FILTRIRANJE SPLETA

**Ime in Priimek: Blaž Šifrer**

**Postopek filtriranja pošte:** Slika, ki vsebuje besede besedilo, posnetek zaslona

Opis je samodejno ustvarjen

Kliknemo na ustvari nov filter

Slika, ki vsebuje besede besedilo, posnetek zaslona

Opis je samodejno ustvarjen

Izpolnemo podatke in kliknemo iskanje

Slika, ki vsebuje besede besedilo, posnetek zaslona, spletno mesto, spletna stran

Opis je samodejno ustvarjen

**Program za filtriranje:**

Slika, ki vsebuje besede besedilo, posnetek zaslona, programska oprema, spletna stran

Opis je samodejno ustvarjen

Kliknemo na settings

Slika, ki vsebuje besede besedilo, posnetek zaslona, programska oprema, računalniška ikona

Opis je samodejno ustvarjen

Pritisnemo ikono spam tools, nato Filters ter dodaj filter. Izberemo katere maile želimo filtrirati.

Slika, ki vsebuje besede besedilo, programska oprema, računalniška ikona, spletna stran

Opis je samodejno ustvarjen

Izberemo barvo, ime in pisavo

Tukaj lahko izberemo različne filtre in jih dodamo.

**Filtriranje pri brskalnikih**

**Google Chrome**

a. Nastavitve se nahajajo v zgornjem desnem kotu brskalnika. Kliknite na ikono s tremi pikami, da se odpre padajoči meni, in izberite možnost "Nastavitve". Nato se pomaknite na dno strani in kliknite na "Napredne nastavitve". Pod sekcijo "Zasebnost in varnost" izberite možnost "Nastavitve vsebine".

b. V nastavitvah vsebine lahko prilagajate filtriranje spletnih strani na naslednje načine: Blokiraj piškotke

Omeji dostop do lokacije

Blokiraj slike

Prepreči predvajanje zvoka

Blokiraj vse piškotke

Omeji dostop do mikrofona

Omeji dostop do kamere

Blokiraj vse vtičnike

Omogoči ali onemogoči samodejno predvajanje

Blokiraj oglase na spletnih straneh

c. Za preizkus delovanja filtra za blokiranje piškotkov lahko v nastavitvah vsebine omogočite ta filter. Nato obiščite spletno stran, ki uporablja piškotke (na primer spletno trgovino). Če je filter uspešen, piškotki ne bodo več uporabljeni na tej spletni strani.

**Mozilla Firefox**

a. Nastavitve se nahajajo v zgornjem desnem kotu okna brskalnika. Kliknite na ikono z tremi črticami, da se odpre padajoči meni, in izberite možnost "Nastavitve". Nato se pomaknite na "Zasebnost in varnost" ter izberite "Nastavitve".

b. V nastavitvah lahko filtrirate spletne strani na naslednje načine:

Blokiraj piškotke

Blokiraj spletne sledilce

Omeji dostop do lokacije

Omeji dostop do mikrofona

Omeji dostop do kamere

Blokiraj samodejno predvajanje avdio in video vsebine

Omogoči zaščito pred sledenjem

Blokiraj oglase na spletnih straneh

c. Za testiranje filtra blokiranja spletnih sledilcev lahko omogočite ta filter v nastavitvah. Nato obiščite spletno stran, ki uporablja sledilce (na primer spletno trgovino). Če je filter uspešen, sledilci ne bodo več uporabljeni na tej spletni strani.

**Apple Safari**

a. Nastavitve filtriranja v Apple Safariju se nahajajo v zavihku "Safari" in nato "Nastavitve" (Preferences). Nato izberite "Spletni viri" (Websites) in ustrezno možnost.

b. V Apple Safariju lahko filtrirate vsebine, kot so spletne strani z neprimerno vsebino, nezaželeni oglasni bloki, nevarne spletne strani in druge vsebine, ki jih ne želite videti. Na primer, lahko izberete, da blokirate neprimerne spletne strani ali uporabljate "Omejitve" (Restrictions), ki filtrirajo spletne vsebine glede na starostno primernost.

c. Za testiranje lahko vklopite omejitve za vsebine za odrasle in poskusite obiskati spletne strani z neprimerno vsebino. Na primer, če poskusite obiskati spletno stran za odrasle, bo Safari blokiral dostop do te spletne strani in prikazal opozorilo.

**Microsoft Edge**

a. Nastavitve filtriranja v Microsoft Edgeu se nahajajo v zavihku "Nastavitve in več" (Settings and more) in nato "Nastavitve" (Settings). Nato izberite "Zasebnost, varnost in storitve" (Privacy, search, and services) ter ustrezno možnost.

b. V Microsoft Edgeu lahko filtrirate vsebine, kot so spletne strani z neprimerno vsebino, nezaželeni oglasni bloki, nevarne spletne strani in druge vsebine, ki jih ne želite videti. Na primer, lahko izberete, da blokirate neprimerne spletne strani ali uporabljate SmartScreen filtre, ki filtrirajo spletne strani in preprečujejo nevarne prenose.

c. Za testiranje lahko vklopite SmartScreen filtre in poskusite prenesti nevarno datoteko. Microsoft Edge bo preprečil prenos in prikazal opozorilo.

Podaljški oz. extensioni:

**Adblock:**

Opis: NoScript je razvil italijanski razvijalec Giorgio Maone in je na voljo kot dodatek za brskalnik Firefox. Ta podaljšek zagotavlja zaščito pred izvajanjem nezaželenih skript na spletnih straneh.

Uporabnikom omogoča nadzor nad izvajanjem skript in preprečuje morebitne varnostne ranljivosti. Filtriranje:

NoScript privzeto blokira izvajanje vseh skript na spletni strani in uporabniku omogoča ročno odločanje, katere skripte želi dovoliti. S tem preprečuje izvajanje morebitno škodljivih skript ter zagotavlja večjo varnost brskanja. Testiranje:

NoScript je deloval pravilno in blokiral izvajanje vseh skript na strani. Uporabniku sem omogočil izvajanje določenih skript, ki so bili potrebni za normalno delovanje strani. Podaljšek je zagotovil dodatno varnost in nadzor nad izvajanjem skript.

**Privacy Badger (za Mozilla Firefox)**

Opis: uBlock Origin je podaljšek, ki je na voljo v Microsoftovem trgovinskem središču. Razvil ga je Raymond Hill.

Ta podaljšek omogoča blokiranje oglasov in izboljšanje hitrosti brskanja. Uporabnikom nudi boljši nadzor nad prikazom vsebine na spletnih straneh. Filtriranje:

uBlock Origin blokira oglase, sledilce, škodljive skripte, elemente družbenih omrežij, vtičnike in druge moteče vsebine. Uporabnikom omogoča tudi prilagajanje filtriranja po meri, kar pomeni, da lahko sami določijo, katere vsebine želijo blokirati. Testiranje:

Podaljšek uBlock Origin je deloval pravilno in uspešno blokiral oglase ter druge moteče elemente. Poleg tega je izboljšal hitrost brskanja in omogočil boljšo uporabniško izkušnjo pri brskanju po spletnih straneh.

**uBlock Origin (za Microsoft Edge)**

Opis: Privacy Badger je podaljšek, ki je na voljo v dodatkih za brskalnik Firefox. Razvil ga je Electronic Frontier Foundation (EFF).

Ta podaljšek je namenjen varovanju zasebnosti uporabnikov in preprečevanju sledenja na spletu. Privacy Badger samodejno odkriva in blokira nezaželene sledilce na obiskanih spletnih straneh. Filtriranje: Privacy Badger analizira sledilce na spletni strani in blokira tiste, ki sledijo uporabniku brez njegovega dovoljenja. Filtrira sledilne piškotke, skripte za sledenje, slikovne pike in druge sledilne elemente. Testiranje:

Privacy Badger je uspešno zaznal in blokiral sledilce ter sledilne elemente na spletni strani. Podaljšek je deloval učinkovito, kar je preprečilo nezaželeno sledenje uporabnika.

**NoScript (za Mozilla Firefox)**

Opis: Adblock Plus je podaljšek, ki je na voljo v Chrome Web trgovini. Ustvaril ga je nemški razvijalec Wladimir Palant. Gre za enega najbolj priljubljenih podaljškov za blokiranje oglasov na spletu.

Adblock Plus omogoča filtriranje in blokiranje neželenih oglasov na spletnih straneh, kar uporabnikom omogoča bolj čisto in neprekinjeno brskanje. Filtriranje:

Adblock Plus blokira oglasne pasice, sponzorirane povezave, slikovne oglase, avtomatsko predvajanje videov, sledilce in druge moteče elemente na spletnih straneh. S tem omogoča uporabnikom, da se osredotočijo na vsebino, ki jo želijo videti, in zmanjša moteče elemente na spletnih straneh. Testiranje:

Adblock Plus je deloval brezhibno in uspešno blokiral vse oglase, ki so se pojavili na spletni strani. Uporabnikom je zagotovil boljšo brskalno izkušnjo z manj motečimi elementi na spletnih straneh.

**Programi, ki delujejo kot požarni zidovi:**

**PROGRAM 1:** Norton Firewall

Norton Firewall je del varnostnega paketa Norton, ki ponuja celovito zaščito pred grožnjami in vključuje tudi požarni zid. Norton Firewall zagotavlja zaščito omrežja pred napadi in zlonamerno programsko opremo ter omogoča uporabnikom nadzor nad omrežnimi povezavami.

Možnosti:

Filtriranje omrežnega prometa in nadzor nad povezavami

Prilagajanje pravil za dovoljene in blokirane povezave

Zaznavanje in blokiranje zunanjih napadov

Avtomatsko prilagajanje varnostnih pravil glede na mrežno okolje

Opozorila in poročila o omrežnih aktivnostih

Integracija z drugimi Norton varnostnimi funkcijami (na primer protivirusna zaščita)

**Slika, ki vsebuje besede besedilo, posnetek zaslona, večpredstavnostna programska oprema, programska oprema

Opis je samodejno ustvarjen**

**Prva stran**

**Prva stran**

**PROGRAM 2:** ZoneAlarm Firewall

ZoneAlarm Firewall je programski požarni zid, ki zagotavlja zaščito pred zunanjimi napadi in nepooblaščenim dostopom do računalnika. Ponuja napredne funkcije in orodja za nadzor omrežnega prometa ter varnostno zaščito.

Možnosti:

Nadzor nad omrežnimi povezavami in filtriranje prometa

Prilagajanje pravil za omrežne povezave, aplikacije in protokole

Zaznavanje in preprečevanje napadov ter zlonamerne programske opreme

Varovanje brezžičnih omrežij

Funkcija SmartDefense za samodejno zaznavanje groženj in napadov

Opozorila in poročila o omrežnih aktivnostih

Slika, ki vsebuje besede besedilo, posnetek zaslona, programska oprema, spletna stran

Opis je samodejno ustvarjen

Primerjava:

ZoneAlarm Firewall je samostojen programski požarni zid z naprednimi funkcijami za nadzor omrežja. Norton Firewall je del celovitega varnostnega paketa Norton s preprosto uporabo in dodatnimi funkcijami. Oba zagotavljata učinkovito varnostno zaščito, vendar se razlikujeta v funkcionalnostih in pristopu. Izbor je odvisen od uporabnikovih potreb.

**Enkripcija gesel:**

**PROGRAM 1:** LastPass

LastPass je program za varno upravljanje gesel z možnostjo shranjevanja in enkripcije gesel ter uporabniških računov. Na voljo je spletna različica preko brskalnika in program, ki se namesti na računalnik.

Glavni nadzorni panel: Po prijavi v LastPass se odpre glavni nadzorni panel, kjer so na voljo različne funkcije. Na tej strani lahko uporabniki pregledajo shranjena gesla, ustvarijo nove račune, generirajo varna gesla, organizirajo shranjene podatke in še več.

Enkripcija gesel: LastPass avtomatično izvede enkripcijo gesel, ko se nova gesla shranjujejo ali obstoječa posodabljajo. Uporabnikovo geslo se zakodira z močnim algoritmom enkripcije, ko ga vpiše v LastPass. Zakodirano geslo se nato shrani na strežnikih LastPass, kjer je dostopno samo uporabniku.

**Slika, ki vsebuje besede besedilo, posnetek zaslona, programska oprema, računalniška ikona

Opis je samodejno ustvarjen**