# Internet zaštita

za Android

Jedan za sve.

# Sadržaj

1 Uvod u aplikaciju A1 Sigurniji internet ..... 5
1.1 Sistemski preduvjeti ..... 6
1.2 Gdje mogu kupiti A1 Sigurniji internet? ..... 6
2 Početak rada ..... 7
2.1 Instalacija aplikacije na vaš uređaj ..... 7
2.1.1 Kako aplikacija radi s privatnim prostorima ..... 8
2.1.2 Deinstaliranje aplikacije s vašeg uređaja ..... 8
2.2 Pristupanje informacijama o vašem računu ..... 9
2.3 Obavijesti o potrebnim i preporučenim zadacima ..... 9
2.4 Upravljanje postavkama proizvoda ..... 10
2.4.1 Pristupanje postavkama proizvoda ..... 10
2.5 Prikaz statusa vašeg proizvoda ..... 11
2.5.1 Ikone stanja zaštite ..... 11
2.5.2 Prikaz statistike zaštite ..... 11
2.5.3 Promjena postavki obavijesti u aplikaciji ..... 12
2.5.4 Brinemo se da vaša zaštita i dalje radi ..... 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? ..... 18
3.3.2 Prestanite dijeliti zaštitu s članom obitelji ili prijateljem ..... 19

3.4 Oslobađanje licence s uređaja ....19
3.5 Premještanje aplikacije A1 Sigurniji internet sa vašeg starog uređaja na novi ....20
4 Zaštita uređaja ....21
4.1 Pokretanje ručnog skeniranja ....21
4.2 Uključivanje automatskog skeniranja ....22
4.3 Upotreba mrežne veze s ograničenim prometom ....22
4.4 Provjera rezultata skeniranja ....23
4.5 Pregled dopuštenja aplikacije na vašem uređaju ....23
4.6 Zaštita uređaja ....24
5 Zaštita od prijevare ....25
5.1 Postavljanje proširenja preglednika Chrome ....25
5.2 Dopuštanje određenih web-stranica ....26
5.3 Prikaz sigurnosnih ocjena za web stranice ....27
5.4 Nailazite na blokiranu web stranicu ....27
5.5 Zaštita od prijevara tekstualnim porukama ....27
5.6 Provjerite je li vaša Wi-Fi veza sigurna ....28
5.7 Provjera sadržaja zbog prijevara ....29
5.7.1 Primjeri kategorija prijevara ....30
6 Spremište za lozinke ....33
6.1 Početak rada sa Spremištem za lozinke ....33
6.2 Korištenje Spremišta za lozinke ....34
6.2.1 Pohranjivanje nove lozinke na mobilni uređaj ....34
6.2.2 Pohranjivanje podataka o platnoj kartici na mobilni uređaj ....35
6.2.3 Uređivanje postojećih podataka ....36
6.2.4 Brisanje unosa ....36
6.2.5 Dopuštanje aplikaciji da generira novu lozinku za postojeći unos ....36
6.2.6 Pristup vašim starim lozinkama ....37

6.3 Povezivanje uređaja za sinkronizaciju vaših podataka iz Spremišta za lozinke na svim vašim uređajima ....38
6.4 Postavljanje automatskog popunjavanja za brži pristup aplikacijama i web stranicama ....39
6.5 Promjena glavne lozinke ....39
6.6 Stvaranje QR koda za oporavak za glavnu lozinku ....40
6.7 Upotreba QR koda za oporavak u svrhu oporavka vaše zaboravljene glavne lozinke ....41
6.8 Otključavanje i zaključavanje Spremišta za lozinke ....41
6.9 Korištenje biometrijske provjere autentičnosti za otključavanje Spremišta za lozinke ....42
7 Nadzor ID-a ....43
7.1 Dodavanje stavki za praćenje ....43
7.2 Brisanje nadziranih stavki ....44
7.3 Promjena adrese e-pošte za kontakt ....45
8 Tehnička podrška ....46
8.1 Gdje se nalaze podaci o verziji proizvoda? ....46
8.2 Slanje zapisa podršci ....46
8.3 Telefonske prijevare i što učiniti ako mislite da ste meta ....47

# 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
- Zaštititi svoje osobne podatke i osobne podatke svoje obitelji od računalnog kriminala.

## 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 aplikacije na vaš 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 Google Playa, 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 Google Playa 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) Pratite upute za instalaciju poslane na uređaj.

**5.** Kada instalacija završi, otvorite aplikaciju.

**6.** Ako se slažete s Licencnim uvjetima za krajnjeg korisnika, odaberite **Prihvati i nastavi**. Od vas se može tražiti da se prijavite na svoj račun kada prvi put pokrenete aplikaciju.

**7.** Dok postavljate zaštitu za sebe, odaberite **Nastavi** kako biste dovršili postavljanje zaštite uređaja.

**Važno:** Kako biste mogli zaštititi svoj uređaj i veze, aplikacija zahtijeva da dopustite pristup fotografijama, medijima i datotekama na vašem uređaju. Sada ste postavili zaštitu za svoj uređaj.

### 2.1.1 Kako aplikacija radi s privatnim prostorima

Android 15 predstavio je značajku privatnog prostora koja može utjecati na funkcionalnost instaliranih aplikacija.

**Važno:** Privatni prostor je dodatna značajka unutar operativnog sustava Android. Ako ne koristite ovu značajku na svom uređaju, ne morate poduzimati ništa.

Privatni prostor omogućava izolaciju određenih aplikacija i njihovih podataka na vašem uređaju sa sustavom Android. To znači da, kada instalirate aplikaciju u svoj privatni prostor, ona radi samo kada je vaš privatni prostor otključan i ne može pristupiti podacima ili aplikacijama koje se nalaze u vašem glavnom prostoru. Možete upotrebljavati zasebni Google račun za privatni prostor, ali također možete upotrebljavati isti račun kao svoj glavni profil uređaja.

Ograničeni pristup između prostora također utječe na aplikaciju A1 Sigurniji internet. Na primjer:

▪ Zaštita uređaja može skenirati samo aplikacije i datoteke unutar prostora u kojem instalirate aplikaciju.

▪ Biometrija koja se koristi za Sef možda neće funkcionirati.

▪ Zaštita za Chrome radi samo s preglednikom Chrome pokrenutim iz prostora u kojem instalirate aplikaciju.

▪ VPN radi samo za aplikacije instalirane u istom prostoru kao i aplikacija A1 Sigurniji internet, uključujući preglednike.

▪ Obavijesti aplikacija možda neće raditi.

Preporučujemo da instalirate aplikaciju A1 Sigurniji internet u glavnom prostoru vašeg uređaja. Da biste upotrebljavali značajke zaštite u glavnom i u privatnom prostoru, morate također instalirati aplikaciju u svom privatnom prostoru, što zahtijeva upotrebu druge licence.

Za više informacija o privatnom prostoru i upute za postavljanje i upotrebu, pogledajte Centar za pomoć za uređaje sa sustavom Android.

### 2.1.2 Deinstaliranje aplikacije s vašeg uređaja

Kada deinstalirate aplikaciju, izgubit ćete sve spremljene podatke i postavke, a uređaj više neće biti zaštićen.

Da biste deinstalirali aplikaciju sa svog uređaja:

**1.** Otvorite aplikaciju A1 Sigurniji internet.

**2.** Na glavnom prikazu proizvoda odaberite ikonu profila u gornjem desnom kutu > **Postavke**.

Otvara se prikaz **Postavke** s popisom svih značajki za zaštitu koje su vam trenutačno aktivne.

**3.** U odjeljku **Ostale postavke** odaberite **Deinstaliraj** > **U redu**.

Aplikacija je uklonjena s vašeg uređaja. Ne zaboravite također osloboditi njezinu licencu ukoliko ju i dalje želite koristiti. Tek tada možete ponovno upotrebljavati izdanu licencu na drugom uređaju.
Deinstalacijom aplikacije A1 Sigurniji internet nije deaktiviran te se naplata i dalje nastavlja.

## 2.2 Pristupanje informacijama o vašem računu

Možete jednostavno pristupiti podacima o svom računu putem glavnog prikaza aplikacije.

Ako želite provjeriti detalje svog računa, poput imena vlasnika računa i adrese e-pošte koja se koristi za prijavu na račun, učinite sljedeće:
**1.** Otvorite aplikaciju A1 Sigurniji internet.
**2.** Odaberite ikonu profila u gornjem desnom kutu zaslona. 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 karticu **Svi zadaci**.

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.<br>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.

Svaka se značajka proizvoda može dinamički uključiti ili isključiti u aplikaciji, ovisno o vašoj pretplati.

Dopuštenja aplikacije traže se kada se značajka uključi prvi put, a ne na prvom pokretanju aplikacije.

Međutim, ako želite, možete napraviti vlastite prilagodbe postavki.

## 2.4.1 Pristupanje postavkama proizvoda

Možete brzo pristupiti postavkama proizvoda kako biste prilagodili značajke zaštite svojim potrebama.

Postavkama možete pristupiti na sljedeći način:

**1.** Otvorite aplikaciju A1 Sigurniji internet.

**2.** Na glavnom prikazu proizvoda odaberite ikonu profila > **Postavke**.

Otvara se prikaz **Postavke** s popisom svih značajki za zaštitu koje su vam trenutačno aktivne.

**3.** Odaberite značajku da biste vidjeli njezine trenutačne postavke.

U prikazu **Postavke** navedene su i druge postavke proizvoda, kao što su analitika upotrebe i obavijesti, koje ćete možda željeti podesiti.

Postavkama možete pristupiti i putem glavne stranice proizvoda tako da prvo odaberete značajku zaštite, a zatim ikonu izbornika Postavke u gornjem desnom kutu zaslona.

## 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.<br>Značajke su uključene i pravilno funkcioniraju. |
|  | Upozorenje | Vaš uređaj nije u potpunosti zaštićen.<br>Proizvod traži vašu pažnju, na primjer zato što dugo nije ažuriran ili je neka sigurnosna značajka isključena. |
|  | Opasnost | Vaš uređaj nije zaštićen.<br>Ovaj proizvod zahtijeva trenutačnu akciju, na primjer zato što je kritična značajka onemogućena ili je pretplata istekla. |

### 2.5.2 Prikaz statistike zaštite

Proizvod prikuplja statističke podatke kako bi vam pokazao kako je zaštitio vaš uređaj i vaše pregledavanje weba.

Da biste vidjeli kako je proizvod zaštitio vaš uređaj:

**1.** Otvorite aplikaciju A1 Sigurniji internet.

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

U prikazu **Zaštita uređaja** možete vidjeti vrijeme posljednjeg potpunog pregledavanja i ukupan broj provjerenih datoteka i aplikacija.

Ako želite vidjeti informacije o ranijim pregledavanjima, odaberite **Povijest pregledavanja**, a zatim dodirnite bilo koje od ranijih pregledavanja da biste vidjeli pojedinosti o njemu.

Da biste vidjeli kako je proizvod zaštitio vaše pregledavanje:

**1.** Otvorite aplikaciju A1 Sigurniji internet.

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

U prikazu **Zaštita od prijevara** možete vidjeti broj blokiranih štetnih web-mjesta.

## 2.5.3 Promjena postavki obavijesti u aplikaciji

Aplikacija vam šalje obavijesti o određenim aktivnostima u aplikaciji.

Možete odabrati koje će vam sigurnosne obavijesti aplikacija prikazivati ili isključiti sve obavijesti.

Neke od obavijesti aplikacije uvijek su vidljive, druge nestaju nakon određenog vremena. Prema

zadanim postavkama uključene su obavijesti koje dolaze iz aplikacije. Preporučujemo da ove zadane postavke ostanu uključene kako biste osigurali najbolju zaštitu.

Važne obavijesti, primjerice obavijest o tome da je određena instalirana aplikacija štetna, prikazuju se čak i ako isključite obavijesti.

Kao što je slučaj sa svim aplikacijama na uređajima sa sustavom Android, možete prilagoditi postavke obavijesti za aplikaciju. Imajte na umu da se način na koji se upravlja postavkama može razlikovati u različitim verzijama sustava Android.

Da biste pristupili postavkama obavijesti za aplikaciju, učinite sljedeće:

**1.** Otvorite aplikaciju A1 Sigurniji internet.

**2.** Odaberite ikonu profila u gornjem desnom kutu zaslona.

**3.** Odaberite **Postavke**.

**4.** Pod opcijom **Obavijesti** odaberite vezu **Obavijesti aplikacije**.

Otvara se stranica **Obavijesti aplikacije** za aplikaciju A1 Sigurniji internet. Prema zadanim postavkama dopuštene su obavijesti aplikacije.

**5.** Ako želite isključiti sve obavijesti, ovisno o verziji sustava Android, učinite nešto od sljedećeg:

- Dodirnite **Prikaži obavijesti**.
- Dodirnite **Dopusti obavijesti**.

**6.** Ako popis svih dostupnih obavijesti nije vidljiv, odaberite **Kategorije obavijesti**.

Pojavljuje se popis s različitim vrstama obavijesti koje se odnose na aplikaciju A1 Sigurniji internet.

**7.** Ako želite, možete prilagoditi postavke obavijesti za svaku obavijest zasebno. Dostupne opcije ovise o verziji sustava Android s kojom vaš uređaj radi. Pogledajte dokumentaciju uređaja za detaljnije upute o tome kako prilagoditi obavijesti vlastitim potrebama.

### 2.5.4 Brinemo se da vaša zaštita i dalje radi

Ako isključite aplikaciju putem postavki uređaja ili obavijesti, više nećete biti zaštićeni od mrežnih prijetnji i štetnih aplikacija.

Ako zaustavite aplikaciju, bilo u postavkama uređaja ili putem obavijesti o statusu, ona se neće automatski ponovno pokrenuti. Umjesto toga, u potpunosti isključuje sve usluge zaštite, uključujući automatsko skeniranje, zaštitu pregledavanja i ograničenja Pravila za obitelj. To vas čini ranjivima na mrežne prijetnje i štetne datoteke ili aplikacije na vašem uređaju.

Stoga preporučujemo da ne zaustavljate aplikaciju osim ako je to potrebno za rješavanje problema na vašem uređaju ili kao privremena mjera. Ako trebate zaustaviti aplikaciju, preporučujemo da je ponovno pokrenete u postavkama uređaja što je prije moguće kako bi vaš uređaj ostao zaštićen.

## 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 Sefa.

Za odjavu iz aplikacije:

**1.** Otvorite aplikaciju A1 Sigurniji internet.

**2.** U glavnom prikazu dodirnite u gornjem desnom kutu, zatim na dnu odaberite **Odjava**. Imajte na umu da će se vaše postavke i podaci izbrisati nakon što se odjavite.

**3.** Kako biste potvrdili da se želite odjaviti, odaberite **Odjava** u skočnom prozoru. Sada ste odjavljeni iz aplikacije na ovom uređaju.

Vaš uređaj više nije zaštićen, a postavke Pravila za obitelj, ako postoje, ne rade.

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.

## 3.1 Zaštita vlastitih uređaja

Ova tema opisuje kako početi štititi svoje druge mobilne uređaje.

Za postavljanje zaštite za vlastiti uređaj:

**1.** Otvorite aplikaciju A1 Sigurniji internet.

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

**3.** U prikazu **Osobe i uređaji** odaberite **+ Dodaj uređaj**.

**4.** Odaberi **Moj uređaj** > **Nastaviti**.

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

**6.** 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.

**7.** Preuzmite i instalirajte aplikaciju na uređaj.

**8.** Kada instalacija završi, otvorite aplikaciju.

**9.** Ako se slažete s Uvjetima licence za krajnjeg korisnika, odaberite **Prihvati i nastavi**.

**10.** Dok postavljate zaštitu za sebe, odaberite **Nastavi** kako biste dovršili postavljanje zaštite uređaja.

**Važno:** Kako biste mogli zaštititi svoj uređaj i veze, aplikacija zahtijeva da dopustite pristup fotografijama, medijima i datotekama na vašem uređaju.

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

### 3.2.1 Postavljanje filtriranja sadržaja za dijete

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

Kada prvi put postavite filtriranje sadržaja na djetetovom uređaju, od vas će se tražiti da postavite PIN kod koji osigurava da vaše dijete ne može promijeniti postavke koje odlučite koristiti.

**Bilješka:** Filtriranje sadržaja koristi VPN vezu za blokiranje neželjenog sadržaja koji odaberete. Ako uključite VPN značajku, filtriranje sadržaja neće raditi.

Za postavljanje zaštite za vaše dijete:

**1.** Otvorite aplikaciju A1 Sigurniji internet.

**2.** U glavnom prikazu odaberite **Filtriranje sadržaja**.

**3.** Odaberi **Započnite**.
Ako prvi put postavljate filtriranje sadržaja, aplikacija će vas zamoliti da kreirate PIN Obiteljske zaštite.
a) Unesite PIN koji lako možete zapamtiti, a zatim odaberite **Nastavi**.
b) Ponovite uneseni PIN, a zatim odaberite **Nastavi**.
Nakon što postavite ili unesete PIN Obiteljske zaštite, otvorit će se prikaz postavki **filtriranja sadržaja**.

**4.** Uključite **Filtriraj online sadržaj**.

**5.** 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.

**6.** Odaberite **Nastavi**.
Aplikacija vas traži da dopustite VPN konfiguracije. Ovo je nužan korak jer Obiteljska zaštita koristi VPN vezu za blokiranje neželjenog sadržaja.

**7.** Odaberite **Nastavi**.
Ovo otvara sistemsko upozorenje koje vas pita želite li dopustiti VPN konfiguracije za aplikaciju.

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

## 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**.

**3.** Odaberi **Uređaj neke druge osobe** > **Nastavi**.

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

Ova osoba prima e-poštu/SMS 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/SMS 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 **Promijeni**, a zatim odaberite **Nastavi**.
Otvara se vaš portal za upravljanje.

Sada možete upravljati vlastitim uređajima i njihovom zaštitom 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 Sigurnijeg interneta.

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 **Licenca za izdavanje**.

**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 **Licenca za izdavanje**.

**6.** Izaberite **Licenca za izdavanje**.

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

Aplikacija skenira vaš uređaj u potrazi za virusima, štetnim sadržajem i drugim prijetnjama vašem uređaju i vašim podacima.

Kada je skeniranje uključeno, aplikacija svakodnevno automatski skenira uređaj. Također možete ručno skenirati uređaj u bilo kojem trenutku.

Preporučujemo da skenirate svoj uređaj u potrazi za prijetnjama kad god proizvod to od vas zatraži.

Aplikacija također automatski skenira instalirane programe i umetnute memorijske kartice na viruse, špijunski softver i rizične stavke.

**Bilješka:** Značajke optimizacije baterije na nekim uređajima sa sustavom Android mogu spriječiti rad aplikacije u pozadini. Kada se to dogodi ili ako ručno zaustavite aplikaciju, vaš uređaj nije zaštićen od prijetnji. Kako biste izbjegli ovaj problem, provjerite dopuštenja za korištenje baterije na svom uređaju i provjerite ima li aplikacija potrebna dopuštenja kako bi uvijek radila.

## 4.1 Pokretanje ručnog skeniranja

U svakom trenutku možete skenirati svoj uređaj u potrazi za virusima i drugim zlonamjernim kodom.

Za ručno skeniranje datoteka na uređaju:

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

**2.** Odaberi **Pregledaj** pod **Pregledavanje prijetnji**.
Skeniranje započinje.

**3.** Nakon što skeniranje završi, proizvod prikazuje sljedeće informacije:
- Ukupan broj provjerenih datoteka - broj datoteka koje su skenirane
- Ukupan broj provjerenih aplikacija - broj skeniranih aplikacija

**Savjet:** Odabirom **Povijest skeniranja** unutar odjeljka **Sigurnosne prijave**, možete vidjeti popis pokrenutih ručnih i automatskih skeniranja. Dodirnite željeno skeniranje da biste vidjeli više informacija o rezultatima skeniranja.

## 4.2 Uključivanje automatskog skeniranja

Možete postaviti aplikaciju tako da automatski skenira vaš uređaj u potrazi za virusima i drugim prijetnjama.

Kada je uključena, aplikacija automatski skenira uređaj svaki dan i svaki put kada se instalira nova aplikacija.

Kako biste bili sigurni da je automatsko skeniranje omogućeno na vašem uređaju, učinite sljedeće:

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

**2.** Odaberite  u gornjem desnom kutu i provjerite je li uključena postavka

**UKLJUČEN je antivirusni program**.

Aplikacija svakodnevno automatski skenira nove aplikacije i datoteke. Ako želite da aplikacija skenira vaš uređaj čak i kada je uređaj povezan na mrežu s ograničenim prometom, provjerite je li uključena postavka **Pregledavanje na vezi s podatkovnim ograničenjem UKLJUČENO**.

**Bilješka:** Uključivanje ove opcije može dovesti do dodatnih troškova.

## 4.3 Upotreba mrežne veze s ograničenim prometom

Mrežna veza s ograničenim prometom ona je veza koja ima ograničenje količine podataka koju možete upotrebljavati.

Kada je uključena, aplikacija skenira čak i kad je povezana na mrežu s ograničenim prometom. To može rezultirati povećanim podatkovnim prometom i dodatnim troškovima.

Da biste omogućili skeniranje dok ste na povezani na mrežu s ograničenim prometom, učinite sljedeće:

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

**2.** Odaberite  u gornjem desnom kutu i provjerite je li uključena postavka **Pregledavanje na vezi s podatkovnim ograničenjem UKLJUČENO**.

## 4.4 Provjera rezultata skeniranja

Kada skeniranje završi, možete provjeriti rezultate.

Ako aplikacija tijekom pregledavanja otkrije datoteku koja sadrži virus ili neki drugi zlonamjerni kod, pojavljuje se obavijest u prikazu **Zaštita uređaja**. Na primjer, možete vidjeti sljedeću obavijest:
- 1 otkrivanje – potencijalno neželjena aplikacija
- 1 zaraza – otkrivena je štetna aplikacija

Za procjenu otkrivene datoteke učinite sljedeće:

**1.** U prikazu **Zaštita uređaja** odaberite obavijest ispod opcije **Sigurnosne prijave**. Otvara se stranica s pojedinostima o skeniranju.

**2.** Za uklanjanje datoteke ili datoteka odaberite **Ukloni sva otkrivanja** kako biste ih u isto vrijeme uklonili sa svog uređaja.

- Da biste vidjeli više pojedinosti, na stranici **Pojedinosti o skeniranju** odaberite obavijest kako biste vidjeli više o pojedinostima otkrivanja. Možete vidjeti sljedeće pojedinosti:
- Naziv aplikacije
- Naziv paketa
- Otkriveni problemi
- Veličina
- Odaberite **Ukloni** da biste uklonili datoteku.

Datoteka ili datoteke u potpunosti su uklonjene s vašeg uređaja.

## 4.5 Pregled dopuštenja aplikacije na vašem uređaju

Zaštita uređaja daje vam pregled dopuštenja koja aplikacije instalirane na vašem uređaju trenutačno upotrebljavaju.

Preporučujemo da redovito provjeravate dopuštenja koja su omogućena za vaše instalirane aplikacije.

Neke aplikacije primjerice mogu zahtijevati dopuštenja koja su potrebne za značajke koje nikada ne upotrebljavate. Osim toga, provjera dopuštenja aplikacije dobar je način da vidite imaju li neke aplikacije opsežan pristup podacima i funkcijama vašeg uređaja, što može utjecati na vašu privatnost.

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

**2.** Pod opcijom **Pregled privatnosti aplikacije** odaberite ikonu filtra, a zatim opciju **Putem aplikacije** da biste pregledali trenutačno omogućena dopuštenja prema aplikaciji.

**3.** Odaberite aplikaciju da biste vidjeli više pojedinosti o omogućenim dopuštenjima za tu aplikaciju.

Ovo vam prikazuje popis svih dopuštenja za uređaj koja su omogućena za aplikaciju, s kratkim opisom svakog dopuštenja.

**4.** Izaberite **Upravljanje dozvolama** da biste otišli na postavke uređaja i promijenili dopuštenja za odabranu aplikaciju.

Ovdje možete opozvati dopuštenja iz aplikacije ako smatrate da nisu potrebna. Međutim, imajte na umu da opoziv dopuštenja može utjecati na funkcionalnost aplikacije.

## 4.6 Zaštita uređaja

Zaštita uređaja upozorava vas ako niste postavili PIN ili biometrijsko zaključavanje za svoj uređaj.

**Bilješka:** Dostupne opcije identifikacije, kao što su PIN kod, prepoznavanje lica ili prepoznavanje otiska prsta, razlikuju se ovisno o modelu i verziji vašeg uređaja.

Aplikacija vam prikazuje obavijest ako se zaključavanje uređaja ne koristi. Slijedite upute navedene u obavijesti kako biste riješili problem.

Ako ne vidite obavijest na glavnom prikazu ili ako ste odbacili obavijest, također možete provjeriti status u **Zaštita uređaja** pogled:

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

**2.** Odaberite sva upozorenja koja vidite pod **Sigurnosne prijave**.

▪ Izaberi **Zaključavanje uređaja** kako biste vidjeli upute o tome kako koristiti zaključavanje uređaja.

**3.** Slijedite upute za rješavanje problema.

Nakon što ste riješili probleme, poruka upozorenja nestaje iz **Zaštite uređaja**.

# 5 Zaštita od prijevare

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

Korištenjem Chrome zaštite, sigurnost web-stranice automatski se provjerava prije nego što joj pristupite. Ako je stranica ocijenjena kao sumnjiva ili štetna, A1 Sigurniji internet blokira pristup stranici. Ocjena sigurnosti web-stranice temelji se na analizi naše usluge za ugled web-stranice.

## 5.1 Postavljanje proširenja preglednika Chrome

Aplikacija zahtijeva određena dopuštenja za pružanje zaštite u pregledniku Chrome. Kada odobrite ova dopuštenja, aplikacija štiti vaše pregledavanje weba u Chromeu i prikazuje vam sigurnosne informacije dok pregledavate internet.

**Bilješka:** Proširenje preglednika upotrebljava adresu web-mjesta za provjeru njegove reputacije i utvrđivanje sigurnosti stranice. Ne provjerava sadržaj, poveznice ili skripte koje se nalaze na stranici.

Za početak korištenja Zaštita preglednika Chrome:

**1.** Otvorite aplikaciju A1 Sigurniji internet.

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

**3.** Izaberi **Zaštita preglednika Chrome**.

Od vas se traži da dopustite dopuštenja za aplikaciju. Aplikacija zahtijeva dopuštenja pristupačnosti za provjeru sigurnosti web-mjesta koja posjećujete i dopuštenje za prikaz sadržaja preko drugih aplikacija kako bi vam se prikazala ocjena sigurnosti za web-mjesta.

**4.** Izaberi **Nastaviti** i slijedite upute na zaslonu kako biste omogućili potrebna dopuštenja. Nakon što dopustite dopuštenja, vaše je pregledavanje u Chromeu zaštićeno.

Kada posjetite web mjesto u pregledniku Chrome, na desnom rubu zaslona pojavljuje se ikona koja vam pokazuje ocjenu sigurnosti web mjesta. Dodirnite ikonu da vidite više informacija o ocjeni sigurnosti. Ikona se nakon nekog vremena zatamni, a možete je sakriti u postavkama aplikacije ako želite ili je povući na bilo koji drugi rub zaslona. Štetne web stranice automatski se blokiraju.

Kako sakriti Chrome preklapajuću ikona:

**1.** Otvorite aplikaciju A1 Sigurniji internet.

**2.** U glavnom prikazu aplikacije odaberite **Zaštita od prijevare**.

**3.** Izaberi **Zaštita preglednika Chrome**.

**4.** Odaberite  u gornjem desnom kutu zaslona za otvaranje postavki.

**5.** Odaberite koje vrste web-mjesta trebaju prikazati ili sakriti ikonu sloja.

**Bilješka:** Na nekim uređajima ažuriranja preglednika Chrome ili drugih alata sustava mogu poništiti vezu između Zaštite preglednika Chrome i usluga pristupačnosti na vašem Android uređaju. Kao rezultat toga, ikona preklapanja nije prikazana, bankarska zaštita ne radi, a nesigurne stranice nisu blokirane. Da biste riješili ovaj problem, idite na dopuštenja aplikacije u postavkama uređaja i promijenite dopuštenja pristupačnosti za Zaštitu preglednika Chrome isključiti i ponovno uključiti.

## 5.2 Dopuštanje određenih web-stranica

Možete ručno dopustiti web-stranice ako ste sigurni da su sigurne.

Da biste dopustili web-mjesto:

**1.** Otvorite aplikaciju A1 Sigurniji internet.

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

**3.** Odaberite  u gornjem desnom kutu zaslona za otvaranje postavki.

**4.** Odaberite **Dopuštena web-mjesta**.

**5.** Odaberite **Dodaj dopušteno web-mjesto**.

**6.** Unesite adresu web-mjesta koje želite dodati, a zatim odaberite **Dopusti ovo web-mjesto**

Da biste dopustili sve poddomene web-mjesta, unesite glavnu domenu. Na primjer, ako unesete example.com, to će omogućiti i test.example.com i sample.example.com uz www.example.com.

Proizvod ne podržava upotrebu zamjenskih znakova, na primjer *. Web-mjesto je sada navedeno kao dopušteno.

Da biste uklonili web-mjesto s popisa, odaberite web-mjesto, a zatim odaberite **Ukloni**.

## 5.3 Prikaz sigurnosnih ocjena za web stranice

U postavkama aplikacije možete odabrati kada će se sigurnosne ocjene prikazivati kao preklapajuća ikona.

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

**2.** Odaberite ikonu **Postavke** u gornjem desnom kutu zaslona.
Ovo otvara prikaz postavki.

**3.** Upalite **Preklopna ikona** za prikaz sigurnosnih ocjena web stranica koje posjećujete.

Preklopna ikona također vam pokazuje kada posjećujete bankovno web mjesto i mogu li se vjerovati web stranicama za kupnju koje posjećujete.

Kada je ikona preklapanja u upotrebi, možete odabrati ikonu u pregledniku da biste vidjeli više informacija o ocjeni za trenutnu web stranicu.

## 5.4 Nailazite na blokiranu web stranicu

Ova tema objašnjava što učiniti ako slučajno pristupite štetnom mjestu.

Ako slučajno pristupite štetnoj web stranici dok koristite Chrome s uključenom Zaštitom preglednika Chrome, aplikacija automatski blokira pristup i prikazuje stranicu koja vas obavještava da je web stranica koju ste upravo pokušali posjetiti štetna.

Ako mislite da je stranica sigurna, možete je prijaviti kao netočno ocijenjenu slijedeći Ovdje prijavite lažno pozitivno vezu. Za podnošenje stranice na analizu, odaberite s lijeve strane stranice **URL sample**, ispunite potrebna polja i odaberite **Continue**.

## 5.5 Zaštita od prijevara tekstualnim porukama

Kada primite tekstualnu poruku (SMS) od nepoznatog pošiljatelja, postoji rizik od toga da je poruka prijevara koja uključuje poveznice na štetna web-mjesta. Na primjer, kriminalci često koriste tekstualne poruke kako bi prevarili ljude da im pošalju osjetljive osobne podatke ili posjete štetno web-mjesto. Može se činiti da je poruke poslao legitiman pošiljatelj - banka ili kurirska služba.

Zaštita SMS poruka upotrebljava umjetnu inteligenciju (AI) za usporedbu tekstualnih poruka koje primate s poznatim prijevarnim porukama, a također provjerava sadrži li poruka štetne poveznice.

Zaštita SMS poruka automatski premješta sve otkrivene prijevarne poruke u mapu bezvrijedne pošte vaše aplikacije za razmjenu poruka.

**Bilješka:** Zaštita SMS poruka ne prikuplja osobne podatke iz vaših poruka.

Da biste postavili Zaštitu SMS poruka:

**1.** Otvorite aplikaciju A1 Sigurniji internet.

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

**3.** Odaberite **Zaštita poruka** > **Započni**.

Od vas se traži dopuštenje za pristup vašim SMS porukama i kontaktima, a od vas se također može tražiti da dopustite obavijesti.

**4.** Dopusti tražena dopuštenja.

Kada omogućite potrebna dopuštenja, aplikacija vas obavještava o nadolazećim porukama za koje je utvrđeno da su štetne. Da biste pogledali pojedinosti o otkrivenim porukama, otvorite aplikaciji i idite na **Zaštita od prijevara** > **Zaštita poruka** > **Izvješća o prijevarama**.

## 5.6 Provjerite je li vaša Wi-Fi veza sigurna

Kada upotrebljavate Wi-Fi za povezivanje uređaja s mrežom, Wi-Fi zaštita provjerava je li siguran ili biste ga trebali izbjegavati.

Kriminalci mogu upotrebljavati nesigurno konfigurirane Wi-Fi žarišne točke za krađu podataka ili prisluškivanje vaše mrežne komunikacije, na primjer putem napada „čovjek u sredini" (Man-in-the-Middle). Ova vrsta napada znači da se može činiti da vaša internetska veza radi normalno, ali zapravo napadač može presresti vaše prenesene podatke i preusmjeriti vas na lažna web-mjesta koja izgledaju autentično.

Wi-Fi zaštita provjerava različite sigurnosne aspekte vaše veze kad god bežično povežete svoj uređaj s mrežom. Ove provjere uključuju certifikate i enkripciju za vezu kao i testiranje mrežnih zahtjeva za sve neočekivane ili sumnjive promjene. Nakon što se veza provjeri, Wi-Fi zaštita vas obavještava je li sigurna za upotrebu ili ne.

Wi-Fi zaštita upotrebljava obavijesti da vam pokaže je li vaša WiFi veza sigurna ili ne. Ako aplikacija nema dopuštenje za prikazivanje obavijesti na vašem uređaju, od vas se traži da dopustite to dopuštenje kada odete na prikaz **WiFi zaštita**.

Također možete postaviti aplikaciju tako da vam prikazuje obavijesti o otvorenim Wi-Fi vezama (veze koje ne zahtijevaju lozinku), kao i o sigurnim i nesigurnim vezama.

**Bilješka:** Za prepoznavanje otvorenih Wi-Fi veza na uređajima sa sustavom Android starijim od verzije 12, aplikaciji je potrebno dopuštenje za lokaciju, a lokacijske usluge moraju biti uključene na vašem uređaju.

Kako biste bili sigurni da su vaše Wi-Fi veze sigurne:

**1.** Otvorite aplikaciju A1 Sigurniji internet.

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

**3.** Odaberite opciju **Wi-Fi zaštita**.
Ovo otvara prikaz **Wi-Fi zaštita**. Kada je Wi-Fi zaštita uključena, ovaj vam prikaz pokazuje statistiku o broju sigurnih i nesigurnih Wi-Fi veza.

**4.** Uključite **Wi-Fi zaštitu**.

**6.** Pod  u gornjem desnom kutu odaberite obavijesti koje želite vidjeti.

## 5.7 Provjera sadržaja zbog prijevara

Skener prijevara analizira snimke zaslona i slikovne datoteke kako bi identificirao potencijalne pokušaje krađe identiteta (phishing), lažni sadržaj i razne vrste prijevara te vas tako zaštitio.

**Bilješka:** Ova značajka trenutačno je u beta fazi razvoja, što znači da se mogu očekivati neki problemi s funkcionalnošću.

Ako na internetu pronađete nešto što smatrate sumnjivim, bilo da se radi o poruci na društvenim mrežama, oglasu, objavljenom otvorenom radnom mjestu ili nekom drugom sadržaju, možete snimiti zaslon i upotrijebiti Skener prijevara kako biste provjerili je li to legitimno ili prijevara.

Skener prijevara koristi umjetnu inteligenciju za otkrivanje obrazaca, sumnjivih elemenata i znakova taktika psihološke manipulacije koje bi mogle ukazivati na to da je sadržaj prijevara.

Nakon što se sadržaj analizira, aplikacija vam prikazuje odluku o tome čini li se sadržaj sigurnim ili prijevarom ili ako analiza ne može pružiti jasan rezultat. Također vam daje objašnjenje razloga za odluku. Ako se sadržaj čini prijevarom, dobit ćete i smjernice o tome što biste trebali učiniti kada naiđete na takvu vrstu prijevare.

**Bilješka:** Objašnjenja odluke i preporučene radnje prikazane su samo na engleskom jeziku, čak i ako ste aplikaciju instalirali na drugom jeziku.

Kada vidite sadržaj koji želite provjeriti:

**1.** Napravite snimku zaslona sadržaja na svom uređaju.

**2.** Ako snimka zaslona sadrži bilo koje vaše osobne podatke, izrežite sliku kako biste isključili te podatke.

**3.** Otvorite aplikaciju A1 Sigurniji internet.

**4.** Odaberite **Skener prijevara** na glavnom prikazu.
Ovim se otvara prikaz slika u zadanoj aplikaciji za fotografije na vašem uređaju.

**5.** Odaberite sliku koju želite analizirati.
Aplikacija prenosi i počinje analizirati sliku koju ste odabrali. Nakon što je analiza dovršena,

aplikacija vam prikazuje rezultate. Ako se sadržaj smatra prijevarom, vidjet ćete i objašnjenje odluke kao i preporuke o tome što biste trebali učiniti.

**6.** Ako se ne slažete s rezultatom, odaberite **Ne** pod **Je li ovo bilo korisno**, a zatim odaberite **Rezultat je bio pogrešan** > **Pošaljite povratne informacije**.

To nam pomaže da analiza bude dosljednija i točnija kako bismo vam u budućnosti mogli pružiti relevantnije rezultate.

Snimku zaslona za analizu možete prenijeti i izravno iz zadane aplikacije za fotografije na uređaju: da biste to učinili, odaberite sliku koju želite analizirati i podijelite je s aplikacijom A1 Sigurniji internet.

**Bilješka:** Ovisno o vašoj pretplati, može postojati ograničenje broja slika koje možete analizirati unutar određenog vremena.

## 5.7.1 Primjeri kategorija prijevara

Iako ovo nije potpuni popis i može se s vremenom mijenjati, evo nekoliko kategoriziranih primjera uobičajenih prijevara.

| **Kategorija prijevare** | **Opis** |
|---|---|
| Dobrotvorna organizacija | Iskorištavanje katastrofa, aktualnih događaja ili emocionalnih uzroka lažnim predstavljanjem kao lažne dobrotvorne organizacije radi krađe donacija. Prevaranti koriste taktike visokog pritiska, daju nejasne detalje o svojoj misiji i često traže nemogućnost praćenja plaćanja ili plaćanja samo u gotovini. |
| Oslobađanje od duga | Obećavaju da će eliminirati ili značajno smanjiti vaš dug uz unaprijed plaćene naknade, ali bez obećanih rezultata. Pružatelji ovih lažnih usluga često tvrde da mogu pregovarati s vjerovnicima ili zaustaviti pozive za naplatu bez da zapravo pruže legitimnu pomoć u vezi s dugom. |
| Lažna e-trgovina | Internetske trgovine koje prodaju krivotvorene ili nepostojeće proizvode po nerealnim cijenama spadaju u ovu kategoriju. Ove stranice obično imaju loš dizajn, sumnjive načine plaćanja i lažne recenzije kako bi prevarile kupce koji nikada ne prime svoje narudžbe. |
| Lažna ponuda za posao | Lažne mogućnosti zapošljavanja, često rad od kuće, osmišljene za krađu novca ili osobnih podataka. Ove prijevare mogu zahtijevati plaćanje obuke ili opreme unaprijed, sadržavati nejasne opise poslova i obećavati nerealnu naknadu. |
| Igre | Korištenje lažnih valuta u igri, ukradenih računa, lažnih nagradnih natjecanja ili krađe identiteta u svrhu otkrivanja podataka za prijavu igrača. Prevaranti obično iskorištavaju zajednice igrača ponudama rijetkih predmeta, šifri za varanje ili nadogradnji računa koje su previše dobre da bi bile istinite. |
| Nagradna igra | Ponude nagrada, besplatnih proizvoda ili natjecanja koja zahtijevaju plaćanje troškova dostave unaprijed ili osobne podatke. Obećane nagrade često su lažne, a prevaranti mogu koristiti preporuke slavnih |

| | |
|---|---|
| | osoba ili ponude koje su previše dobre da bi bile istinite kako bi namamili žrtve. |
| Zdravstvo | Ponude lažnih medicinskih proizvoda, tretmana ili usluga s pretjeranim tvrdnjama o liječenju bolesti ili poboljšanju zdravlja. Ove lažne sheme često prodaju krivotvorene lijekove, neprovjerene terapije ili kradu podatke o osiguranju i osobne medicinske podatke. |
| Lažno predstavljanje | Kriminalci se pretvaraju da su legitimne organizacije, vladine agencije, poznate osobe ili osobe s autoritetom kako bi iskoristili povjerenje. Ove prijevare često koriste službeni izgled brendiranja i stvaraju hitne situacije s prijetnjama posljedicama kako bi se izvršilo trenutno djelovanje. |
| Ulaganje | Obećanja o zajamčenim visokim prinosima ili ekskluzivnim prilikama kako bi vas se prisililo da brzo uložite novac. Ove prijevarne sheme često uključuju kriptovalute, lažne dionice ili nerealne tvrdnje o dobiti potkrijepljene izmišljenim svjedočanstvima. |
| Posao | Lažne mogućnosti zapošljavanja osmišljene za prikupljanje osobnih podataka, krađu novca putem lažnih postupaka zapošljavanja ili regrutiranje žrtava za ilegalne aktivnosti. Ove prijevare često obećavaju visoku plaću za minimalan rad, obavljaju intervjue samo putem tekstualnih poruka ili traže osjetljive informacije prije legitimne provjere. |
| Zajam | Obećanja brzog pristupa novcu uz zajamčeno odobrenje bez obzira na kreditnu povijest, ali uz unaprijed plaćene naknade prije isplate sredstava. Prevaranti obično nestaju nakon naplate naknada. |
| Lutrija | Obavijesti o osvojenim nagradama ili nagradnim igrama u kojima nikada niste sudjelovali, nakon čega slijede zahtjevi za plaćanje poreza ili naknada za preuzimanje dobitaka. Legitimne lutrije nikada ne zahtijevaju plaćanje unaprijed, a ove prijevare često se lažno predstavljaju kao poznate lutrijske organizacije. |
| Mirovina | Prijevare usmjerene na mirovinsku štednju putem lažnih investicijskih shema, lažnih pregleda mirovina ili neovlaštenih prijenosa koji obećavaju veće prinose. Prevaranti vrše pritisak na žrtve da premjeste mirovinske fondove u visokorizična ili nepostojeća ulaganja, što rezultira značajnim financijskim gubicima i poreznim kaznama. |
| Krađa identiteta | Pokušaji krađe vaših osobnih podataka ili podataka za prijavu putem lažnih web stranica, e-pošte, poruka ili drugih sredstava. U takvim pokušajima prevaranti se često lažno predstavljaju kao legitimne organizacije. Prevaranti obično stvaraju hitne scenarije kako bi vas prisilili da kliknete na sumnjive poveznice ili podijelite osjetljive podatke poput lozinki, brojeva kreditnih kartica ili podataka o računu. |
| Piramidalna shema | Riječ je o lažnim poslovnim modelima usmjerenima na regrutiranje drugih, a ne na prodaju stvarnih proizvoda, gdje prihod prvenstveno dolazi od naknada za regrutiranje. Sudionicima se obećava prihod na temelju regrutiranja novih članova, sa složenim strukturama naknada koje koriste samo onima na vrhu. |
| Nekretnina | Lažni oglasi za nekretnine, lažne ponude za najam ili investicijske sheme usmjerene na kupce nekretnina, najmoprimce ili investitore. Prevaranti objavljuju nekretnine koje ne posjeduju, traže polog prije prikazivanja nekretnina ili nude ponude znatno ispod tržišne vrijednosti. |

| | |
|---|---|
| Romantika | Lažne romantične veze osmišljene kako bi se nekoga emocionalno izmanipuliralo da pošalje novac ili podijeli osobne podatke. Prevaranti obično izbjegavaju video pozive i brzo pojačavaju emocionalnu povezanost prije nego što podnesu financijske zahtjeve. |
| Seksualno iznuđivanje | Prijetnje dijeljenjem intimnih slika ili izmišljenog kompromitirajućeg sadržaja osim ako žrtve ne plate. Prevaranti mogu tvrditi da su hakirali kamere, dobili osobne fotografije ili snimili privatne aktivnosti kako bi iznudili plaćanje na osnovu straha i srama. |
| Kupovina | Lažne ponude na mreži, nepostojeći proizvodi ili krivotvorena roba koja se oglašava s velikim popustima. Ove prijevare često se pojavljuju kao oglasi na društvenim mrežama ili lažne maloprodajne web stranice koje naplaćuju, ali nikada ne isporučuju legitimne proizvode. |
| Pretplata | Neke prijevare mogu zarobiti žrtve neželjenim ponavljajućim naplatama putem obmanjujućih besplatnih probnih razdoblja, skrivenih uvjeta ili lažnih usluga. Prevaranti izuzetno otežavaju otkazivanje i nastavljaju naplaćivati uz malu ili nikakvu stvarnu vrijednost usluge. |
| Porez | Prijevare u kojima se kriminalci lažno predstavljaju kao porezne vlasti ili nude lažne porezne usluge kako bi ukrali novac ili osobne podatke. Prevaranti obično stvaraju osjećaj hitnosti prijeteći uhićenjem ili pravnim postupcima zbog neplaćenog poreza, zahtijevajući trenutno plaćanje putem metoda koje se ne mogu pratiti. |
| Tehnička podrška | Prijevare u kojima se netko lažno predstavlja kao legitimna tehnološka tvrtka, često tvrdeći da vaš uređaj ima viruse ili sigurnosne probleme. Prevaranti obično vrše pritisak na žrtve da omoguće daljinski pristup računalima, plate nepotrebne usluge ili dijele financijske podatke kako bi riješili nepostojeće probleme. odaberite protokol koji želite koristiti. |

# 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 koristiti Spremište za lozinke na uređaju koji trenutno koristite.

Kada počnete koristiti  Spremište za lozinke, prva stvar koju trebate učiniti je stvoriti glavnu lozinku. Glavna lozinka jedina je lozinka koju trebate zapamtiti nakon postavljanja Spremišta za lozinke.

Kako postaviti Spremište za lozinke:

**1.** Otvorite aplikaciju A1 Sigurniji internet.

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

**3.** Odaberi **Početak rada** te **Novi sam korisnik.**

**Bilješka:** Ako želite pristupiti svom Spremištu za lozinke stvoren na drugom uređaju ili aplikaciji, možete povezati uređaje za sinkronizaciju svojih zaporki odabirom **Postojeći sam korisnik**.

**4.** Stvorite jaku glavnu lozinku i odaberite **Nastavi**.

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

**6.** Stvorite QR kod za oporavak odabirom **Spremi kao sliku**. Kod se sprema kao slika u vašu Galeriju.

Ako vaš uređaj radi na Androidu 9 ili starijem, morate dopustiti Spremištu za lozinke  pristup vašim fotografijama, medijima i datotekama na vašem uređaju.

**Važno:** Također preporučujemo da odmah izradite QR kôd za oporavak glavne lozinke. To je jedini način da povratite glavnu lozinku ako je zaboravite.

**7.** Ako vaš uređaj podržava biometrijsku autentifikaciju, na primjer otisak prsta, i ako ste to postavili, možete pristupiti svom Spremištu za lozinke brže omogućavanjem opcije **Biometrijsko otključavanje**. Imajte na umu da ako sada ne želite koristiti biometrijsku autentifikaciju, to možete učiniti kasnije u postavkama Spremišta.

**Zapamtite:** Nemojte zaboraviti svoju glavnu lozinku. S vremena na vrijeme morat ćete

unijeti svoju glavnu lozinku da biste otključali Spremište za lozinke.

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

a) U Spremištu za lozinke, Odaberi > **Automatska ispuna**.

b) Upali **Automatsku ispunu** i odaberite željenu uslugu automatskog popunjavanja u postavkama uređaja.

Sada ste spremni dodati svoju prvu lozinku Spremište za lozinke.

Ako još niste izradili QR kod za oporavak za glavnu lozinku, obavijest za izradu koda prikazivat će vam se dok ga ne izradite.

## 6.2 Korištenje Spremišta za lozinke

Uz Spremište 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 Pohranjivanje nove lozinke na mobilni uređaj

Nove lozinke možete pohraniti u aplikaciju na svom mobilnom uređaju.

Za pohranu nove lozinke:

**1.** Otvorite aplikaciju A1 Sigurniji internet.

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

**3.** Odaberi **+ Dodaj** > **Zaporka**.
Otvaraju se detalji unosa.

**4.** u **Naslov** polje, svom unosu dajte opisni naziv.

**5.** Za promjenu ikone unosa s lijeve strane dodirnite je i odaberite boju pozadine i simbol za unos. Kada završite, potvrdite svoj odabir odabirom .

**6.** u **Korisničko ime** polje unesite korisničko ime koje koristite za aplikaciju ili mrežnu uslugu.

**7.** u **Lozinka** polje, stvorite jaku lozinku ili zaporku.

**Savjet:** Odaberi  kako bi se otvorio izbornik **Generiraj lozinku** gdje možete dopustiti aplikaciji da za vas generira jaku, nasumičnu lozinku. Pritisnite  sve dok ne budete zadovoljni generiranom lozinkom. Za spremanje lozinke odaberite .

**8.** u **Web-adresa** unesite web-adresu (URL) stranice za prijavu na internetsku uslugu.

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

**9.** U polje **Napomene** unesite bilo koju drugu informaciju koju želite dodati.

**10.** Za spremanje unosa odaberite ✓.

Nove vjerodajnice sada su dodane u trezor lozinki.

**Važno:** Ako promijenite ili generirate lozinku u Spremištu za lozinke, ne zaboravite promijeniti svoju lozinku i u dotičnoj online usluzi ili aplikaciji.

## 6.2.2 Pohranjivanje podataka o platnoj kartici na mobilni uređaj

Sve podatke o platnoj kartici, poput podataka o kreditnoj i debitnoj kartici, možete sigurno pohraniti u aplikaciju na svom mobilnom uređaju.

Za pohranu podataka o platnoj kartici:

**1.** Otvorite aplikaciju A1 Sigurniji internet.

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

**3.** Odaberi **+ Dodaj** > **Kreditna kartica**.
Otvaraju se detalji unosa.

**4.** Za promjenu ikone unosa s lijeve strane dodirnite je, odaberite boju i jedan od dostupnih simbola platne kartice te odaberite ✓.

**5.** u **Naslov** polje unesite naziv platne kartice.

**6.** u **Ime i prezime vlasnika kartice** polje unesite svoje ime onako kako je na platnoj kartici.

**7.** u **Broj kreditne kartice** polje unesite broj vaše kartice.

**8.** u **PIN** polje unesite osobni identifikacijski broj vezan uz karticu.

**9.** u **Datum isteka** polje unesite datum (u formatu MM/GG) do kojeg kartica vrijedi.

**10.**u **Šifra za potvrdu** polje, unesite 3- ili 4-znamenkasti sigurnosni kod vaše kartice koji vam pomaže u zaštiti od prijevare s kreditnom karticom.

**11.**u **Web-adresa** polje unesite web adresu (URL) usluge.

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

**13.**Za spremanje novog unosa odaberite ✓.

Podaci o vašoj platnoj kartici sada su pohranjeni u Sef za lozinke.

### 6.2.3 Uređivanje postojećih podataka

Možda ćete morati urediti podatke 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.** Odaberi  za uređivanje pojedinosti unosa.

**5.** Napravite potrebne promjene.

**6.** Odaberi za spremanje promjena .

### 6.2.4 Brisanje unosa

Možete izbrisati unose u Spremištu 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.** Odaberi  za uređivanje pojedinosti unosa.

**5.** Za brisanje unosa odaberite  > **Izbrisati**.

### 6.2.5 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  za uređivanje pojedinosti unosa.

**5.** u **Lozinka** polje, odaberite .

**6.** u **Generiraj lozinku** pogled, 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.
▪ Odaberi  za generiranje nove lozinke.

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

## 6.2.6 Pristup vašim starim lozinkama

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

Nakon što ste promijenili lozinku u Spremištu 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.
**Povijest lozinki** pogled se otvara.

**5.** Za prikaz skrivene lozinke odaberite  u gornjem desnom uglu.

**Bilješka:** Možete kopirati željenu lozinku u međuspremnik odabirom .

**6.** Za zatvaranje **Povijest lozinki** prikaz, odaberite strelicu u gornjem lijevom kutu. Ako želite, možete izbrisati povijest lozinki odabirom .

## 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.** U gornjem desnom kutu zaslona odaberite  . Otvorit će se prikaz **Postavke Spremišta za lozinke**.

**4.** Odaberite **Povezani uređaji**. **Povezani uređaji** pogled se otvara.

**5.** Odaberi **Generiranje šifre za sinkronizaciju**.
Sinkronizacijski kod se generira automatski i vrijedi 60 sekundi. Novi kod se generira odmah nakon isteka trenutnog koda.

**6.** Otvorite aplikaciju na uređaju s kojim se želite povezati i sinkronizirati svoje podatke i odaberite **Skladište lozinki**.

**7.** Ovisno o tome je li drugi uređaj mobilni ili stolni uređaj, učinite nešto od sljedećeg:
▪ Na mobilnom uređaju:
**a.** Odaberi **Ja sam postojeći korisnik**. Pogled **Povezani uređaji** se otvara.
**b.** Unesite kod za sinkronizaciju generiran na prvom uređaju i odaberite **Spojiti**.

▪ Na stolnom uređaju:
**a.** Odaberite **Povezani uređaji**.
**b.** Unesite kod za sinkronizaciju generiran na prvom uređaju i odaberite **Povezani uređaji**.

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

**9.** Konačno, ako želite početi koristiti biometrijsku provjeru autentičnosti za otključavanje Spremišta za lozinke. Odaberi **Spremiti**.

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 automatskog popunjavanja za brži pristup aplikacijama i web stranicama

Možete brzo pristupiti aplikacijama i web-stranicama bez potrebe za ručnim unosom prijavnih podataka.

**Bilješka:** Na nekim modelima uređaja možda neće sve aplikacije u potpunosti podržavati automatsko popunjavanje.

Da bi automatska ispuna funkcionirala, korisničko ime, lozinka i web-adresa usluge moraju biti spremljeni u Spremištu za lozinke. Kad se u aplikaciju ili na web-mjesto prijavljujete pomoću vjerodajnica spremljenih u Spremištu za lozinke, aplikacija može vaše korisničko ime i lozinku unijeti automatski.

Da biste postavili automatsko popunjavanje na svom Android uređaju:

**1.** Otvorite aplikaciju A1 Sigurniji internet.

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

**3.** U gornjem desnom kutu zaslona odaberite  . Otvorit će se prikaz **Postavke Spremišta za lozinke**.

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

**5.** Upaliti **Automatsko popunjavanje**. Otvara se pogled **Usluga automatskog popunjavanja** u postavkama vašeg uređaja.

**6.** Izaberi **A1 Sigurniji internet** kao uslugu automatskog popunjavanja, a zatim odaberite **u redu** za potvrdu vašeg odabira.
Sada možete pristupiti svojim aplikacijama i online uslugama bez potrebe za ručnim unosom prijavnih podataka.

## 6.5 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.** U gornjem desnom kutu zaslona odaberite  . Otvorit će se prikaz **Postavke Spremišta za lozinke**.

**4.** Odaberite **Promijeni glavnu lozinku**.

**5.** Unesite staru glavnu lozinku i odaberite **Nastavi**.

**6.** Unesite snažnu novu glavnu lozinku.

**7.** Ponovite novu glavnu lozinku i odaberite **Potvrdi**.

**Bilješka:** Ako upotrebljavate biometrijsku autentifikaciju, pružite traženu autentifikaciju.

**8.** Budući da ste promijenili glavnu lozinku, morate izraditi novi QR kod za oporavak. Odaberite **Izradi sada**, a zatim odaberite **Spremi kao sliku**.
Kod se sprema na zadanu lokaciju na vašem uređaju.

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 kôd više neće biti valjan. Stoga pazite da QR kôd za oporavak uvijek bude ažuriran i valjan za trenutačnu glavnu lozinku.

## 6.6 Stvaranje QR koda za oporavak za glavnu lozinku

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

**Važno:** Također preporučujemo da odmah izradite QR kôd za oporavak glavne lozinke. To je jedini način da povratite glavnu lozinku ako je zaboravite.

Za izradu QR koda za oporavak vaše glavne lozinke:

**1.** Otvorite aplikaciju A1 Sigurniji internet.

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

**3.**U gornjem desnom kutu zaslona odaberite . Otvorit će se prikaz **Postavke Spremišta za lozinke**.

**4.** Odaberi **Stvorite kod za oporavak** i učinite nešto od sljedećeg:
▪ Ako koristite biometrijsku autentifikaciju, navedite traženu autentifikaciju. Alternativno, odaberite **Koristi lozinku** i unesite svoju glavnu lozinku.
▪ Unesite svoju glavnu lozinku i odaberite **Potvrdi** za izradu QR koda za oporavak.
Slika koda za oporavak automatski se stvara.

**5.** Odaberi **Spremi kao sliku**.
Kod se sprema na zadanu lokaciju na vašem uređaju. Ovo je obično mapa Galerija.

**6.** Idite u mapu, odaberite sliku i pošaljite je servisu odakle je možete ispisati.

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

## 6.7 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 kôd 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.

## 6.8 Otključavanje i zaključavanje Spremišta za lozinke

Ova tema pokazuje kako otključati Sef za lozinke.

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

Za otključavanje Sefa za lozinke učinite sljedeće:

**1.** Otvorite aplikaciju A1 Sigurniji internet.

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

**3.** Unesite svoju glavnu lozinku i odaberite **Otključaj** ili upotrijebite biometrijsku provjeru autentičnosti za otključavanje Spremišta za lozinke.

**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 Spremišta za lozinke**  > **Automatski zaključaj nakon** i odaberite vrijeme. Opcije su odmah, 5 minuta, 15 minuta, 30 minuta, 1 sat, 10 sati i 1 tjedan.

**4.** Za ručno zaključavanje Sefa za lozinke, odaberite **Postavke Spremišta za lozinke**  > **Zaključaj odmah**.

## 6.9 Korištenje biometrijske provjere autentičnosti za otključavanje Spremišta za lozinke

Na određenim modelima mobilnih uređaja možete koristiti biometrijsku provjeru autentičnosti za otključavanje Spremišta za lozinke.

Da biste mogli koristiti otisak prsta za otključavanje Spremišta za lozinke, prvo morate registrirati svoj otisak prsta. Pogledajte korisnički priručnik uređaja kako biste saznali kako koristiti prepoznavanje otiska prsta na svom uređaju.

U Spremište za lozinke, možete koristiti biometrijsku provjeru autentičnosti kada izradite svoju glavnu lozinku ili kasnije u Spremište za lozinke postavke ili stranicu za prijavu.

**Važno:** Nemojte, međutim, zaboraviti svoju glavnu lozinku jer vam je potrebna, na primjer, nakon svake nadogradnje softvera.

Također, toplo preporučujemo da izradite QR kod za oporavak za svoju glavnu lozinku. To je jedini način na koji možete pristupiti svojim podacima ako zaboravite glavnu lozinku.

# 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 prikazu **Nadzor ID-a**, odaberite **Dodaj unos**.

Otvara se dijaloški okvir **Dodaj novo** s popisom svih dostupnih vrsta informacija koje možete odabrati.

**4.** Odaberite vrstu stavke koju želite dodati za praćenje.

**5.** 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 **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-ja** odaberite **Vaši podaci**.
Otvara se popis vaših praćenih stavki.

**4.** Za brisanje stavke s popisa odaberite ⋮ pored stavke koju želite ukloniti, a zatim odaberite **Izbriši unos**.
Otvara se dijaloški okvir za potvrdu.

**5.** Da biste potvrdili kako želite prestati pratiti stavku, odaberite **Izbriši**.
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

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

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-ja** odaberite **Vaši podaci**.
Otvara se popis vaših praćenih stavki.

**4.** Ako još niste dodali adresu e-pošte koju želite koristiti kao novu kontaktnu adresu e-pošte praćenim stavkama, učinite sljedeće:
a) Odaberite **+** > **E-pošta**, zatim unesite adresu e-pošte i odaberite **Spremi**.
E-pošta s poveznicom za potvrdu šalje se na adresu koju ste unijeli.
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 **Vaši podaci**, 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 Tehnička podrška

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

## 8.1 Gdje se nalaze podaci 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.** Odaberite ikonu profila u gornjem desnom kutu zaslona.

**3.** Izaberite **Podaci o aplikaciji**.
Otvara se prikaz **Podaci o aplikaciji** koji prikazuje razne informacije o proizvodu. Osim informacija o verziji proizvoda, prikaz **Informacije** sadrži informacije, kao što su licencni ključ, licencni uvjeti za krajnjeg korisnika, pravila o privatnosti i softver treće strane.

## 8.2 Slanje zapisa podršci

Ova tema objašnjava kako poslati zapisničke datoteke podršci ako se to zatraži.

Našoj tehničkoj podršci ponekad mogu trebati detaljnije informacije o vašem uređaju kako bi mogli riješiti neki problem.

Za izradu i slanje zapisničkih datoteka podršci:

**1.** Otvorite aplikaciju A1 Sigurniji internet.

**2.** Odaberite ikonu profila u gornjem desnom kutu zaslona.

**3. Izaberite Podaci o aplikaciji.**
**Otvara se prikaz Podaci o aplikaciji**

**4.** Odaberite **Pošalji zapisnik** na dnu ekrana i spremite datoteke na svoj uređaj.

**5.** Odgovorite na e-poruku koju ste primili od naše tehničke podrške i priložite spremljene zapisničke datoteke svom odgovoru kao privitke.

**6.** Opišite sve ostale detalje o problemu i pošaljite e-poruku našoj podršci.
Pričekajte dok vas naša podrška ne kontaktira.

# 8.3 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.