Internet zaštita

za Windows

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 Instaliranje proizvoda na računalo 8
2.1.2 Deinstaliranje proizvoda 9
2.2 Prikaz podataka o vašem računu 10
2.3 Obavijesti o potrebnim i preporučenim zadacima 11
2.4 Upravljanje postavkama proizvoda 12
2.4.1 Brz pristup postavkama proizvoda 12
2.4.2 Upotreba načina rada za igranje 12
2.5 Prikaz statusa vašeg proizvoda 14
2.5.1 Ikone stanja zaštite 14
2.5.2 Prikaz statistike zaštite 14
2.5.3 Prikaz nedavnih događaja za proizvod 15
2.5.4 Promjena postavki obavijesti 16
2.5.5 Prikaz najnovijih ažuriranja 16
2.6 Odjava iz aplikacije 17
2.7 Poboljšanje proizvoda 17
3 Osobe i uređaji 18
3.1 Zaštita vlastitih uređaja 18
3.2 Ograničavanje internetskog sadržaja za djecu 19
3.2.1 Postavljanje filtriranja sadržaja za dijete 19
3.3 Dijeljenje zaštite s članom obitelji ili prijateljem 22
3.3.1 Jeste li dobili poziv da zaštitite svoje uređaje? 23

3.3.2 Prestanite dijeliti zaštitu s članom obitelji ili prijateljem 23
3.4 Oslobađanje licence s uređaja 24
3.5 Premještanje aplikacije A1 Sigurniji internet sa vašeg starog uređaja na novi 25
4 Zaštita uređaja 26
4.1 Korištenje automatskog skeniranja 26
4.1.1 Kako funkcionira automatsko skeniranje 26
4.1.2 Privremeno isključivanje automatskog traženja 27
4.2 Pokretanje pregledavanja zlonamjernog softvera 28
4.2.1 Spremanje izvješća o skeniranju u datoteku 29
4.3 Pregledavanje stavki u karanteni 29
4.3.1 Vraćanje stavki iz karantene 30
4.4 Izuzimanje datoteka ili mapa iz skeniranja 30
4.5 Zakazivanje pregledavanja 31
4.6 Skeniranje u Windows Exploreru 32
4.7 Omogućavanje blokiranih aplikacija 32
4.7.1 Upravljanje izuzetim aplikacijama 33
4.8 Sprječavanje aplikacija da zatvore sigurnosne procese 34
4.9 Koristi se AMSI integracija da bi se napadi prepoznavali na temelju skripti 34
4.10 Što radi štetan sadržaj 35
4.10.1 Potencijalno neželjene aplikacije (PUA, Potentially unwanted applications) i neželjene aplikacije (UA, Unwanted applications) 35
4.10.2 Crvi 36
4.10.3 Trojanci 36
4.10.4 Programi za neovlašten ulazak u sustav 37
4.10.5 Kodovi koji se koriste slabim točkama 37
4.10.6 Paketi kodova koji se koriste slabim točkama 38
4.11 Slanje uzorka 38
5 Zaštita od prijevara 40

5.1 Ikone ocjene ugleda u rezultatima pretraživanja....40
5.2 Blokiranje štetnih web-mjesta....41
5.2.1 Automatsko blokiranje sumnjivih i zabranjenih web-mjesta....42
5.2.2 Ručno blokiranje web-stranica....42
5.2.3 Ručno dopuštanje blokiranih web-mjesta....43
5.2.4 Dopuštanje određenih web-stranica....43
5.2.5 Uvoz i izvoz popisa blokiranih i dopuštenih web-mjesta....44
5.3 Sigurno internetsko bankarstvo....45
5.3.1 Koristi se sigurno online plaćanje....46
5.3.2 Blokator daljinskog pristupa....46
5.3.3 Dodavanje Zaštite bankarstva za određene web-stranice....47
5.4 Sigurna online kupnja....48
5.5 Blokiranje oglasa na web-mjestima....49
5.6 Odbijanje nepotrebnih kolačića....49
5.7 Provjera koriste li se proširenja preglednika....50
5.7.1 Instaliranje i omogućavanje proširenja preglednika za Chrome....50
5.7.2 Instaliranje i omogućavanje proširenja preglednika za Edge....51
5.7.3 Instaliranje i omogućavanje proširenja preglednika za Firefox....51
6 Spremište za lozinke....53
6.1 Početak rada sa Spremištem za lozinke....53
6.2 Korištenje trezora lozinki....54
6.2.1 Prijava na internetsku uslugu sa Spremištem za lozinke....55
6.2.2 Pohranjivanje nove lozinke u Spremište za lozinke....56
6.2.3 Pohranjivanje podataka vaše platne kartice u Spremište za lozinke...57
6.2.4 Uređivanje postojećih podataka....58
6.2.5 Brisanje unosa....58
6.2.6 Dopuštanje aplikaciji da generira novu lozinku za postojeći unos....58
6.2.7 Pristup vašim starim lozinkama....59
6.2.8 Provjerite jesu li vaše lozinke jake....60

6.3 Povezivanje uređaja za sinkronizaciju vaših podataka iz Spremišta za lozinke na svim vašim uređajima 60
6.4 Postavljanje automatske ispune za brži pristup uslugama na mreži 61
6.5 Uvoz lozinki iz drugih upravitelja lozinki....63
6.6 Izvoz podataka iz trezora lozinki....64
6.7 Promjena glavne lozinke....64
6.8 Stvaranje QR koda za oporavak za glavnu lozinku....65
6.9 Upotreba QR koda za oporavak u svrhu oporavka vaše zaboravljene glavne lozinke 65
6.10 Otključavanje i zaključavanje Spremišta za lozinke 66
7 Nadzor ID-a 67
7.1 Dodavanje stavki za praćenje 67
7.2 Brisanje nadziranih stavki....68
7.3 Promjena adrese e-pošte za kontakt 69
8 Tehnička podrška....70
8.1 Gdje pronaći ID računa? 70
8.2 Gdje se nalaze podaci o verziji proizvoda? 70
8.3 Korištenje alata za podršku....70
8.4 Otklanjanje pogrešaka proizvoda....71
8.5 Ponovno postavljanje predmemorije reputacije 72
8.6 Telefonske prijevare i što učiniti ako mislite da ste meta....72

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 proizvoda na vaš prvi uređaj

Nakon što stvorite svoj račun za A1 Sigurniji internet, možete preuzeti i instalirati proizvod na svoj prvi uređaj putem portala Moj A1 Sigurniji internet.

Također možete upotrijebiti Moj A1 Sigurniji internet za slanje veze za instalaciju proizvoda na drugi uređaj e-poštom ili SMS porukom, što vam olakšava početak instalacije proizvoda na svim drugim uređajima koje želite zaštititi.

Bilješka: Da biste bili sigurni da proizvod radi kako je predviđeno, uklonite sve antivirusne proizvode trećih strana u sukobu s računala, ako ih ima.

2.1.1 Instaliranje proizvoda na računalo

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 Windows 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 Windows 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) Pratite upute za instalaciju poslane na uređaj.

Bilješka: Ako koristite Windows 11 u načinu rada S, on dopušta samo aplikacije iz trgovine Microsoft Store. Da biste mogli preuzeti naš instalacijski paket, morate napustiti način rada S. Za informacije o tome kako napustiti način rada S, pogledajte sljedeći članak Službe za podršku tvrtke Microsoft: Napuštanje načina rada S u sustavu Windows. Također imajte na umu da ćete, ako izađete iz načina rada S, morati nastaviti koristiti standardnu verziju sustava Windows 11.

5. 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.

6. Kada instalacija završi, otvorite aplikaciju.

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 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**.

2.1.2 Deinstaliranje proizvoda

Upute o tome kako deinstalirati proizvod s vašeg računala sa sustavom Windows.

Način deinstalacije programa s računala ovisi o verziji operativnog sustava Windows. U ovoj temi opisujemo jedan način deinstalacije za verzije sustava Windows koje naš proizvod podržava.

Za deinstalaciju proizvoda u sustavu Windows 11:

1. Otvorite **izbornik Start** i kliknite **Postavke**.

2. U odjeljku **Aplikacije** > **Instalirane aplikacije** potražite proizvod A1 Sigurniji internet.

3. Kliknite gumb **Više opcija** pored A1 Sigurniji internet proizvoda i odaberite **Deinstaliraj**. Zatim će se od vas tražiti da potvrdite da želite deinstalirati proizvod.

4. Odaberite **Deinstaliraj**. Ako se to zatraži, unesite administratorske vjerodajnice.

Za deinstalaciju proizvoda u sustavu Windows 10:

1. Otvorite **izbornik Start** i kliknite **Postavke**.

2. U odjeljku **Aplikacije** > **Aplikacije i značajke** kliknite proizvod A1 Sigurniji internet.

3. Kliknite **Deinstaliraj**. Zatim će se od vas tražiti da potvrdite da želite deinstalirati proizvod.

4. Odaberite **Deinstaliraj**. Ako se to zatraži, unesite administratorske vjerodajnice.

Za deinstalaciju proizvoda u sustavima Windows 7 i 8:

1. Otvorite **izbornik Početak**, zatim odaberite **Upravljačka ploča**.

2. Odaberite **Deinstaliraj program** ili **Programi i značajke**, ovisno o tome u kojem ste prikazu.

3. Pod opcijom **Programi i značajke** pomičite se prema dolje do proizvoda i kliknite na njega da biste ga istaknuli.

4. Odaberite **Deinstaliraj**.

5. Odaberite **Da** da biste potvrdili deinstalaciju.

6. Ako se to zatraži, ponovo pokrenite računalo.

Bilješka: Kada deinstalirate proizvod sa svog računala, ne zaboravite također poništiti njegovu licencu u aplikaciji A1 Sigurniji internet. Tek tada možete 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  .

Otvara se kontekstni izbornik koji vam prikazuje adresu e-pošte upotrijebljenu za prijavu na račun, valjanost vaše pretplate i naziv trenutačno zaštićenog uređaja.

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.

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.

2.4.1 Brz pristup postavkama proizvoda

Nekim postavkama proizvoda možete pristupiti putem kontekstnog izbornika ikone u paleti sustava.

Da biste otvorili kontekstni izbornik ikone u paleti sustava, slijedite ove upute:

1. Kliknite desnom tipkom miša ikonu proizvoda na programskoj traci sustava Windows.

Bilješka: Ako je ikona proizvoda skrivena, najprije kliknite strelicu **Pokaži skrivene ikone**.

2. Na kontekstnom izborniku nalaze se sljedeće mogućnosti.

Mogućnost	Opis
Otvori	Otvara korisničko sučelje sigurnosnog proizvoda.
Potraži ažuriranja	Traži i preuzima najnovija ažuriranja.
Prikaži nedavne događaje	Prikazuje radnje koje je proizvod poduzeo za zaštitu računala.
Otvori postavke	Otvara postavke proizvoda.
O programu	Prikazuje podatke o verziji proizvoda.
Renderiranje putem softvera	Pomaže u rješavanju problema korisničkog sučelja povezanih s renderiranjem. **Bilješka:** Da biste vidjeli ovu opciju u izborniku, pritisnite i držite tipku shift i istovremeno desnom tipkom miša kliknite ikonu palete sustava proizvoda.

2.4.2 Upotreba načina rada za igranje

U ovoj se temi navode informacije o načinu rada za igranje koji je dostupan u proizvodu.

Za automatski način rada za igranje na računalu morate imati Windows 10 verzije 1809 ("ažuriranje za listopad 2018.") ili noviju verziju.

Način rada za igranje prema zadanim je postavkama omogućen u proizvodu. Čim proizvod otkrije da na računalu pokrećete igru, automatski zaustavlja sve zakazane preglede i obustavlja ažuriranja proizvoda i baze podataka. Time se smanjuje utjecaj proizvoda na upotrebu računala i mreže. Oslobađa se više sistemskih resursa za računalne igre, a pritom se zadržavaju nužne funkcije proizvoda. Način rada za igranje automatski se isključuje kad prestanete igrati igru.

Bilješka: Ako na više od 60 sekundi s igre prijeđete na neku drugu otvorenu aplikaciju kombinacijom tipki Alt + tab, proizvod pretpostavlja da ste prestali igrati i isključuje način rada za igranje.

Ako ne želite da se način rada za igranje uključuje automatski, isključite ga na sljedeći način:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu odaberite gornji lijevi gumb izbornika ☰.

3. Odaberite **Postavke** > **Postavke pregleda.**

4. Odaberite **Uređivanje postavki**.

5. Isključite način rada za igranje.
Sad se način rada za igranje neće automatski uključivati.

Bilješka: U prikazu **Postavke** možete vidjeti kad je zadnji put započela sesija igranja.

Što učiniti ako se način rada za igranje ne pokrene kad i igra?

U ovoj se temi navode upute za to što učiniti ako se u sustavu Windows ne pokrene način rada za igranje.

Način rada za igranje prema zadanim se postavkama aktivira kad Windows otkrije da je pokrenuta igra.

No Windows katkad možda neće prepoznati igru, pa se način rada za igranje neće aktivirati. U tom slučaju na sljedeći način možete ručno dodati otkrivanje te igre na traku igre za Xbox:

1. Pokrenite igru.

2. Pritisnite **tipku s logotipom sustava Windows + G**.
Otvara se **traka igre**.

3. Na traci igre odaberite **Postavke** > **Općenito** pa potvrdite okvir **Zapamti da je ovo igra**.

Bilješka: Ako ne vidite tu postavku, traka igre već prepoznaje igru.

Proizvod će odsad nadalje svaki put aktivirati način rada za igranje čim pokrenete igru.

Bilješka: Tu postavku možete upotrebljavati za igre kupljene u bilo kojoj trgovini igara.

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 za preglednik Microsoft Edge nije u upotrebi**
- **Pretplata je istekla**

2.5.2 Prikaz statistike zaštite

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

Proizvod vam prikazuje rotirajući brojač statistike zaštite u prikazima **Zaštita uređaja** i **Sigurno pregledavanje**.

Prikaz **Pretplata** prikazuje istu statistiku na jednom mjestu:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu odaberite gornji lijevi gumb izbornika .

3. Odaberi **Pretplata**.
U prikazu **Pretplata** možete vidjeti kako je proizvod zaštitio vaš uređaj i vaše pregledavanje.

Statistika	Opis
Datoteke su provjerene	Broj datoteka koje je proizvod pregledao. Zbroj obuhvaća statistiku za sve korisničke račune na ovom računalu. **Bilješka:** To obuhvaća duplicirane preglede, pa se zbroj, primjerice, poveća za dva ako proizvod dvaput pregleda istu datoteku.
Zaštićene sesije internetskog bankarstva	Broj sesija internetskog bankarstva koje je proizvod zaštitio. Broj se poveća svaki put kad se aktivira značajka sigurnog online plaćanja kad pristupite web mjestu za internetsko bankarstvo.
Provjerene su web-adrese	Broj web-mjesta koja ste posjetili, a za koja je proizvod provjerio reputaciju.
Blokirane potencijalno štetne datoteke	Broj štetnih, potencijalno neželjenih i neželjenih datoteka koje je proizvod blokirao. To ne obuhvaća preuzete datoteke koje je proizvod blokirao prije pohranjivanja na računalo. Zbroj obuhvaća statistiku za sve korisničke račune na ovom računalu. **Bilješka:** Ako proizvod, primjerice, dvaput blokira istu datoteku, zbroj se povećava za dva.
Blokirana štetna webmjesta	Broj štetnih web-mjesta koja je proizvod blokirao.

2.5.3 Prikaz nedavnih događaja za proizvod

Na stranici **Povijest događaja** možete pogledati što je proizvod radio i kako je štitio vaše računalo.

U glavnom prikazu proizvoda možete vidjeti najnovije događaje povezane s proizvodom.

Povijest događaja prikazuje različite događaje za instalirani proizvod i pojedinosti o zaštitnim mjerama koje je proizvod poduzeo. Na primjer, prikazuje vam sve štetne stavke koje su otkrivene i izbrisane ili stavljene u karantenu.

Prikaz cijele povijesti događaja u proizvodu:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. U donjem desnom kutu glavnog prikaza proizvoda odaberite **Prikaži cijelu vremensku crtu**. Otvorit će se stranica **Povijest događaja**.

Povijest događaja prikazuje vrijeme i opis svakog događaja. Ovisno o vrsti događaja, dodatne pojedinosti o događaju možete pronaći u stupcu **Više**. Na primjer, za štetne datoteke možete vidjeti sljedeće informacije:

- Datum i vrijeme pronalaska štetne datoteke
- Naziv zlonamjernog softvera i njegovu lokaciju na računalu te
- Provedenu radnju.

2.5.4 Promjena postavki obavijesti

U ovoj se temi navode upute za promjenu obavijesti koje se prikazuju.

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu odaberite gornji lijevi gumb izbornika .

3. Odaberite **Postavke**.

4. Odaberite **Obavijesti**.

5. Odaberite ili poništite **Prikazuj korisne savjete i ažuriranja**.

Kada je ova postavka uključena, proizvod prikazuje obavijesti o novostima, savjetima i posebnim ponudama. Obavijesti o kritičnim proizvodima uvijek se prikazuju čak i ako ova postavka nije odabrana.

2.5.5 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.

Savjet: Ažuriranja možete brzo provjeriti i tako da desnom tipkom miša kliknete ikonu proizvoda u traci sustava te odaberete **Provjeri ima li ažuriranja**. Proizvod provjerava nova ažuriranja i odmah ih instalira.

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.

3. Kako biste potvrdili da se želite odjavite, odaberite **Da, odjavi se**.
Sada ste odjavljeni iz aplikacije na ovom uređaju.

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.

2.7 Poboljšanje proizvoda

Slanjem podataka o upotrebi možete nam pomoći da poboljšamo proizvod.

Slanje podataka o upotrebi:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu odaberite gornji lijevi gumb izbornika .

3. Odaberite **Postavke**.

4. Idite na **Privatnost** stranicu postavki.

5. Odaberite **Uređivanje postavki**.

6. U odjeljku **Poboljšanje proizvoda** odaberite **Šalji depersonalizirane podatke o korištenju**.

Bilješka: Možete pročitati našu Izjavu o privatnosti ovdje.

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 A1 Sigurniji internet račun i zaštitili svoj prvi uređaj, možete nastaviti štititi svoje ostale uređaje putem instalirane sigurnosne aplikacije.

Da biste počeli štititi svoje druge uređaje putem aplikacije:

1. Otvorite aplikaciju A1 Sigurniji internet.

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

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

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 odgovarajući instalacijski paket za uređaj i pokrenite instalacijski program.

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

9. 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 **Uređivanje postavki**.

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) Odaberite **Dodaj novo**.
c) Unesite adresu web-stranice koju želite dopustiti.
d) Odaberite **U redu**.

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.

4.2.2 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. Otvorite aplikaciju A1 Sigurniji internet.

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

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

4. Odaberi **Uređaj neke druge osobe** > **Nastaviti**.

5. 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. Otvorite aplikaciju A1 Sigurniji internet.

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

3. Odaberite podkorisnika s kojim želite prestati dijeliti zaštitu.

4. Izaberite **Ukloni iz grupe**.

5. 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**,

6. 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.

Proizvod prati i ima li na računalu promjena koje mogu upućivati na to da se na njemu nalaze štetne datoteke. Kada proizvod otkrije opasne promjene sustava, primjerice promjene postavki sustava ili pokušaje promjene važnih procesa sustava, proizvod zaustavlja aplikaciju jer bi mogla biti štetna.

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 štetan sadržaj, stavlja datoteku u karantenu prije nego što može prouzročiti 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.

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. Otvorite aplikaciju A1 Sigurniji internet.

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

3. Odaberite **Postavke**.

4. Pod, ispod **Zaštita od virusa,** odaberite vezu "Privremeno isključi automatsko skeniranje".

Bilješka: Za pristup postavkama potrebna su vam administratorska prava.

Otvara se prozor **Isključite automatsko skeniranje**.

5. Kako biste smanjili rizike, prvo odaberite vrijeme kada želite ponovno automatski uključiti

skeniranje, a zatim odaberite **Isključiti**.

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.

4.2 Pokretanje pregledavanja zlonamjernog softvera

Da biste bili potpuno sigurni da na računalu nema štetnih datoteka ni neželjenih aplikacija, možete ga u potpunosti pregledati.

Potpuno skeniranje računala skenira sve interne i vanjske tvrde diskove u potrazi za virusima, špijunskim softverom i potencijalno neželjenim aplikacijama. Potpuno skeniranje računala može potrajati. Također možete skenirati samo dijelove sustava koji sadrže instalirane aplikacije kako biste učinkovitije pronašli i uklonili neželjene aplikacije i štetne stavke na računalu.

Da biste pregledali računalo, slijedite ove upute:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Ako želite optimizirati način na koji ručno skeniranje skenira vaše računalo, odaberite **Zaštita uređaja** > **Postavke**.
a) U odjeljku **Zaštita uređaja** pomaknite se prema dolje do **Ručno skeniranje**.
b) Ako ne želite pregledati sve datoteke, odaberite **Pregledaj samo vrste datoteka koje obično sadrže štetni kod (brži način)**.
Primjeri su poznatih vrsta datoteka datoteke sa sljedećim nastavcima: com, doc, dot, exe, htm, ini, jar, pdf, scr, wma, xml, zip.
c) Da biste pregledali datoteke koje se nalaze unutar komprimiranih arhivskih datoteka, npr. zip datoteka, odaberite **Pregledaj unutar komprimiranih datoteka (sporije)**. Ako odaberete tu mogućnost, pregledavanje će trajati dulje. Da biste pregledali arhivsku datoteku, ali ne i datoteke koje se nalaze unutar nje, nemojte označiti ovu opciju.
d) Zatvori **Postavke** prozor.

3. Vratit ćete se natrag na **Zaštita uređaja** pogled, odaberite bilo koji **Brzo skeniranje** > **Pokrenite brzo skeniranje** ili **Kompletno skeniranje** > **Započni skeniranje**.
▪ **Brzo skeniranje** skenira samo dijelove vašeg sustava koji sadrže instalirane aplikacije, a zatim lokacije na kojima se obično nalaze virusi, uključujući mape dokumenata. Može pronaći i ukloniti neželjene aplikacije i štetne stavke na vašem računalu u kraćem vremenu.
▪ **Kompletno skeniranje** skenira sve unutarnje i vanjske tvrde diskove u potrazi za virusima, špijunskim softverom i potencijalno neželjenim aplikacijama. Potpuno skeniranje računala može potrajati dugo.
Skeniranje počinje. Tijekom skeniranja možete vidjeti detekcije, ako ih ima, u krugu napretka. Možete vidjeti pojedinosti svake detekcije tako da iznad njih prijeđete mišem.

4. Ako skeniranje pronađe štetne stavke, prikazuje popis otkrivenih štetnih stavki.

5. Kliknite otkrivenu stavku da biste odabrali način na koji želite rukovati štetnim sadržajem.

Mogućnost	Opis
Očisti	Automatski očistite datoteke. Datoteke koje se ne mogu očistiti stavljaju se u karantenu.
Karantena	Pohranite datoteke na sigurno mjesto gdje se ne mogu širiti ni štetiti računalu.
Izbriši	Trajno uklonite datoteke s računala
Preskoči	Nemojte ništa učiniti i zadržite datoteke na računalu.

Izuzmi	Dopustite aplikaciju da biste je pokrenuli i isključili iz budućih pregledavanja.

Bilješka: Neke mogućnosti nisu dostupne za sve vrste štetnih stavki.

6. Da biste pokrenuli proces čišćenja, odaberite **Rukuj svima**.

7. Skeniranje pokazuje konačne rezultate i broj štetnih predmeta koji su očišćeni.

Skeniranje može zahtijevati da ponovno pokrenete računalo kako biste dovršili proces čišćenja. Ako čišćenje zahtijeva ponovno pokretanje računala, odaberite **Ponovno pokretanje** dovršite čišćenje štetnih stavki i ponovno pokrenite računalo.

4.2.1 Spremanje izvješća o skeniranju u datoteku

Ova tema opisuje kako spremiti izvješće o skeniranju u datoteku.

Za spremanje izvješća o skeniranju u datoteku:

1. Otvorite aplikaciju A1 Sigurniji internet.

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

3. Za početak skeniranja odaberite bilo koji **Brzo skeniranje** > **Pokrenite brzo skeniranje** ili **Kompletno skeniranje** > **Započni skeniranje**.

4. Nakon što skeniranje završi, odaberite **Pogledajte izvješće o skeniranju**.
Ovo otvara izvješće u html formatu u vašem zadanom pregledniku.

5. Za spremanje izvješća u datoteku desnom tipkom miša kliknite stranicu izvješća i odaberite **Spremi kao...**

6. Datoteci dajte opisni naziv i spremite je.

4.3 Pregledavanje stavki u karanteni

Proizvod stavlja štetne predmete i potencijalno neželjene aplikacije u karantenu kako bi ih učinio bezopasnima.

Karantena je sigurno spremište za datoteke i aplikacije koje automatsko skeniranje smatra potencijalno štetnima. Aplikacije ili datoteke iz karantene možete kasnije vratiti ako vam trebaju. Ako vam stavka u karanteni nije potrebna, možete je izbrisati. Brisanjem stavke u karanteni trajno je uklanjate s računala.

Za prikaz više informacija o stavkama u karanteni:

1. Otvorite aplikaciju A1 Sigurniji internet.

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

3. U prikazu **Zaštita uređaja** odaberite **Upravljanje izuzecima skeniranja**.

Bilješka: Da biste pristupili tim postavkama, potrebna su vam administratorska prava.

4. Odaberite karticu **U karanteni**.
Na popisu su prikazani naziv, datum otkrivanja i vrsta zaraze za svaku stavku u karanteni.

5. Dvaput kliknite na stavku u karanteni da biste vidjeli više informacija o njoj.
Za pojedinačne stavke to vam pokazuje izvornu lokaciju stavke u karanteni.

4.3.1 Vraćanje stavki iz karantene

Možete vratiti stavke iz karantene koje su vam potrebne.

Možete vratiti aplikacije ili datoteke iz karantene ako ih trebate. Ne vraćajte stavke iz karantene osim ako niste sigurni da ne predstavljaju prijetnju. Stavke koje vratite vraćaju se na izvornu lokaciju na vašem računalu.

Da biste vratili stavke u karanteni:

1. Otvorite aplikaciju A1 Sigurniji internet.

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

3. U prikazu **Zaštita uređaja** odaberite **Upravljanje izuzecima skeniranja**.

Bilješka: Da biste pristupili tim postavkama, potrebna su vam administratorska prava.

4. Odaberite karticu **U karanteni**.

5. Odaberite stavke u karanteni koje želite vratiti.

6. Odaberite **Dopusti**.

7. Odaberite **Da** kako biste potvrdili da želite vratiti stavku iz karantene.
Odabrana stavka automatski se vraća na izvornu lokaciju.

Ovisno o vrsti infekcije, stavka može biti isključena iz budućih skeniranja. Za pregled svih trenutno izuzetih datoteka i aplikacija odaberite **Isključen** karticu u **Upravljanje izuzecima skeniranja** pogled.

4.4 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**.

Bilješka: Da biste pristupili tim postavkama, potrebna su vam administratorska prava.

4. Odaberite karticu **Izuzeto**.
Ovaj prikaz sadrži popis izuzetih datoteka i mapa.

5. Odaberite **Dodaj novo**.

6. Odaberite datoteke ili mape koje želite izuzeti.

7. Odaberite **U redu**.
Odabrane datoteke ili mape izuzete su iz budućih pregledavanja.

4.5 Zakazivanje pregledavanja

Postavite računalo tako da automatski pregledava i uklanja viruse i druge štetne aplikacije kada ga ne koristite ili pak postavite redovite intervale pregledavanja da biste bili sigurni da je čisto.

Da biste zakazali pregledavanje:

1. Otvorite aplikaciju A1 Sigurniji internet.

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

3. U prikazu **Zaštita uređaja** odaberite **Postavke**.

4. Odaberite **Uređivanje postavki**.

5. Pomaknite se prema dolje do **Zakazano skeniranje** i uključite ga.

6. U odjeljku **Izvrši pregledavanje** odaberite koliko često želite automatski pregledati računalo.

Mogućnost	Opis
Svakodnevno	Računalo se pregledava svakodnevno.
Tjedno	Skenirajte svoje računalo na odabrani dan u tjednu. Odaberite dan u tjednu s popisa.
Mjesečno	Skenirajte svoje računalo prvi put odabranog radnog dana svakog mjeseca. Odaberite dan u tjednu s popisa.

7. U odjeljku **Vrijeme početka** odaberite kada zakazani pregled počinje.

8. Ako ne želite pregledati sve datoteke, odaberite **Pregledaj samo vrste datoteka koje obično sadrže štetni kod (brži način)**.
Primjeri su poznatih vrsta datoteka datoteke sa sljedećim nastavcima: com, doc, dot, exe, htm, ini, jar, pdf, scr, wma, xml, zip.

9. Da biste pregledali datoteke koje se nalaze unutar komprimiranih arhivskih datoteke, npr. zip datoteka, odaberite **Pregledaj unutar komprimiranih datoteka (sporije)**. Ako odaberete tu

mogućnost, pregledavanje će trajati dulje. Da biste pregledali arhivsku datoteku, ali ne i datoteke koje se nalaze unutar nje, nemojte označiti ovu opciju.

Bilješka: Zakazana skeniranja se otkazuju kada je uključen način rada za igranje. Kad okreneš *način igre u* isključeni, skeniranja se opet vrte prema rasporedu.

Na glavnom prikazu proizvoda, ispod **Nedavni događaji** , možete vidjeti napredak zakazanog skeniranja. Ako želite otkazati zakazano skeniranje koje je u tijeku, odaberite **Pogledajte cijelu vremensku traku** u donjem desnom kutu za otvaranje **Povijest događaja** pregledajte, pronađite predmetno planirano skeniranje i odaberite **Otkazati**.

4.6 Skeniranje u Windows Exploreru

Možete pregledavati diskove, mape i datoteke u potrazi za štetnim datotekama i neželjenim aplikacijama u programu Windows Explorer.

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.

Da biste pregledali disk, mapu ili datoteku:

1. Desnom tipkom miša kliknite disk, mapu ili datoteku koje želite pregledati.

2. S kontekstnog izbornika odaberite **Traži viruse**.

Bilješka: U sustavu Windows 11 odaberite **Prikaži više opcija** a zatim odaberite **Skenirajte viruse** .
Pokreće se antivirusno pregledavanje te se pregledava odabrani disk, mapa ili datoteka.

Ako se tijekom pregledavaju otkriju štetne datoteke ili neželjene aplikacije, protuvirusno pregledavanje vodi vas kroz faze čišćenja.

4.7 Omogućavanje blokiranih aplikacija

Možete kontrolirati koje aplikacije proizvod omogućuje i blokira.

Ponekad proizvod može spriječiti pokretanje sigurne aplikacije, čak i ako želite upotrebljavati aplikaciju i znate da je sigurna. To se događa jer aplikacija pokušava izvršiti promjene sustava koje bi mogle biti potencijalno štetne.

Omogućivanje aplikacije koja je blokirana:

1. Otvorite aplikaciju A1 Sigurniji internet.

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

3. U prikazu **Zaštita uređaja** odaberite **Upravljanje izuzecima skeniranja**.

Bilješka: Da biste pristupili tim postavkama, potrebna su vam administratorska prava.

4. Odaberite karticu **Blokirano**.
To prikazuje popis aplikacija koje su blokirane.

5. Pronađite aplikaciju koju želite omogućiti i odaberite **Omogući**.

6. Odaberite **Da** kako biste potvrdili da želite omogućiti aplikaciju.
Odabrana aplikacija dodaje se na popis **Izuzeto** i dopušta joj se da ponovno unosi promjene sustava.

4.7.1 Upravljanje izuzetim aplikacijama

Možete pregledati aplikacije koje ste isključili iz skeniranja i, ako želite, ukloniti ih s popisa izuzetih stavki ako ih želite ponovno krenuti skenirati.

Zaštita uređaja nadzire vaše računalo i osigurava da koristite samo sigurne aplikacije. Ako otkrije potencijalno neželjenu aplikaciju za koju znate da je sigurna ili špijunski softver koji trebate držati na računalu da biste koristili neku drugu aplikaciju, možete je isključiti iz skeniranja kako vas proizvod više ne bi upozoravao na to.

Međutim, ako se aplikacija ponaša kao virus ili druga štetna aplikacija, ne možete je isključiti. Također, Zaštita uređaja ne blokira određene Steam igre. Stoga ne morate isključiti Steam igre iz skeniranja ili isključiti Virus Protection da biste ih pokrenuli.

Za pregled aplikacija koje su izuzete iz skeniranja:

1. Otvorite aplikaciju A1 Sigurniji internet.

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

3. U prikazu **Zaštita uređaja** odaberite **Upravljanje izuzecima skeniranja**.

Bilješka: Da biste pristupili tim postavkama, potrebna su vam administratorska prava.

4. Odaberite karticu **Izuzeto**.
Ovaj prikaz sadrži popis izuzetih datoteka i mapa.

5. Ako želite ponovno skenirati izuzetu aplikaciju:
a) Odaberite aplikaciju koju želite uvrstiti u pregledavanje.
b) Kliknite **Ukloni**.

Nove aplikacije ne mogu se izravno dodati na popis isključenja; pojavljuju se na popisu izuzetaka tek nakon što ih isključite tijekom skeniranja.

4.8 Sprječavanje aplikacija da zatvore sigurnosne procese

Zaštita od neovlaštenog mijenjanja sprječava štetne aplikacije da isključe temeljne sigurnosne procese proizvoda.

Zaštita od neovlaštenog mijenjanja štiti instalirani sigurnosni proizvod i njegove usluge, procese, datoteke i unose registra od promjena ili bilo kakvih pokušaja kontrole.

Prema zadanim postavkama, tamper protection je uključena kada instalirate sigurnosni proizvod na svoje računalo.

Kako biste bili sigurni da je tamper protection uključena:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Ako se u glavnom prikazu proizvoda prikazuje obavijest o isključenim značajkama za zaštitu, odaberite **Uključi sve**.
Za detaljnije informacije o isključenim značajkama za zaštitu odaberite **Više pojedinosti...**

3. Ako propustite obavijest na glavnoj stranici proizvoda, možete uključiti sve značajke zaštite u prikazu **Zaštita uređaja** tako da odaberete **Zaštita uređaja** > **Uključi sve**.
Ako ste namjerno isključili neke od značajki za zaštitu, razumijete rizike i ne želite više vidjeti obavijest, odaberite **Ne pitaj više**.

Također možete pristupiti postavkama tamper protection mijenjanja iz postavki proizvoda odabirom **Postavke** > **zaštite uređaja**.

4.9 Koristi se AMSI integracija da bi se napadi prepoznavali na temelju skripti

Sučelje za pregled protiv zlonamjernog softvera (AMSI) komponenta je sustava Microsoft Windows koja omogućuje dublji pregled ugrađenih servisa za skriptiranje.

Napredni zlonamjerni softver koristi skripte koje su prikrivene ili šifrirane da bi izbjegao tradicionalne načine skeniranja. Takav se zlonamjerni softver često učitava izravno u memoriju, pa ne koristiti nikakve datoteke na uređaju.

AMSI je sučelje koje aplikacije i usluge koje se izvode u sustavu Windows mogu koristiti za slanje zahtjeva za skeniranje antimalware proizvodu instaliranom na računalu. Ovo pruža dodatnu zaštitu od štetnog softvera koji koristi skripte ili makronaredbe na osnovnim komponentama sustava Windows, kao što su PowerShell i Office365, ili drugim aplikacijama za izbjegavanje otkrivanja.

Prema zadanim postavkama AMSI se uključuje kada instalirate sigurnosni proizvod na svoje računalo.

Proizvod vas obavještava o svakom štetnom sadržaju koji AMSI otkrije i bilježi te detekcije u povijesti događaja.

Da bismo se uvjerili u to:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Ako se u glavnom prikazu proizvoda prikazuje obavijest o isključenim značajkama za zaštitu, odaberite **Uključi sve**.
Za detaljnije informacije o isključenim značajkama za zaštitu odaberite **Više pojedinosti...**

3. Ako propustite obavijest na glavnoj stranici proizvoda, možete uključiti sve značajke zaštite u prikazu **Zaštita uređaja** tako da odaberete **Zaštita uređaja** > **Uključi sve**.
Ako ste namjerno isključili neke od značajki za zaštitu, razumijete rizike i ne želite više vidjeti obavijest, odaberite **Ne pitaj više**.

Postavci AMSI također možete pristupiti iz postavki proizvoda odabirom **Postavke** > **zaštite uređaja**.

4.10 Što radi štetan sadržaj

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

4.10.1 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.

4.10.2 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

4.10.3 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.

4.10.4 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.

4.10.5 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.

4.10.6 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.

4.11 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.

Bilješka: Neka web-mjesta upotrebljavaju tzv. iframe okvire da bi prikazivala sadržaj izravno s drugih web-mjesta. Aplikacija blokira sve iframe okvire u kojima otkrije štetan izvorni sadržaj. To znači da neki dijelovi inače sigurne stranice mogu izgledati neispravno. Aplikacija će prikazati skočni prozor na web mjestu za sve iframe okvire koje blokira.

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

Zaštita pregledavanja kompatibilna je s web-preglednicima 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 **Uređivanje postavki**.

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 stranicama kada je uključena.

Zaštita pregledavanja automatski se uključuje kada stavite proizvod u upotrebu.

Bilješka: Neka web-mjesta upotrebljavaju tzv. iframe okvire da bi prikazivala sadržaj izravno s drugih

web-mjesta. Aplikacija blokira sve iframe okvire u kojima otkrije štetan izvorni sadržaj. To znači da neki dijelovi inače sigurne stranice mogu izgledati neispravno. Aplikacija će prikazati skočni prozor na web mjestu za sve iframe okvire koje blokira.

Provjerite je li uključena zaštita pregledavanja.

1. Otvorite aplikaciju A1 Sigurniji internet.

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

3. Odaberite **Postavke**.

4. Odaberite **Uređivanje postavki**.

5. Uključite **Zaštitu pregledavanja**.

6. 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.

5.2.1 Automatsko blokiranje sumnjivih i zabranjenih web-mjesta

Zaštita pregledavanja može vas spriječiti pri nehotičnom pristupu web-mjestima koja nisu pouzdana ili na kojima se nalazi zabranjeni sadržaj.

Ponekad ćete možda naići na web mjesto na kojem se nalazi sumnjiv sadržaj, sadržaj koji krši tuđa prava ili zabranjen sadržaj. Web mjesto može, primjerice, biti lažno web mjesto koje je poznato po širenju neželjenog sadržaja, može sadržavati potencijalno neželjene programe ili pak može biti zakonom zabranjeno bez obzira na to gdje se nalazite.

Da biste izbjegli nenamjerno pristupanje ovim web-mjestima:

1. Otvorite aplikaciju A1 Sigurniji internet.

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

3. Odaberite **Postavke**.

4. Odaberite **Uređivanje postavki**.

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

6. Ako, uz ona koja se smatraju štetnima, želite blokirati i web-mjesta koja su ocijenjena kao sumnjiva, odaberite **Blokiraj sumnjiva web-mjesta**.

7. Ako želite blokirati web-mjesta sa zabranjenim sadržajem, odaberite **Blokiraj zabranjena web-mjesta**.

8. 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.

5.2.2 Ručno blokiranje web-stranica

Možete ručno blokirati web-mjesta za koja mislite da su štetna ili neprikladna.

Da biste ručno blokirali 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**.

Bilješka: Da biste promijenili postavke, potrebna su vam administratorska prava.

4. Odaberite karticu **Blokirano**.

5. Odaberi **Dodaj novo** za dodavanje novog web-mjesta na popis.

6. Unesite adresu web-mjesta koje želite dodati, a zatim odaberite **U redu**
▪ Za blokiranje svih stranica na određenom web mjestu unesite domenu tog web-mjesta. Na primjer, example.com blokovi http://www.example.com i bilo koja druga stranica koja upotrebljava istu domenu, kao što je https://test.example.com/samples.
▪ Da biste blokirali samo skup stranica unutar mjesta koje upotrebljava slične adrese, unesite dio adrese. Na primjer, example.com/sampl blokovi http://www.example.com/sample, https://test.example.com/samples, i http://example.com/sampling.

Proizvod ne podržava upotrebu zamjenskih znakova, na primjer *.

Web mjesto je sada navedeno kao blokirano.

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

5.2.3 Ručno dopuštanje blokiranih web-mjesta

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

Bilješka: Ako se stranica za blokiranje ne prikaže, provjerite je li proširenje Zaštita pregledavanja uključeno u web-pregledniku koji koristite.

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

1. Odaberite **Dopusti web mjesto na ovom računalu**. Da biste dopustili blokirana web-mjesta, potrebna su vam administratorska prava.
Otvorit će se prozor **Dodavanje dopuštenog web-mjesta** s prikazanom adresom koju ćete dopustiti.

2. Odaberite **U redu**.

Otvorit će se blokirano web mjesto. Uz to, proizvod će web mjesto dodati na popis dopuštenih webmjesta.

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

5.2.4 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 **Upravljanje dopuštenim i blokiranim web-mjestima**.

Bilješka: Da biste promijenili postavke, potrebna su vam administratorska prava.

4. Odaberite karticu **Dopušteno**.

5. Odaberi **Dodaj novo** za dodavanje novog web-mjesta na popis.

6. Unesite adresu web-mjesta koje želite dodati, a zatim odaberite **U redu**

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**.

5.2.5 Uvoz i izvoz popisa blokiranih i dopuštenih web-mjesta

Možete izvesti blokirana i dopuštena web-mjesta te ih uvesti ako trebate ponovno instalirati proizvod, na primjer.

Kada ste dodali web-mjesta koja želite blokirati ili dopustiti, možete izvesti taj popis web-mjesta u JSON datoteku. Zatim možete uvesti datoteku da primijenite isti popis web-mjesta na drugom računalu ili ako trebate ponovno instalirati proizvod.

1. Otvorite aplikaciju A1 Sigurniji internet.

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

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

Bilješka: Da biste promijenili postavke, potrebna su vam administratorska prava.

4. Odaberite karticu **Dopušteno** ili **Blokirano**.

Za izvoz navedenih web-mjesta:
a) Kliknite na **Izvoz**.
b) Idite do mape u koju želite spremiti datoteku, unesite naziv datoteke i kliknite na **Spremi**.

Za uvoz popisa web-mjesta:
a) Kliknite na **Uvoz**.
b) Potražite mapu koja sadrži prethodno izvezenu datoteku, odaberite datoteku i kliknite na **Otvori**.

Uvezena web-mjesta dodaju se na popis dopuštenih ili blokiranih web-mjesta.

5.3 Sigurno internetsko bankarstvo

Zaštita bankarstva dodaje još jedan sloj sigurnosti kako bi se spriječilo napadače da se upliću u vaše povjerljive transakcije i štiti vas od štetnih aktivnosti kada pristupate svojoj banci ili obavljate druge transakcije na mreži.

Kontrola povezivanja automatski prepoznaje sigurne veze s web-mjestima za internetsko bankarstvo te blokira sve veze koje ne upućuju na određeno web mjesto. Kad otvorite web mjesto internetskog bankarstva, dopuštene su samo veze prema web-mjestima internetskog bankarstva ili web-mjestima koja se smatraju sigurnima za internetsko bankarstvo.

Zaštita bankarstva trenutačno podržava sljedeće preglednike:
- Microsoft Edge (Chromium)
- Mozilla Firefox
- Google Chrome

Bilješka: Zaštita bankarstva zahtijeva da se upotrebljavaju 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 **Uređivanje postavki**.

5. Uključite **Sigurno online plaćanje**.

6. Za podešavanje postavki zaštite bankarstva:
- Izbrišite odjeljak **Odspoji nepouzdane aplikacije** ako ne želite da zaštita bankarstva zatvori već otvorene veze. Ako ostavite odabranu postavku, zaštita bankarstva zatvara vaše trenutačne internetske veze, osim za pouzdane aplikacije, kada se aktivira.
- Ako morate koristiti vanjski alat koji sesija Sigurnog online plaćanja blokira, poništite okvir **Prekini vezu alata naredbenog retka i alata za skriptiranje**.

Bilješka: Preporučujemo vam da tu postavku držite odabranom osim ako nije apsolutno nužna jer neki zlonamjerni napadi mogu koristiti ugrađene komponente sustava Windows, npr. PowerShell, da bi ostvarili pristup bankovnim vjerodajnicama i osobnim podacima.
- Odaberite na koji način želite da Zaštita bankarstva rukuje podacima koji su kopirani u vaš međuspremnik. Prema zadanim postavkama odabrana je opcija **Očistite međuspremnik nakon bankarskih sesija** i Zaštita bankarstva briše sve podatke iz međuspremnika kako bi se zaštitila vaša privatnost na kraju sesije Bankarske zaštite.

Poništite tu postavku ako ne želite da Sigurno online plaćanje čisti međuspremnik.
- Prema zadanim postavkama daljinski pristup vašem uređaju blokiran je tijekom vaše bankarske sesije. Bankovne transakcije uvijek su privatne i povjerljive i nikada se ne biste trebali prijavljivati u svoje internetsko bankarstvo ako netko ima udaljeni pristup vašem uređaju.

Važno: Ni na čiji zahtjev nemojte brisati postavku **Blokiraj daljinski pristup tijekom bankarske sesije**, osim ako ne znate i osobu koja traži pristup i točnu svrhu zahtjeva.

5.3.1 Koristi se sigurno online plaćanje

Kada je zaštita bankarstva uključena, automatski otkriva kada pristupate web-mjestima internetskog bankarstva ili drugim stranicama koje sadrže osjetljive informacije.

Kada otvorite web mjesto internetskog bankarstva u svojem pregledniku, aktivira se zaštita bankarstva te se oko zaslona vašeg računala pojavi okvir **Zaštita bankarstva** sa zelenom kvačicom na vrhu. Ovo ukazuje na to da je **Zaštita bankarstva** aktivna. Dok je aktivna, zaštita bankarstva dopušta samo veze koje smatra sigurnima, a sve su druge veze blokirane.

Ako **Zaštita bankarstva** ne prepoznaje vaše web mjesto kao stranicu za bankarstvo ili internetsku kupnju, pošaljite nam URL stranice.

Bilješka: Možda ćete htjeti promijeniti postavke proizvoda za zaštitu bankarstva kada je aktivna, na primjer:
- Ako ne želite prekidati vaše druge aktivne veze kada je zaštita bankarstva aktivna ili
- Ako ne želite da zaštita bankarstva izbriše međuspremnik kada završi sesija zaštite bankarstva.

Dok je zaštita bankarstva uključena, pristupite postavkama na sljedeći način:

1. Odaberite zelenu kvačicu na vrhu zaslona, a zatim odaberite .
Ovo otvara izbornik **Postavke**.

2. Izmijenite postavke za odjeljak **Zaštita bankarstva** prema vašim potrebama.

Nakon što zatvorite preglednik ili završite bankarsku sesiju, ne morate ništa učiniti. **Zaštita bankarstva** automatski otkriva da je bankarska sesija završila i zatvara okvir **Zaštita bankarstva**.

Bilješka: Ako se **Zaštita bankarstva** ne aktivira i ne vidite da se pojavio okvir, provjerite je li u web pregledniku kojim se koristite uključeno proširenje za uslugu **Zaštita pregledavanja**. Ako je proširenje uključeno, postoji mogućnost da **Zaštita bankarstva** ne prepoznaje web mjesto kao stranicu za bankarstvo ili internetsku kupovinu. U tom slučaju nam pošaljite URL stranice. Analizirat ćemo je i dodati na popis podržanih stranica za bankarstvo i internetsku kupovinu.

5.3.2 Blokator daljinskog pristupa

Blokator daljinskog pristupa sprječava da postanete žrtvom telefonskih prijevara dok upotrebljavate usluge internetskog bankarstva.

Prevaranti svakodnevno zovu tisuće nasumičnih korisnika i pokušavaju ih prevariti putem društvenog inženjeringa. Prijevare s daljinskim pristupom postale su sve raširenij način izvlačenja novca od korisnika interneta.

Postoje različiti načini na koje vas ti varalice pokušavaju prevariti. Na primjer, smisle neki izgovor kako bi vas natjerali da instalirate softver alata za daljinski pristup na svoje računalo. Pretvaraju se da su iz legitimne tvrtke, kao što je Microsoft, ili na primjer iz podrške vašega lokalnog operatera te vas obavještavaju da je vaš uređaj zaražen. Putem daljinskog pristupa pokazuju obavijesti o virusnoj infekciji, a zatim vam pokušavaju prodati potpuno lažni sigurnosni softver. Također, nakon što imaju pristup vašem uređaju, mogu od vas tražiti da se prijavite u svoje Internet bankarstvo.

Dobio/la sam upozorenje o potencijalnoj prijevari dok sam obavljao/la svoje internetsko bankarstvo

Tijekom sesije internetskog bankarstva možete dobiti obavijest upozorenja da netko pokušava daljinski pristupiti vašem uređaju. Blokator pristupa na daljinu dodaje još jedan sloj zaštite vašim sesijama internetskog bankarstva. Ako detektira aktivnu vezu s daljinskim pristupom vašem uređaju dok je zaštita bankarstva aktivna, Blokator pristupa na daljinu odmah prekida vezu.

Što trebam učiniti ako iskoči upozorenje?

Nakon što se prikaže obavijest upozorenja:
▪ Nema potrebe za panikom. Sigurni ste. Zaštita bankarstva prekinula je svaki aktivni daljinski pristup vašem uređaju.
▪ Ako s nekim nepoznatim vodite telefonski razgovor, spustite slušalicu. Ne nasjedajte na telefonsku prijevaru.
Kad god primite neželjeni telefonski poziv, budite posebno oprezni. Za više informacija o telefonskim prijevarama pogledajte temu „Telefonske prijevare i što učiniti ako mislite da ste njihova meta".
▪ Ako niste sigurni u namjere pozivatelja, jednostavno zatvorite karticu bankarske sesije ili cijeli web preglednik.
▪ Uvijek možete pokrenuti potpuno skeniranje računala kako biste otkrili sve aplikacije koje je možda instalirao prevarant.

Što ako stvarno trebam nekome odobriti daljinski pristup svojem uređaju?

Nismo svi toliko tehnički potkovani i ponekad se nađemo u situaciji da nam je potrebna tehnička pomoć stručnjaka. Ako nekome privremeno želite dopustiti pristup svojem uređaju, kao što je agent tehničke podrške, provjerite jeste li vi pokrenuli zahtjev za podršku. Tek tada isključite Blokator daljinskog pristupa kako biste omogućili instalaciju alata za daljinski pristup koji je potreban agentu tehničke podrške. Kako biste saznali kako isključiti Blokator daljinskog pristupa, pogledajte temu „Uključivanje zaštite bankarstva".

5.3.3 Dodavanje Zaštite bankarstva za određene web-stranice

Osim web-mjesta koja automatski aktiviraju Zaštitu bankarstva, možete dodati određena web-mjesta na kojima želite ovaj dodatni sloj sigurnosti.

Za dodavanje Zaštite bankarstva za web stranicu:

1. Otvorite aplikaciju A1 Sigurniji internet.

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

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

Bilješka: Da biste promijenili postavke, potrebna su vam administratorska prava.

4. Odaberite karticu **Bankarstvo**.

5. Odaberi **Dodaj novo** za dodavanje novog web-mjesta na popis.

6. Unesite adresu web-mjesta koje želite dodati, a zatim odaberite **U redu**

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 *.

Sada kada posjetite dodanu web stranicu, aktivira se Zaštita bankarstva.

5.4 Sigurna online kupnja

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

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

Zaštita kupovine je prema zadanim postavkama uključena kako bi se poboljšala sigurnost vaše online kupnje. Nakon ulaska na web mjesto za kupovinu, 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 kupovinu sigurno, skočni prozor nestaje nakon nekoliko sekundi i više se neće prikazati na toj stranici tijekom sesije kupovine. 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. Ako smatrate da je stranica netočno ocijenjena, možete predložiti novu ocjenu za stranicu.

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 **Uređivanje postavki**.

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. Pomaknite se prema dolje i isključite **Blokiranje oglasa**.

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 Chrome

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

Da biste postavili proširenje preglednika za Chrome:

1. Otvorite aplikaciju A1 Sigurniji internet.

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

3. Odaberite **Postavke**.

4. Na stranici **Sigurno pregledavanje** otvorite **Proširenja preglednika**.

5. Pod opcijom **Proširenja preglednika** odaberite **Otvori Chrome Web Store**.
Otvara se stranica proširenja **Zaštita pregledavanja A1 Sigurniji internet**.

6. Odaberite **Dodaj u Chrome** > **Dodaj proširenje**.

Ako je proširenje već instalirano u pregledniku Chrome, ali je onemogućeno, odaberite vezu **Omogući ovu stavku** u natpisu na vrhu stranice.

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.

5.7.2 Instaliranje i omogućavanje proširenja preglednika za Edge

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

Da biste postavili proširenje preglednika za Edge:

1. Otvorite aplikaciju A1 Sigurniji internet.

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

3. Odaberite **Postavke**.

4. Na stranici **Sigurno pregledavanje** otvorite **Proširenja preglednika**.

5. Pod opcijom **Proširenja preglednika** odaberite **Otvori dodatke za Edge**.
Otvara se stranica proširenja **Zaštita pregledavanja A1 Sigurniji internet**.

6. Odaberite **Dohvati** > **Dodaj proširenje**.

Ako je proširenje već instalirano u pregledniku Edge, ali je onemogućeno, odaberite **Uključi** da biste ga omogućili

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.

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.

Da biste postavili proširenje preglednika za Firefox:

1. Otvorite aplikaciju A1 Sigurniji internet.

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

3. Odaberite **Postavke**.

4. Na stranici **Sigurno pregledavanje** otvorite **Proširenja preglednika**.

5. Pod opcijom **Proširenja preglednika** odaberite **Otvori dodatke za Firefox**. Otvara se stranica s dodacima **Zaštita pregledavanja A1 Sigurniji internet**.

6. Odaberite **Dodaj u Firefox** > **Dodaj**.

Kad se instalira proširenje, otvara se dijaloški okvir za pristanak korisnika. Proširenje preglednika zahtijeva vaše dopuštenje za pristup informacijama o web-adresama koje posjećujete.

7. Prvo omogućite **Dopusti zaštiti pregledavanja A1 Sigurniji internet prikupljanje mojih osobnih podataka**, a zatim odaberite **Prihvati**.

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.

8. 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.

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 Spremište 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 uzmete 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;
▪ postavite 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.

Za početak 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. Odaberi **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**
Kod za sinkronizaciju automatski se generira.
d. Unesite generirani kod za sinkronizaciju u polje **Sinkronizacijski kod** 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, Odaberi  **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

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 Prijava na internetsku uslugu sa Spremištem za lozinke

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

4. 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.

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

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

7. 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.

8. 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.

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

10. 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 Vault.

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. Od **Tip** padajući izbornik, 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 **CVV** polje, unesite 3- ili 4-znamenkasti sigurnosni kod vaše kartice koji vam pomaže u zaštiti od prijevare s kreditnom karticom.

12. Ako želite, možete urediti zadanu internetsku adresu u polju **Internetska adresa**.

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

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 a Spremište za lozinke ulazak 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. Odaberite  za uređivanje pojedinosti unosa.

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. Odaberite  za uređivanje pojedinosti unosa.

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

Za brisanje više unosa odjednom:

1. U prikazu unosa odaberite unose koje želite izbrisati: držite pritisnutu **Ctrl** 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. Odaberite  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 **Koristiti** > **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 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 .

Bilješka: Ako ne vidite ikonu 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. Odaberite  **Analiza lozinki**.
Otvara se prikaz **Analiza lozinki** 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 kod 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 **Skladište lozinki**.

5. Ovisno o tome je li drugi uređaj mobilni ili stolni uređaj, učinite nešto od sljedećeg:
▪ Na mobilnom uređaju:
a. Odaberi **Postojeći sam korisnik**.
Otvara se pogled **Povežite uređaj**.
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

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 Sef lozinki 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
- 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 instaliranu aplikaciju A1 Sigurniji internet ili verziju 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 s Windows i Mac verzijama proizvoda.

Za izvoz vašeg Spremište za lozinke podaci:

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 vaše lozinke 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 za Spremište 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 kod 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 za Spremište za lozinke.

Važno: Preporučujemo da kreirate QR kôd 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 Sefa 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.

6.10 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 Spremišta 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

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-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 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 Tehnička podrška

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

8.1 Gdje pronaći ID računa?

Kada kontaktirate našu korisničku podršku, oni mogu zatražiti ID vašeg računa.

Da biste saznali svoj ID računa:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu odaberite gornji lijevi gumb izbornika ☰.

3. Odaberite **Pomoć i podrška**.

4. ID računa pronaći ćete u odjeljku **Šifra identiteta**.

8.2 Gdje se nalaze podaci o verziji proizvoda?

Ako nam se budete obraćali, korisnička podrška možda će od vas tražiti verziju proizvoda.

Da biste pogledali aktualne podatke o verziji, učinite sljedeće:

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu odaberite gornji lijevi gumb izbornika ☰.

3. Odaberite **Pomoć i podrška**.

4. Podatke o trenutno instaliranom proizvodu pronaći ćete u odjeljku **Podaci o verziji**.

8.3 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. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu odaberite gornji lijevi gumb izbornika ☰.

3. Odaberite **Pomoć i podrška**.

4. Odaberite **Pokreni alat za podršku**.
Za pristup alatu potrebna su vam administratorska prava.

5. Odaberite **Pokreni dijagnostiku** u prozoru **Alat za podršku**.
Pokrenut će se alat za podršku i prikazati tijek prikupljanja podataka.

Kada alat završi s radom, sprema prikupljene podatke u arhivu (**fsdiag.zip**) na radnoj površini. Kada se to od vas zatraži, pošaljite datoteku korisničkoj podršci.

Savjet: Ako ne možete pristupiti alatu za podršku putem samog proizvoda, idite na web mjesto Alati za podršku i ispod **Alat za podršku (FSDIAG) za Windows** odaberite **Preuzimanje** i spremite datoteku fsdiag_standalone.exe, primjerice u mapi Preuzimanja. Dvaput kliknite datoteku da pokrenete alat.

8.4 Otklanjanje pogrešaka proizvoda

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

Našoj korisničkoj podršci možete privremeno dati posebno dopuštenje za analizu problema u proizvodu. Imajte na umu da se informacije prikupljene zapisom otklanjanja pogrešaka mogu smatrati osjetljivima.

WebView2 je tehnologija koja se koristi za ugradnju web sadržaja u izvorne aplikacije. Na primjer, naša stranica za prijavu na račun koristi tehnologiju WebView2.

Ako imate poteškoća s ugrađenim web-prikazima, program za otklanjanje pogrešaka konzole WebView2 može pomoći našoj korisničkoj podršci da umjesto vas analizira probleme s mrežnim prikazom.

Da biste našoj podršci dali privremenu dozvolu za otklanjanje pogrešaka s proizvodom:

Bilješka: Uključite **Zapisivanje otklanjanja pogrešaka** samo kada naš agent korisničke podrške to od vas zatraži.

1. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu odaberite gornji lijevi gumb izbornika ☰.

3. Odaberite **Pomoć i podrška**.

4. Odaberite **Uređivanje postavki**.

5. Pod **Alati**, odaberite prekidač za uključivanje **Zapisivanja otklanjanja pogrešaka**.
Nakon što je omogućeno bilježenje otklanjanja pogrešaka, opcija **Program za pronalaženje pogrešaka konzole WebView2** postaje vidljiva.

6. Ako želite uključiti **program za ispravljanje pogrešaka konzole WebView2**, odaberite preklopni gumb.
Nakon što uđete u ugrađeni web prikaz, otvara se prozor konzole.

7. Čim naša korisnička podrška završi s analizom problema, isključite **Zapisivanje otklanjanja pogrešaka** odabirom prekidača.

8.5 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. Otvorite aplikaciju A1 Sigurniji internet.

2. Na glavnom prikazu odaberite gornji lijevi gumb izbornika ☰.

3. Odaberite **Pomoć i podrška**.

4. Odaberite **Uređivanje postavki**.

5. Pod **Alati**, izaberite **Ponovno postavi predmemoriju reputacije**.

8.6 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.