi se spriječilo učitavanje sadržaja s uobičajenih poslužitelja za oglase. Gornji desni kut prikaza **Sigurno pregledavanje** pokazuje vam broj oglasa koje je proizvod blokirao.

Ako se stranica koju posjećujete ne učitava ispravno bez oglasa, možete privremeno isključiti Blokiranje oglasa:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu aplikacije odaberite **Zaštita od prijevara**.

3. Odaberite **Postavke**.

4. Odaberite ikonu zaključavanja u donjem lijevom kutu.
Za promjenu ovih postavki potrebna su vam administrativna prava.

5. Isključite opciju **Blokiraj oglase**.
Kada ponovno učitate stranicu u svom pregledniku, ona će sadržavati oglase.

5.6 Odbijanje nepotrebnih kolačića

Značajka Blokator skočnih prozora kolačića pomaže u zaštiti vaše privatnosti tijekom pregledavanja izbjegavanjem nepotrebnih kolačića.

Web-mjesta koriste kolačiće u različite svrhe, kao što je pohranjivanje informacija povezanih s vašom sesijom, identificiranje vašeg računa ili praćenje stranica koje pregledavate. Dok su neki kolačići često potrebni kako bi web mjesto bilo upotrebljivo, neki se mogu koristiti za prikupljanje podataka o vašoj mrežnoj aktivnosti. Zbog toga su različite regionalne vlasti uvele zakone koji zahtijevaju da web stranice traže pristanak za korištenje kolačića od bilo koga tko posjećuje tu stranicu.

Blokator skočnih prozora kolačića identificira poznate pružatelje pristanka za kolačiće na web mjestima koje posjećujete i automatski odbija nepotrebne kolačiće. Međutim, ne koriste sva web mjesta takve pružatelje, pa značajka ne radi na tim web mjestima.

Za promjenu postavki Blokatora skočnih prozora kolačića:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu aplikacije odaberite **Zaštita od prijevara**.

3. Odaberite **Postavke**.

4. Uključite ili isključite **Blokator skočnih prozora kolačića** .

5.7 Provjera koriste li se proširenja preglednika

Za zaštitu pregledavanja **obavezna su** proširenja za preglednik da bi vaše pregledavanje mreže, internetsko bankarstvo i kupovina bili zaštićeni te da bi se mogli prikazivati podaci o sigurnosti dok pregledavate internet.

Kada instalirate proizvod na svoje računalo, proizvod zahtijeva da instalirate i omogućite proširenje za web-preglednik koji upotrebljavate.

Nadalje, glavni prikaz proizvoda obavještava vas ako proširenje za preglednik još nije postavljeno.

Najlakši je način na koji možete postaviti proširenje za preglednik da odaberete **Postavljanje** u obavijesti prikazanoj na glavnom prikazu proizvoda pa slijedite upute na zaslonu.

Da biste instalirali i uključili proširenja za preglednike koje upotrebljavate, pogledajte povezane upute.

5.7.1 Instaliranje i omogućavanje proširenja preglednika za Safari

Morate instalirati i omogućiti proširenje preglednika za Safari kako biste mogli sigurno koristiti preglednik Safari.

Za postavljanje proširenja preglednika:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu aplikacije odaberite **Zaštita od prijevara**.

3. Odaberite **Proširenja pregledavanja**.

4. U odjeljku **Safari web proširenje** odaberite **Instaliraj proširenje**.

5. Nakon što je instalacija završena, odaberite **Omogući dopuštenja**.
Otvorene su postavke **Proširenja**. S lijeve strane možete vidjeti koja su proširenja instalirana na vašem Macu.

6. Označite potvrdni okvir pored odjeljka **Sigurno pregledavanje** da biste omogućili proširenje.

7. U odjeljku **Dozvole**, odaberite **Uvijek dopusti na svakom web mjestu**.
Sada možete sigurno pregledavati internet pomoću Safarija.

Da biste provjerili funkcionira li proširenje za preglednik, u pregledniku otvorite stranicu za testiranje:
https://unsafe.fstesting.net. Prikazat će vam se stranica za blokiranje proizvoda.

5.7.2 Instaliranje i omogućavanje proširenja preglednika za Chrome

Morate instalirati i omogućiti proširenje preglednika za Chrome kako biste mogli sigurno koristiti preglednik Chrome.

Za postavljanje proširenja preglednika:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu aplikacije odaberite **Zaštita od prijevara**.

3. Odaberite **Proširenja pregledavanja**.

4. Pod **Web proširenje za Chrome** odaberite **Instaliraj proširenje**.
Otvorit će se stranica **Zaštita pregledavanja A1 Sigurniji internet**.

5. Odaberite **Dodaj u Chrome** > **Dodaj proširenje**.
Sada možete koristiti Chrome za sigurno pregledavanje interneta.
Da biste provjerili funkcionira li proširenje za preglednik, u pregledniku otvorite stranicu za testiranje:
https://unsafe.fstesting.net. Prikazat će vam se stranica za blokiranje proizvoda.

5.7.3 Instaliranje i omogućavanje proširenja preglednika za Firefox

Morate instalirati i omogućiti proširenje preglednika za Firefox kako biste mogli sigurno koristiti preglednik Firefox.

Za postavljanje proširenja preglednika:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu aplikacije odaberite **Zaštita od prijevara**.

3. Odaberite **Proširenja pregledavanja**.

4. Pod **Proširenje za Firefox** odaberite **Instaliraj proširenje**.
Otvorit će se stranica **Zaštita pregledavanja A1 Sigurniji internet**.

5. Odaberite **Dodaj u Firefox** > **Dodaj**.
Nakon što instalirate proširenje, otvorit će se dijaloški okvir za pristanak korisnika. Proširenje preglednika zahtijeva vaše dopuštenje za pristup informacijama o web-mjestima koja posjećujete.

6. Odaberite **Dopusti**.
Ako odbijete dati dopuštenje, nećete moći upotrebljavati proširenje, a zaštita od pregledavanja neće moći blokirati štetna web-mjesta niti prikazati ocjene rezultata pretraživanja. Također, proširenje će biti uklonjeno iz preglednika.

7. Da biste dovršili postavljanje proširenja odaberite **U redu**.

Sada možete koristiti Firefox za sigurno pregledavanje interneta.

Da biste provjerili funkcionira li proširenje za preglednik, u pregledniku otvorite stranicu za testiranje:
https://unsafe.fstesting.net. Prikazat će vam se stranica za blokiranje proizvoda.

5.7.4 Instaliranje i omogućavanje proširenja preglednika za Edge

Morate instalirati i omogućiti proširenje preglednika za Microsoft Edge kako biste mogli sigurno koristiti preglednik Edge.

Za postavljanje proširenja preglednika:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu aplikacije odaberite **Zaštita od prijevara**.

3. Odaberite **Proširenja pregledavanja**.

4. U odjeljku **Proširenje za Microsoft Edge** odaberite **Instaliraj proširenje**.
Otvorit će se stranica **Zaštita pregledavanja A1 Sigurniji internet**.

5. Odaberite **Dohvati** > **Dodaj proširenje**.
Sada možete koristiti Edge za sigurno pregledavanje interneta.

Da biste provjerili funkcionira li proširenje za preglednik, u pregledniku otvorite stranicu za testiranje:
https://unsafe.fstesting.net. Prikazat će vam se stranica za blokiranje proizvoda.

6 Spremište za lozinke

Uz Spremište za lozinke možete poboljšati svoju sigurnost stvaranjem jakih i jedinstvenih lozinki. Također vam omogućuje sinkronizaciju lozinki na svim vašim uređajima, što znači da su vam lozinke dostupne bez obzira na to koji uređaj upotrebljavate. To čini prijavu na vaše mrežne račune lakšom i sigurnijom.

Bilješka: Ta značajka nije dostupna u svim verzijama aplikacije.

6.1 Početak rada sa Spremištem za lozinke

Ova tema opisuje kako započeti s korištenjem Spremišta za lozinke.

Prije nego počnete koristiti svoje lozinke i osobne podatke u Spremištu za lozinke, morate
▪ stvoriti svoju glavnu lozinku - jedinu lozinku koju morate zapamtiti nakon što je stavite Spremište za lozinke u upotrebu;
▪ izraditi QR kod za oporavak - jedinstveni i osobni kod koji je jedini način da ponovno dobijete pristup Spremištu za lozinke ako zaboravite glavnu lozinku;
▪ postaviti automatsko popunjavanje za automatsko popunjavanje pohranjenih korisničkih imena i zaporki na web stranicama.

Bilješka: Ako ste postojeći korisnik Spremišta za lozinke, jednostavno povežite svoje uređaje i sinkronizirajte svoje lozinke i osobne podatke.

Kako postaviti Spremište za lozinke:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. U glavnom prikazu odaberite **Spremište za lozinke**.

3. Odaberi **Započnite**.

4. Odaberite jedno od sljedećeg:
▪ **Ako ste novi korisnik**:
a. Odaberite **Kreiraj glavnu lozinku**.
b. Odaberite lozinku ili zaporku koju je lako zapamtiti, ali ima smisla samo za vas.
c. Ponovite glavnu lozinku.
d. Odaberite **Kreiraj glavnu lozinku**.
e. Ako zaboravite svoju glavnu zaporku, jedini način da je vratite je korištenje QR koda za oporavak koji morate prethodno izraditi. Odaberite **Spremi QR kod za oporavak**.
f. Odaberite mjesto na koje želite spremiti sliku QR koda za oporavak i zatim odaberite **Spremi**.
g. Počnite dodavati svoje lozinke i podatke o kreditnoj kartici u Spremište za lozinke.

▪ Ako već koristite Spremište za lozinke na drugom uređaju ili aplikaciji, jednostavno povežite uređaje i sinkronizirajte svoje lozinke i osobne podatke:

a. Odaberite **Povezivanje uređaja**.
b. Otvorite Spremište za lozinke na vašem drugom uređaju koji već ima Spremište za lozinke instalirano.
c. Ovisno o tome je li drugi uređaj mobilni ili stolni uređaj, učinite nešto od sljedećeg:

▪ Na mobilnom uređaju odaberite  > **Povežite uređaje** > **Generirajte kod za sinkronizaciju**.

▪ Na stolnom uređaju odaberite  **Povežite uređaje**

Kôd za sinkronizaciju automatski se generira.
d. Unesite generirani kod za sinkronizaciju u **Sinkronizacijski kod** polje i odaberite **Povežite uređaje**.
e. Kada se to od vas zatraži, unesite svoju glavnu lozinku koju koristite na uređaju na kojem ste generirali kod za sinkronizaciju i odaberite **Potvrdi**.
Vaše lozinke i podaci sada su sinkronizirani na ova dva uređaja.

5. Postavite automatsko popunjavanje za pristup svojim internetskim uslugama bez potrebe za ručnim unosom korisničkog imena i lozinke:

a) U Spremištu za lozinke odaberite  **Automatsko popunjavanje**.
Otvara se prikaz **Automatska ispuna**.
b) Odaberite gumb za instaliranje proširenja preglednika ili dodatka za preglednik koji koristite.
c) Nakon instaliranja proširenja, vratite se na **Automatsko popunjavanje** pogledajte i odaberite **Kopiraj kod** za kopiranje autorizacijskog koda.
d) Ponovno u pregledniku kliknite ikonu proširenja upravitelja lozinki u gornjem desnom kutu preglednika i zalijepite kod u polje.
Od sada nadalje, kada postavite miš u polja za korisničko ime i lozinku na stranici za prijavu online usluge kojoj želite pristupiti, u polju će se pojaviti ikona Spremišta za lozinke. Kliknite na ikonu i odaberite uslugu za pristup.

6.2 Korištenje trezora lozinki

U Spremištu za lozinke možete stvarati i uređivati unose zaporki i kartica za plaćanje, dopustiti aplikaciji da generira jake zaporke za vaše online usluge i pristupiti povijesti vaših zaporki.

6.2.1 Prijava na internetsku uslugu sa Spremištem za lozinku

Postoje različiti načini na koje se možete prijaviti na internetsku uslugu čije ste vjerodajnice i web adresu stranice za prijavu pohranili u Spremište za lozinke.

Da biste se mogli prijaviti na online uslugu:
▪ Morate imati tražene podatke - **korisničko ime**, **lozinku** i **web-adresu** mrežne usluge ili web mjesta - pohranjene u trezoru lozinki.

▪ Proširenje preglednika upravitelja lozinki mora biti instalirano za preglednik koji koristite za pristup usluzi. Ovo je potrebno kako bi automatsko popunjavanje radilo.

Upotrijebite bilo koji od sljedećih načina za prijavu na internetsku uslugu ili web mjesto:

1. Za pristup online usluzi izravno iz vašeg web preglednika putem ikone proširenja upravitelja lozinki:
a) Pobrinite se da je vaše Spremište za lozinke je otključano.
b) Na alatnoj traci preglednika kliknite ikonu dijela slagalice da biste otvorili izbornik **Proširenja** i odaberite proširenje **Upravitelj lozinki tvrtke F-Secure**.

Bilješka: Ako **Upravitelj lozinki tvrtke F-Secure** proširenje nije navedeno na izborniku, morate postaviti potrebno proširenje za preglednik koji koristite. Vidjeti **Povezane teme** ispod.

U **Spremištu za lozinke** otvara se skočni dijaloški okvir.
c) Potražite željenu online uslugu i odaberite je kada je pronađete.
d) Izaberi **Idi na web adresu** i kada se otvori stranica za prijavu, kliknite na ikonu Spremišta za lozinke u polju korisničkog imena i odaberite željenu online uslugu.
Aplikacija ispunjava vaše korisničko ime i lozinku. Imajte na umu da na nekim stranicama za prijavu morate zasebno odabrati lozinku za online uslugu.
e) Odaberite gumb za prijavu.

2. Za pristup online usluzi izravno iz vašeg web preglednika:
a) Pobrinite se da je vaše Spremište za lozinke otključano.
b) Otvorite svoj preglednik i idite na stranicu za prijavu online usluge (web stranice) kojoj želite pristupiti.
Ako ste postavili proširenje preglednika upravitelja lozinki za preglednik koji koristite, trebali biste vidjeti ikonu Spremišta za lozinke u polju za korisničko ime.
c) Pritisnite ikonu i odaberite online uslugu s padajućeg popisa koji se otvori.
Aplikacija ispunjava vaše korisničko ime i lozinku. Imajte na umu da na nekim stranicama za prijavu morate zasebno odabrati lozinku za online uslugu.
d) Odaberite gumb za prijavu.

3. Za pristup online usluzi iz Spremište za lozinke:
a) Otvorite aplikaciju A1 Sigurniji internet.
b) U glavnom prikazu odaberite **Spremište za lozinke**.
c) Odaberite unos mrežne usluge kojoj želite pristupiti.
Otvaraju se detalji unosa.
d) Odaberite web adresu usluge.
U vašem pregledniku otvara se stranica za prijavu na uslugu. Ako ste postavili proširenje preglednika upravitelja lozinki za preglednik koji koristite, trebali biste vidjeti ikonu Spremišta za lozinke u polju za korisničko ime.
e) Pritisnite ikonu i odaberite online uslugu s padajućeg popisa koji se otvori.
Aplikacija ispunjava vaše korisničko ime i lozinku. Imajte na umu da na nekim stranicama za prijavu morate zasebno odabrati lozinku za online uslugu.
f) Odaberite gumb za prijavu.

Bilješka: Na nekim stranicama za prijavu korisničko ime i lozinka se automatski popunjavaju, a jedino što trebate učiniti je odabrati gumb za prijavu.

6.2.2 Pohranjivanje nove lozinke u Spremište za lozinke

Ova tema opisuje kako dodati nove lozinke u Spremište za lozinke.

Za pohranu nove lozinke:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. U glavnom prikazu odaberite **Spremište za lozinke**.

3. Odaberi  pored polja **Naslov** i odaberite boju i simbol za unos, zatim odaberite **Ažuriraj**. Ovisno o simbolu koji odaberete, aplikacija može automatski ispuniti naslov i web adresu web stranice ili online usluge.

4. u polje **Titula** unesite naziv web stranice ili online usluge ako aplikacija to već niste učinili.

5. u polje **Korisničko ime** unesite korisničko ime koje koristite za web mjesto ili uslugu.

6. u polje **Zaporka**, učinite nešto od sljedećeg:
- Stvorite jaku lozinku ili pristupni izraz.
- Izaberite  kako bi aplikacija za vas generirala jaku, nasumičnu lozinku. Kada ste zadovoljni lozinkom, odaberite **Ažuriraj**.

Bilješka: Odaberite  ako želite vidjeti lozinku.

7. u polje **Web adresa**, unesite web-adresu (URL) stranice za prijavu online usluge ako aplikacija to već nije učinila.

Bilješka: Format web adrese mora biti https://example.com.

8. U polje **Bilješke** unesite eventualne dodatne informacije.

9. Odaberite **Spremi**.
Podaci o unosu sada su pohranjeni u Spremište za lozinke.

Važno: Ako promijenite ili generirate lozinku u Spremištu za lozinke, također nemojte zaboraviti promijeniti lozinku u web-servisu ili aplikaciji i obratno.

6.2.3 Pohranjivanje podataka vaše platne kartice u Spremište za lozinke

Ova tema opisuje kako pohraniti podatke o platnoj kartici u Spremište za lozinke.

Za pohranu podataka o platnoj kartici:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. U glavnom prikazu odaberite **Spremište za lozinke**.

3. Odaberite **Dodaj novo**.
Otvaraju se detalji unosa, prikazujući „Lozinka" kao zadanu vrstu unosa.

4. U **Tip** padajućem izborniku, odaberite **Kreditna kartica**.

5. Za promjenu ikone unosa s lijeve strane dodirnite je, odaberite boju i jedan od dostupnih simbola platne kartice, zatim odaberite **Ažuriraj**.
Na temelju simbola koji odaberete, aplikacija može umjesto vas ispuniti naziv i web adresu kartičarske kuće.

6. U polje **Titula** unesite naziv kartičarske kuće ako aplikacija to već nije učinila.

7. U polje **Ime vlasnika kartice** unesite svoje ime onako kako je na platnoj kartici.

8. U polje **Broj kreditne kartice** unesite broj vaše kartice.

9. U polje **PIN** unesite svoj osobni identifikacijski broj vezan uz karticu.

10. U polje **Datum isteka roka trajanja** unesite datum (u formatu MM/GG) do kojeg kartica vrijedi.

11. U polje **Kontrolni kod**, unesite 3- ili 4-znamenkasti sigurnosni kod vaše kartice koji vam pomaže u zaštiti od prijevare s kreditnom karticom.

12. Ako želite, možete unijeti internetsku adresu izdavatelja kartice u polje **Internetska adresa**.

13.U polje **Bilješke** unesite bilo koju drugu informaciju koju želite dodati.

14. Odaberite **Spremi**.
Podaci o vašoj platnoj kartici sada su pohranjeni u Spremište za lozinke.

6.2.4 Uređivanje postojećih podataka

Možda ćete morati urediti postojeće unose u Spremištu za lozinke u nekom trenutku.

Za uređivanje unosa:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. U glavnom prikazu odaberite **Spremište za lozinke**.

3. Odaberite unos koji želite urediti.
Otvaraju se detalji unosa.

4. Izaberite **Uredi**.

5. Napravite potrebne promjene.

6. Odaberite **Spremi** za spremanje promjena.

6.2.5 Brisanje unosa

Možete izbrisati unose iz Spremišta za lozinke koji vam više nisu potrebni.

Za brisanje unosa:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. U glavnom prikazu odaberite **Spremište za lozinke**.

3. Odaberite unos koji želite izbrisati.
Otvaraju se detalji unosa.

4. Izaberi **Uredi**.

5. Za brisanje unosa odaberite **Ukloniti** > **u redu**.

Za brisanje više unosa odjednom:

1. U prikazu unosa odaberite unose koje želite izbrisati: držite pritisnutu **Naredba** tipku i odaberite unose. Na desnoj strani možete vidjeti broj odabranih unosa.

2. Za brisanje odabranih unosa odaberite **Izbrisati** > **Izbrisati**.

6.2.6 Dopuštanje aplikaciji da generira novu lozinku za postojeći unos

Kada trebate promijeniti lozinku, Spremište za lozinke može generirati jaku lozinku za vas. Možete odabrati duljinu i složenost lozinke.

Za generiranje lozinke:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. U glavnom prikazu odaberite **Spremište za lozinke**.

3. Odaberite unos čiju lozinku želite promijeniti.
Otvaraju se detalji unosa.

4. Odaberi **Uredi** za uređivanje pojedinosti unosa.

5. U polju **Zaporka**, odaberite  .

6. U pogledu **Generiraj lozinku**, možete učiniti sljedeće:
▪ Povucite klizač s jedne strane na drugu kako biste odabrali broj znakova koje želite u svojoj zaporci.
▪ Odaberite vrstu znakova (mala i velika slova, brojke i posebni znakovi) koje želite u svojoj lozinci.
▪ Odaberite  Generirati za generiranje nove lozinke.

7. Za korištenje generirane lozinke odaberite **Ažuriraj** > **Spremi**.

6.2.7 Pristup vašim starim lozinkama

Dnevnik povijesti lozinki sadrži vaše prethodne lozinke, ako ih ima, za predmetnu mrežnu uslugu.

Nakon što ste promijenili lozinku u Spremište za lozinke, možda ćete se i dalje morati prijaviti na online uslugu sa starom lozinkom. Također, vrlo često, prije nego što možete promijeniti lozinku za uslugu, morate unijeti staru lozinku.

Za pristup prethodnim lozinkama:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. U glavnom prikazu odaberite **Spremište za lozinke**.

3. Odaberite unos čije prethodne lozinke želite vidjeti.
Otvaraju se detalji unosa.

4. U detaljima unosa odaberite **Povijest lozinki**.

Bilješka: Ako ne možete vidjeti **Povijest lozinki** u detaljima unosa nema dostupnih prethodnih lozinki za tu određenu online uslugu.

Otvara se pogled **Povijest lozinki**.

5. Za prikaz skrivene lozinke odaberite  pored lozinke.

Bilješka: Možete kopirati željenu lozinku u međuspremnik odabirom .

6. Za zatvaranje pogleda **Povijest lozinki**, odaberite **Zatvoriti**.
Ako želite, možete izbrisati povijest lozinki odabirom **Očisti**.

6.2.8 Provjerite jesu li vaše lozinke jake

Slabe lozinke čine vas ranjivima na krađu identiteta.

Spremište za lozinke pomaže vam da poboljšate svoje lozinke.

Kako biste saznali koliko su dobre vaše lozinke:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. U glavnom prikazu odaberite **Spremište za lozinke**.

3. Odaberi  **Analiza lozinki**.
Otvara se prikaz koji prikazuje kvalitetu vaših zaporki.

4. Ako imate slabu lozinku, odaberite **Uredi** pored lozinke.
Otvaraju se detalji unosa.

5. Uredite lozinku da bude jača i sigurnija, a zatim odaberite **Spremi** za spremanje promjena.

Važno: Ako promijenite ili generirate lozinku u Spremištu za lozinke, također nemojte zaboraviti promijeniti lozinku u web-servisu ili aplikaciji i obratno.

6. Ponavljajte gore navedeno dok sve vaše lozinke ne postanu jake.

6.3 Povezivanje uređaja za sinkronizaciju vaših podataka iz Spremišta za lozinke na svim vašim uređajima

Ako koristite Spremište za lozinke na drugom uređaju ili aplikaciji, možete povezati svoje uređaje i sinkronizirati svoje podatke kako bi bili dostupni i uvijek ažurni na oba uređaja.

Provjerite imate li pri ruci uređaje koje želite povezati i imate li aplikaciju već instaliranu na oba uređaja.

Za sinkronizaciju podataka na oba uređaja:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. U glavnom prikazu odaberite **Spremište za lozinke**.

3. Odaberite  **Spoji uređaje**.

Otvorit će se prikaz **Poveži uređaje** te će se automatski generirati kôd za sinkronizaciju. Valjan je 60 sekundi. Novi će se kod generirati odmah po isteku trenutačnog koda.

4. Otvorite aplikaciju na uređaju s kojim se želite povezati i sinkronizirati svoje podatke i odaberite **Spremište za lozinke**.

5. Ovisno o tome je li drugi uređaj mobilni ili stolni uređaj, učinite nešto od sljedećeg:
▪ Na mobilnom uređaju:
a. Odaberi **Ja sam postojeći korisnik**. **Povežite uređaje** pogled se otvara.
b. Unesite kod za sinkronizaciju generiran na prvom uređaju i odaberite **Spojiti**.
▪ Na stolnom uređaju:
a. Odaberite **Poveži uređaje**.
b. Unesite kod za sinkronizaciju generiran na prvom uređaju i odaberite **Povežite uređaje**.

6. Kada se to od vas zatraži, unesite svoju glavnu lozinku koju koristite na uređaju na kojem ste generirali kod za sinkronizaciju i odaberite **Potvrdi**.

Vaši podaci sada su sinkronizirani između ova dva uređaja. Ako imate više uređaja za povezivanje, ponovite gornje korake sa svakim uređajem. Imajte na umu da možete generirati kod za sinkronizaciju na bilo kojem od svojih povezanih uređaja.

6.4 Postavljanje automatske ispune za brži pristup uslugama na mreži

Možete brzo pristupiti svojim uslugama na mreži bez potrebe da ručno unosite podatke za prijavu.

Da biste automatski popunili svoja korisnička imena i lozinke za svoje internetske usluge, najprije trebate instalirati proširenje preglednika ili dodatak za preglednike koje upotrebljavate.

Spremište za lozinke podržava sljedeće preglednike:
- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Bilješka: Automatska ispuna trenutačno nije podržana u pregledniku Safari.

Da biste instalirali i odobrili proširenje preglednika:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. U glavnom prikazu odaberite **Spremište za lozinke**.

3. Odaberite  **Automatska ispuna**.
Otvara se prikaz **Automatska ispuna**.

4. Učinite sljedeće za sve preglednike koje upotrebljavate:
- Za Google Chrome

a. Odaberite **Instalacija proširenja za Chrome**.
b. U web-trgovini Chrome odaberite **Dodaj u Chrome** > **Dodaj proširenje**. Proširenje za **Upravitelj lozinki tvrtke F-Secure** sada je dodano u vaša proširenja preglednika.

c. Kliknite ikonu proširenja u gornjem desnom kutu preglednika i odaberite ikonu **Prikvači** pokraj **Upravitelj lozinki tvrtke F-Secure**. To olakšava pristup proširenju kada ga trebate autorizirati.
d. Da biste dovršili instalaciju proširenja preglednika, svejedno morate odobriti proširenje na sljedeći način:
1. Vratite se na Spremište za lozinke i na kraju pogleda **Automatska ispuna** odaberite **Kopiraj šifru** kako biste kopirali šifru odobrenja koja je potrebna za dovršetak postavljanja.
2. U pregledniku odaberite ikonu proširenja u gornjem desnom kutu preglednika, odaberite

Upravitelj lozinki tvrtke F-Secure i zalijepite kopiranu šifru odobrenja u prozor koji se otvori.
3. Odaberite **Autoriziraj** > **Zatvori**. Proširenje za preglednik sada je omogućeno.

▪ Za preglednik Mozilla Firefox:
a. Odaberite **Instalacija dodatka za Firefox**.
b. Na stranici DODATAKA za Firefox odaberite **Dodaj u Firefox** > **Dodaj**. Proširenje je sada dodano u vaš preglednik i ikona **Upravitelj lozinki tvrtke F-Secure** pojavljuje se u gornjem desnom kutu preglednika.
c. Da biste dovršili instalaciju proširenja preglednika, svejedno morate odobriti proširenje na sljedeći način:
1. Vratite se na Spremište za lozinke i na kraju pogleda **Automatska ispuna** odaberite **Kopiraj šifru** kako biste kopirali šifru odobrenja koja je potrebna za dovršetak postavljanja.
2. Kada ponovno pristupite pregledniku, kliknite ikonu preglednika **Upravitelj lozinki tvrtke F-Secure** u gornjem desnom kutu preglednika i zalijepite kopirani kod za autorizaciju u prozor koji se otvara.

3. Odaberite **Autoriziraj** > **Zatvori**. Proširenje za preglednik sada je omogućeno.

▪ Za Microsoft Edge
a. Odaberite **Instalacija dodatka za Edge**.
b. Na stranici dodataka za Edge odaberite **Preuzmi** > **Dodaj proširenje**. Proširenje **Upravitelj lozinki tvrtke F-Secure** sada je dodano u vaša proširenja preglednika.
c. Da biste dovršili instalaciju proširenja preglednika, svejedno morate odobriti proširenje na sljedeći način:
1. Vratite se na Spremište za lozinke i na kraju pogleda **Automatska ispuna** odaberite **Kopiraj šifru** kako biste kopirali šifru odobrenja koja je potrebna za dovršetak postavljanja.
2. U pregledniku odaberite ikonu proširenja u gornjem desnom kutu preglednika, odaberite **Upravitelj lozinki tvrtke F-Secure** i zalijepite kopiranu šifru odobrenja u prozor koji se otvori.
3. Odaberite **Autoriziraj** > **Zatvori**. Proširenje za preglednik sada je omogućeno.

Odsad nadalje, kada postavite miš na polja korisničkog imena i lozinke na stranici za prijavu mrežne usluge kojoj želite pristupiti, ikona Spremište za lozinke prikazat će se u polju. Kliknite ikonu i odaberite uslugu da biste joj pristupili.

6.5 Uvoz lozinki iz drugih upravitelja lozinki

Upute za uvoz lozinki iz drugih kompatibilnih upravitelja lozinki u Spremište za lozinke.

Možete uvesti lozinke iz drugih upravitelja lozinki koji podržavaju izvoz u format otvorenog teksta. Uvoz je moguć samo s Windows i Mac verzijama proizvoda.

Spremište za lozinke podržava uvoz lozinki iz sljedećih upravitelja lozinki:
▪ Dashlane
▪ F-Secure ID PROTECTION
▪ Google Chrome
▪ KeePassX V2

- LastPass
- Microsoft Edge
- Mozilla Firefox
- Pravi ključ

Osim toga, možete uvesti lozinke iz bilo koje druge instance Spremišta za lozinke, na primjer prethodno instalirane aplikacije A1 Sigurniji internet ili verzije davatelja usluga koja uključuje Spremište za lozinke.

Za uvoz lozinki u Spremište za lozinke:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. U glavnom prikazu odaberite **Spremište za lozinke**.

3.  > Odaberi postavke **Uvoz lozinki**.

4. S padajućeg popisa odaberite upravitelj lozinki iz kojeg želite uvesti lozinke.

Bilješka: Prikazane su upute o tome kako izvesti svoje lozinke iz odabranog upravitelja lozinki u datoteku. Da biste saznali detaljne upute o tome kako izvesti lozinke iz vašeg starog proizvoda upravitelja lozinki, pogledajte dokumentaciju proizvoda dotičnog upravitelja lozinki.

5. Nakon što izvezete i spremite datoteku lokalno, povucite je i ispustite u Spremište za lozinke, ili odaberite **Odaberite datoteku za uvoz**, pronađite datoteku i na kraju odaberite **Otvorena**.

Nakon uspješnog uvoza, prikazat će vam se broj uvezenih lozinki.

6.6 Izvoz podataka iz trezora lozinki

Ovdje možete pronaći upute o tome kako izvesti svoje podatke iz Spremišta za lozinke.

Možete izvesti svoje podatke iz Spremišta za lozinke u dekriptiranu datoteku. Izvoz je moguć samo u Windows i Mac verzijama proizvoda.

Za izvoz podataka iz vašeg Spremišta za lozinke:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. U glavnom prikazu odaberite **Spremište za lozinke**.

3.  > Odaberi postavke **Izvoz lozinki**.

4. Odaberi **Izvezi moj trezor**.
Otvara se prozor **Potvrdite glavnom lozinkom**.

5. Unesite glavnu lozinku i odaberite **Potvrdi**.

6. Odaberite mjesto na koje želite spremiti datoteku, a zatim odaberite **Izvezi**.
Prema zadanim postavkama, podaci vaših lozinki bit će spremljeni u ExportedPasswords.fsk datoteku.

7. Odaberite mjesto gdje želite spremiti datoteku, a zatim odaberite **Spremi**.
Prikazuje se broj izvezenih lozinki i put datoteke.

Bilješka: Kada izvozite svoje podatke iz Spremišta za lozinke, datoteka se izvozi kao običan tekst i stoga je drugi mogu lako čitati. Ako trebate pohraniti ovu datoteku, pohranite je na mjesto gdje joj se ne može lako pristupiti ili je teško oštetiti. Također, ne zaboravite izbrisati datoteku nakon što prenesete podatke.

6.7 Promjena glavne lozinke

Ova tema opisuje kako možete promijeniti svoju glavnu lozinku Spremišta za lozinke.

Za promjenu glavne lozinke:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. U glavnom prikazu odaberite **Spremište za lozinke**.

3. Odaberite  **Postavke** > **Promjena glavne lozinke**.

4. Unesite svoju trenutačnu glavnu lozinku.

5. Unesite svoju novu glavnu lozinku.

6. Ponovno unesite novu glavnu lozinku i odaberite **Promjena glavne lozinke**.

Vaša je glavna lozinka sada promijenjena. Nakon što promijenite glavnu lozinku na jednom uređaju, morate upotrebljavati novu lozinku na svim povezanim uređajima.

Bilješka: Ako iz bilo kojeg razloga promijenite glavnu lozinku, morate izraditi novi QR kôd za oporavak. Nijedan stari kod više neće biti valjan. Stoga pazite da QR kod za oporavak uvijek bude ažuriran i valjan za trenutačnu glavnu lozinku.

6.8 Stvaranje QR koda za oporavak za glavnu lozinku

Ova tema objašnjava kako stvoriti QR kod za oporavak glavne lozinke Spremišta za lozinke.

Važno: Preporučujemo da kreirate QR kod za oporavak glavne lozinke kada počnete koristiti Spremište za lozinke.

To je jedini način da vratite glavnu lozinku ako je zaboravite.

Za izradu koda za oporavak glavne lozinke:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. U glavnom prikazu odaberite **Spremište za lozinke**.

3.  > Odaberi postavke **Stvorite QR kod za oporavak**.
Slika koda za oporavak automatski se stvara.

4. Odaberi **Spremi** za spremanje slike.

5. Unesite glavnu lozinku i odaberite **Potvrdi**.

6. Odaberite mjesto na koje želite spremiti datoteku, a zatim odaberite **Spremi**.

7. Idite u mapu i ispišite sliku koda za oporavak.

Bilješka: Preporučujemo da spremite kod kao sliku i ispišete datoteku radi čuvanja, umjesto da je pohranite u uslugu pohrane u oblaku.

6.9 Upotreba QR koda za oporavak u svrhu oporavka vaše zaboravljene glavne lozinke

Ova tema objašnjava kako oporaviti glavnu lozinku Spremišta za lozinke pomoću QR koda za oporavak.

Važno: Glavnu lozinku možete oporaviti samo ako ste prethodno izradili QR kod za njen oporavak.

Da biste oporavili glavnu lozinku pomoću QR koda za oporavak:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. U glavnom prikazu odaberite **Spremište za lozinke**.

3. Na zaslonu za prijavu odaberite **Zaboravili ste glavnu lozinku?**
Otvorit će se pregled **Zaboravili ste glavnu lozinku?**

4. Odaberite **Uvoz**.

5. Pronađite i otvorite slikovnu datoteku QR koda za oporavak koju ste ranije stvorili.
Vaša glavna lozinka pojavit će se na zaslonu.

6. Unesite glavnu lozinku i odaberite **Otključaj**.
Otvorit će se Spremište za lozinke.

6.10 Otključavanje i zaključavanje Spremišta za lozinke

Ova tema pokazuje kako otključati Spremište za lozinke.

Važno: Kako bi vaše lozinke i osobni podaci bili sigurni, preporučujemo da zaključate Spremište za lozinke kad god ga ne upotrebljavate.

Za otključavanje Spremišta za lozinke učinite sljedeće:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. U glavnom prikazu odaberite **Spremište za lozinke**.

3. Unesite glavnu lozinku i odaberite **Otključaj**.

Bilješka: Prema zadanim postavkama Spremište za lozinke automatski se zaključava nakon pet minuta.

Za postavljanje vremena nakon kojeg se Spremište za lozinke zaključava, idite u  **Postavke** > **Automatsko zaključavanje** i odaberite vrijeme. Opcije su 5 minuta, 15 minuta, 30 minuta, 60 minuta, 10 sati i 1 tjedan.

4. Za ručno zaključavanje Sefa za lozinke, odaberite  **Zaključaj** s lijeve navigacije.

7 Nadzor ID-a

Uz **Nadzor ID-a** možete dodati adrese e-pošte i druge stavke za praćenje i dobiti smjernice o tome što učiniti ako je došlo do curenja vaših osobnih podataka tijekom povrede sigurnosti podataka.

Bilješka: Ta značajka nije dostupna u svim verzijama aplikacije.

Da biste počeli koristiti Nadzor ID-ja, morate dodati adresu e-pošte koju želite pratiti, a zatim potvrditi tu adresu. Ta prva adresa koristi se kao primarni kontaktni podatak i sve obavijesti o narušavanju sigurnosti šalju se na tu adresu.

Nakon što unesete svoju adresu e-pošte, aplikacija provjerava pojavljuje li se u nekim curenjima podataka i obavještava vas o rezultatu. Potpuno izvješće vidljivo je tek nakon što potvrdite svoju adresu.

Poruke e-pošte s obavijestima o povredi sigurnosti sadrže informacije o tome koja su osobna podatkovna sredstva (PII) povezana s povredom sigurnosti; o kakvoj se povredi radilo; koja je tvrtka ili organizacija bila povrijeđena; kada se povreda dogodila; te koja su druga osobna podatkovna sredstva povezana s praćenom adresom e-pošte, poput lozinki, brojeva kreditnih kartica, adrese stanovanja i slično.

Možete dodati do 3 stavki svake vrste za praćenje; to jest, 3 adresa e-pošte, 3 platnih kartica, 3 telefonskih brojeva itd.

7.1 Dodavanje stavki za praćenje

Ova tema opisuje kako dodati stavke za praćenje.

Prva stavka za nadzor koju dodate mora biti vaša adresa e-pošte. Nakon što dodate svoju adresu e-pošte za nadzor, možete dodati i druge stavke, kao što su korisnička imena i brojevi kreditnih kartica za nadzor. Vaša adresa e-pošte je također mjesto na koje se šalju obavijesti ako dođe do povrede sigurnosti vaših podataka.

Bilješka: Obavezno potvrdite svoju kontaktnu adresu e-pošte. Ako još niste potvrdili svoju adresu, ne možete vidjeti detaljne informacije o kompromitiranim podacima ili preporučenim radnjama.

Za dodavanje više stavki za praćenje:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. U glavnom prikazu odaberite **Nadzor ID-a**.

3. U pregledu **Nadzor ID-a**, odaberite **Praćene stavke**.
Otvara se pregled **Praćene stavke**.

4. Odaberite **Dodaj novo**.

Bilješka: Ako još niste dodali adresu e-pošte za nadzor, aplikacija će vas prvo zamoliti da dodate adresu e-pošte za nadzor.
Otvara se dijaloški okvir **Dodaj novo** s popisom svih dostupnih vrsta informacija koje možete odabrati.

5. Odaberite vrstu stavke koju želite dodati za praćenje.
Otvara se novi prikaz u koji možete unijeti relevantne podatke.

6. Unesite tražene podatke i odaberite **Spremi**.
Potrebne informacije variraju ovisno o vrsti odabrane stavke.

Nadzor započinje traženjem povreda sigurnosti vaših osobnih podataka i prikazuje vam rezultat pretrage.

Važno: Ako su vaši podaci bili izloženi povredi podataka, potičemo vas da izvršite preporučene radnje što je prije moguće kako biste uklonili rizik od zlouporabe vaših podataka.

Da biste vidjeli detalje o svojim izloženim osobnim podacima i što biste trebali učiniti, odaberite određenu povredu sigurnosti navedenu u prikazu **Popisa povrede sigurnosti** > **Nadzora ID-a**.

7.2 Brisanje nadziranih stavki

Ova tema opisuje kako izbrisati nadziranu stavku.

Bilješka: Ne možete izravno uređivati stavku koja je dodana za praćenje. Ako trebate urediti postojeću praćenu stavku, prvo je izbrišite, a zatim ponovno dodajte za praćenje.

Za brisanje praćene stavke:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. U glavnom prikazu odaberite **Nadzor ID-a**.

3. U prikazu **Nadzor ID-a** odaberite **Nadzirane stavke**.
Otvara se prikaz **Nadzirane stavke** u kojem su navedene sve nadzirane stavke.

4. Odaberite stavku koju želite izbrisati, a zatim odaberite ikonu smeća () u gornjem desnom kutu prikaza stavke.
Aplikacija vas traži da potvrdite da želite prestati pratiti ovu stavku.

5. Da biste potvrdili da želite prestati pratiti stavku, odaberite **Zaustavi praćenje**.
Stavka nestaje iz praćenih stavki.

Bilješka: Da biste izbrisali svoju kontaktnu adresu e-pošte iz nadzora, prvo morate izbrisati sve ostale nadzirane stavke.

7.3 Promjena adrese e-pošte za kontakt

Čim se bilo koja od vaših praćenih stavki pojavi u povredi sigurnosti podataka primit ćete obavijesti na svoju adresu e-pošte za kontakt.

Prva adresa e-pošte koju dodate kao praćenu stavku automatski postaje vaša adresa e-pošte za kontakt.

Za promjenu adrese e-pošte za kontakt:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. U glavnom prikazu odaberite **Nadzor ID-a**.

3. U prikazu **Nadzor ID-a** odaberite **Nadzirane stavke**.
Otvara se popis vaših praćenih stavki.

4. Ako još niste dodali adresu e-pošte koju želite koristiti kao novu kontaktnu adresu e-pošte u praćenim stavkama, učinite sljedeće:
a) Odaberite **Dodaj novu** > **e-poštu**, zatim unesite adresu e-pošte i odaberite **Spremi**.
Na adresu koju ste unijeli šalje se e-poruka s poveznicom za potvrdu.
b) Otvorite e-poštu i potvrdite svoju adresu e-pošte.

Nakon potvrde, adresa e-pošte se može upotrebljavati kao vaša adresa e-pošte za kontakt.

5. U prikazu **Nadzirane stavke** s odabranom adresom e-pošte odaberite ⋮ pored adrese e-pošte, a zatim odaberite **Označi kao primarni kontakt**.
Vaša nova adresa e-pošte za kontakt sada je u upotrebi.

Bilješka: Za uređivanje adrese e-pošte za kontakt ili brisanje iz praćenja, trebate izbrisati sve druge praćene stavke, ako ih ima, prije nego što ćete moći urediti ili izbrisati adresu e-pošte za kontakt.

8 Zaštita privatnosti

Ovaj odjeljak objašnjava što je A1 Sigurniji internet Security Cloud i kako možete doprinijeti anonimnim podacima i pomoći nam da poboljšamo proizvod.

8.1 Sigurnosni podaci

Usluga A1 Sigurniji internet šalje upite o potencijalnim zlonamjernim aktivnostima ili o zaštićenim uređajima *Sigurnosni oblak*.

A1 Sigurniji internet Security Cloud sustav je temeljen na oblaku za analizu kibernetičkih prijetnji kojim upravlja tvrtka FSecure.

Prikupljamo minimalnu količinu podataka kako bismo vam pružili sigurnosne usluge na koje ste se pretplatili i pružili visokokvalitetnu zaštitu za naše korisnike.

Uz A1 Sigurniji internet Security Cloud, A1 Sigurniji internet može održavati ažuran pregled globalnog krajolika prijetnji i zaštititi naše klijente od novih prijetnji u trenutku kada se prvi put otkriju.

Sigurnosni oblak prikuplja samo podatke koji mogu sadržavati informacije o datotekama ili web stranicama koje je A1 Sigurniji internet blokirao iz sigurnosnih razloga. Sigurnosni podaci ne koriste se u personalizirane marketinške svrhe.

Slanje podataka

Kao suradnik, dopuštate Sigurnosnom oblaku da čuva sigurnosne podatke koji nam pomažu ojačati vašu zaštitu od novih prijetnji. Podaci prikupljeni na ovaj način čuvaju se samo ograničeno vrijeme i brišu se nakon tog razdoblja.

1. Odaberite ikonu proizvoda na traci izbornika.

2. Odaberite **Postavke**.

3. Odaberite karticu **Privatnost**.

4. Odaberite ikonu zaključavanja u donjem lijevom kutu.
Za promjenu ovih postavki potrebna su vam administrativna prava.

5. Odaberi **Omogućite dublju analizu**.

8.2 Poboljšanje proizvoda

Slanjem podataka o upotrebi možete nam pomoći da poboljšamo proizvod.

Slanje podataka o upotrebi:

1. Odaberite ikonu proizvoda na traci izbornika.

2. Odaberite **Postavke**.

3. Odaberite karticu **Privatnost**.

4. Odaberite ikonu zaključavanja u donjem lijevom kutu.
Za promjenu ovih postavki potrebna su vam administrativna prava.

5. Odaberi **Šalji nepersonalizirane podatke o korištenju** .

Bilješka: Možete pročitati našu Izjavu o privatnosti ovdje.

9 Tehnička podrška

Ovdje možete pronaći informacije koje će vam pomoći da riješite tehničke probleme.

9.1 Gdje pronaći ID računa?

Ako nas trebate kontaktirati, naša korisnička podrška može vas zatražiti ID vašeg računa.

Da biste saznali svoj ID računa:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. U glavnom prikazu odaberite  u gornjem desnom kutu.

3. Odaberite **Oko**.
ID računa možete pronaći ispod informacija o verziji proizvoda.

9.2 Gdje mogu pronaći informacije o verziji proizvoda?

Ako nas trebate kontaktirati, naša korisnička podrška može vas zatražiti informacije o verziji vašeg proizvoda.

Da biste pogledali aktualne podatke o verziji, učinite sljedeće:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. U glavnom prikazu odaberite  u gornjem desnom kutu.

3. Odaberi **Oko**.

Osim informacija o verziji proizvoda, prozor **Informacije** sadrži informacije o vašem ID-u računa i najnovijoj verziji baze podataka proizvoda.

9.3 Korištenje alata za podršku

Prije nego što se obratite podršci, pokrenite alat za podršku da biste prikupili osnovne podatke o hardveru, operacijskom sustavu, mrežnoj konfiguraciji i instaliranom softveru.

Ako imate tehničkih problema sa svojim sigurnosnim proizvodom, naša korisnička podrška može tražiti da izradite i pošaljete datoteku FSDIAG našoj tehničkoj podršci. Datoteka sadrži informacije koje se mogu upotrebljavati za rješavanje problema specifičnih za vaše računalo.

Datoteku možete izraditi pomoću alata za podršku. Alat prikuplja informacije o vašem sustavu i njegovoj konfiguraciji. Informacije uključuju pojedinosti o proizvodu, zapisnike operativnog sustava i postavke sustava. Imajte na umu da dio informacija može biti povjerljiv. Prikupljene informacije pohranjuju se u datoteku koja se sprema na radnu površinu vašeg računala.

Da biste pokrenuli alat za podršku, učinite sljedeće:

1. Kliknite ikonu proizvoda na traci izbornika i odaberite **Postavke**.

2. Odaberite karticu **Podrška**, a zatim odaberite **Otvori alat za podršku** .

3. Odaberite **Pokreni dijagnostiku** u prozoru **Alat za podršku**.

Bilješka: Potrebna su vam administratorska prava za pokretanje alata.

4. Unesite administratorsku lozinku za svoje računalo.
Pokrenut će se alat za podršku i prikazati tijek prikupljanja podataka.

5. Kada je prikupljanje podataka završeno, odaberite gdje želite spremiti dobivenu arhivu tar.gz i zatim odaberite **Spremi**.
Alat za podršku otvara prozor aplikacije **Finder** u kojoj se prikazuje spremljena datoteka.

6. Kada se to od vas zatraži, pošaljite datoteku korisničkoj podršci.

Savjet: Ako ne možete pristupiti alatu za podršku putem samog proizvoda, idite na web-stranicu Alati za podršku i pod **Alat za podršku (FSDIAG) za Mac** odaberite **Preuzmi** i spremite datoteku Support Tool.zip, na primjer u mapu Preuzimanja. Dvaput kliknite datoteku, zatim kliknite **Alat za podršku** i odaberite **Pokreni dijagnostiku**.

9.4 Problemi otklanjanja pogrešaka proizvoda

Zapisivanje otklanjanja pogrešaka pomaže našoj korisničkoj podršci da analizira i riješi probleme u proizvodu, ako ih ima.

Bilješka: Uključite zapisivanje otklanjanja pogrešaka samo kada to zatraži naš agent za korisničku podršku.

Dok alat za podršku prikuplja puno vrijednih informacija, također izostavlja različite informacije prema zadanim postavkama zbog privatnosti i performansi. Da biste omogućili potpuno bilježenje ispravljanja pogrešaka, morate instalirati poseban konfiguracijski profil prije reproduciranja problema i pokretanja alata za podršku. Konfiguracijski profil automatski istječe nakon 14 dana.

Bilježenje otklanjanja pogrešaka može imati određeni utjecaj na izvedbu jer proizvod pohranjuje više podataka bilježenja na vaše računalo.

1. Kliknite ikonu proizvoda na traci izbornika i odaberite **Postavke**.

2. Odaberite karticu **Podrška**.

3. Odaberite **Omogući bilježenje otklanjanja pogrešaka**.

Bilješka: Potrebna su vam administratorska prava za pokretanje alata.
Od vas se traži da pregledate i instalirate profil.

4. Potvrdite i instalirajte novi profil.
Za macOS 15 (Sequoia) i novije verzije:
a) Otvorite aplikaciju **Postavke sustava**.
b) Odaberite **Općenito** > **Upravljanje uređajem**
c) Dvaput kliknite unos **Bilježenje otklanjanja pogrešaka A1 Sigurniji internet**, zatim slijedite upute na zaslonu.
Za macOS 13 (Ventura) i 14 (Sonoma):
a) Otvorite aplikaciju **Postavke sustava**.
b) Izaberite **Privatnost i sigurnost** > **Profili**.
c) Dvaput kliknite na unos **Bilježenje otklanjanja pogrešaka A1 Sigurniji internet**, a zatim kliknite **Instalirati**.
Za macOS 12 (Monterey):
a) Otvorite aplikaciju **Postavke sustava**.
b) Kliknite na ikonu **Profili**.
c) Odaberite unos **Bilježenje otklanjanja pogrešaka A1 Sigurniji internet**, zatim kliknite **Instaliraj** za prikaz detalja profila.
d) Kliknite **Instaliraj** za potvrdu.
Zapisivanje otklanjanja pogrešaka ostaje aktivno 14 dana.

Ako želite isključiti bilježenje otklanjanja pogrešaka prije isteka 14 dana, idite na **Postavke sustava** > **Privatnost i sigurnost** > **Profili** i ručno uklonite profil.

Na starijim verzijama macOS-a (prethodnim od 13), idite na **Postavke sustava** > **Profili** za ručno uklanjanje profila.

9.5 Ponovno postavljanje predmemorije reputacije

Ova tema opisuje kako osigurati da imate najnovije podatke iz Security Cloud A1 Sigurnijeg interneta.

Ako želite biti sigurni da imate najnovije informacije o datotekama i reputaciji web stranica iz našeg Security Cloud, ponovno postavite predmemoriju reputacije:

1. Kliknite ikonu proizvoda na traci izbornika i odaberite **Postavke**.

2. Odaberite karticu **Podrška**.

3. Izaberite **Ponovno postavi predmemoriju reputacije**.

Bilješka: Za ponovno postavljanje predmemorije potrebna su vam administratorska prava.

9.6 Telefonske prijevare i što učiniti ako mislite da ste meta

Telefonske prijevare nažalost su u porastu jer prevaranti koriste društveni inženjering kako bi ciljali na svoje žrtve.

Ova vam tema pomaže identificirati te pozive, a u najgorem slučaju – ako ste bili ciljani – daje vam neke informacije o tome što učiniti sljedeće.

Što su telefonske prijevare?

Telefonski pozivi mogu započeti ili kao pozivi upućeni na krivi broj ili putem oglasa ili veze koja pokreće skočni prozor na vašem računalu. Ovi vas skočni prozori zatim pozivaju da nazovete oglašeni broj tehničke podrške. Skočni prozori mogu se pojaviti iznenada i nije ih se tako lako riješiti.

Kako mogu prepoznati telefonsku prijevaru?

Ove vrste poziva obično slijede određeni obrazac: prevaranti obično tvrde da vaše računalo ima problem, recimo virus koji zapravo ne postoji, a zatim vas prevarom navedu da platite uslugu koja također ne postoji. Uhvate vas nespremne i iskorištavaju vaše osjećaje. Evo osnovnog scenarija:

- Telefonski prevaranti tvrde da rade u poznatoj tvrtki, poput Microsofta, vašoj banci ili čak tvrtki vašeg mrežnog operatera. Opušteni ste s obzirom da koriste ugledno ime. Također se doimaju upućenima i koriste tehničke izraze, što ih čini legitimnima i uvjerljivima.
- Budući da se rizik čini stvarnim i da ste zabrinuti zbog mogućih računalnih virusa, prevarantima dajete pristup vašem računalu. Uvjeravaju vas da im dopustite da instaliraju aplikaciju koja im omogućuje pristup vašem računalu pomoću alata za daljinski pristup.
- Nakon što prevaranti dobiju pristup vašem računalu, pretvaraju se da rješavaju virus, a mogu tražiti i vaše osobne vjerodajnice. Kada prevaranti "riješe" problem, traže od vas da se prijavite u na svoje internetsko bankarstvo ili da ispunite obrazac s podacima o svojoj kreditnoj kartici. Prevaranti vam naplate lažnu uslugu, a cijena je na kraju mnogo veća nego što ste mislili da će biti. Zapravo, teško je znati koliko vam stvarno naplaćuju.

Što učiniti ako mislite da ste prevareni

Ako mislite da ste prevareni i prepoznajete gore opisan scenarij, učinite sljedeće:

- Djelujte bez odlaganja.
- Odmah se obratite tvrtki ili banci koja vam je izdala kreditnu karticu, prijavite prijevaru i otkažite sve bankovne ili kreditne kartice. Ako reagirate odmah, možda će čak moći zaustaviti transakciju i poništiti troškove.
- Prijavite prijevaru nadležnom tijelu.
- Promijenite sve svoje lozinke na svakom web-mjestu i usluzi koji bi mogli biti pogođeni.
- Deinstalirajte sav nepoznati softver treće strane.
- Pokrenite potpuno pregledavanje na računalu: otvorite svoj sigurnosni proizvod, a zatim odaberite **Zaštita uređaja** > **Potpuno pregledavanje računala**.

Stvari koje trebate zapamtiti o neželjenim telefonskim pozivima

- Ako primite ovakav poziv, razmislite: jesam li ja to tražio?

Bilješka: Obično će vas služba za korisničku podršku nazvati ako ste je već kontaktirali i izradili zahtjev za podršku.
▪ Udaljene sesije obično se koriste u tehničkoj podršci kao način pomoći u rješavanju problema.

Zapamtite: Dopustite udaljene sesije samo s osobama ili tvrtkama koje poznajete i kojima vjerujete. Udaljene sesije dopustite samo ako ste prethodno kontaktirali svojeg davatelja usluga i kod njega imate važeći slučaj podrške. Također, čuvajte svoje podatke za daljinski pristup kao što biste čuvali bilo koju drugu lozinku.
▪ Osobama koje ne poznajete nikada nemojte pružiti pristup svom uređaju. Odobravanje daljinskog pristupa prevarantima znači da zapravo predajete administratorska prava za svoje računalo. Čak i ako imate instaliran antivirusni softver, to vas više ne može zaštititi jer prevaranti preuzimaju kontrolu nad vašim računalom.
▪ Tvrtka Microsoft obavijestila je svoje korisnike da nikada ne uključuju telefonske brojeve u poruke o pogreškama ili poruke upozorenja svog softvera.
▪ Nikada nemojte svojevoljno pružati osobne vjerodajnice ili podatke o kreditnoj kartici.
▪ Odmah prekinite poziv.
▪ Ovakvi su telefonski pozivi protuzakoniti, a ako ste u nedoumici, obratite se nadležnom tijelu koje se bavi prijevarama i podnesite prijavu.

Kako sigurnosni proizvod može pomoći?

S instaliranim sigurnosnim proizvodom vaše je računalo zaštićeno od virusa, trojanskih programa i ucjenjivačkog softvera. Zaštita od pregledavanja, zaštita od bankarstva i značajke zaštite alata za daljinski pristup dodaju još jedan sloj zaštite i brinu se za to da možete sigurno pregledavati i vršiti svoje aktivnosti bankarstva na mreži.

Ako ste bili meta i već imate instaliran sigurnosni proizvod, možete odmah pokrenuti potpuno skeniranje računala kako biste otkrili sve aplikacije koje su možda instalirali prevaranti; te se aplikacije nazivaju potencijalno neželjenim aplikacijama (PUA). Međutim, proizvod vas ne može zaštititi od ovih vrsta telefonskih prijevara.

Budite oprezni i ostanite sigurni.