Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

KAKO SIGURNO KORISTITI INTERNET

VODIČ ZA STARIJE OSOBE

cyber.gov.au

Uvod

Odlaskom na internet možete ostati u kontaktu s prijateljima i obitelji, učiti o temama, pa čak i igrati igrice.

Baš kao i vezivanje pojasa prije vožnje, i prije korištenja interneta trebate poduzeti korake kako biste bili sigurniji.

Australski Centar za kibernetičku sigurnost (Australian Cyber Security Centre – ACSC) želi osigurati da svi budu sigurni dok su na mreži. Ovaj dokument pokriva neke osnovne prakse cyber sigurnosti koje možete koristiti da se zaštitite prilikom pristupa internetu.

Australski Centar za kibernetičku sigurnost, kao dio Australske uprave za signale (Australian Signals Directorate – ASD), pruža savjete, pomoć i operativne odgovore radi sprječavanja, otkrivanja i uklanjanja kibernetičkih prijetnji Australiji. ACSC je tu da pomogne Australiji postati sigurnije mjesto za povezivanje na mreži.

Za više informacija o cyber sigurnosti, vodiče i savjete, posjetite cyber.gov.au

Cyber sigurnost za starije osobe

Savjet 1: Ažurirajte svoje uređaje

Ažuriranje softvera je poput servisiranja automobila. Poboljšava performanse Vašeg uređaja i čini ga sigurnijim.

Kibernetički kriminalci uvijek pronalaze nove načine za hakiranje uređaja. Postavljanje uređaja za automatsko instaliranje ažuriranja može popraviti sve slabosti u Vašem softveru i zadržati hakere podalje.

Da biste pronašli više informacija, potražite 'Updates' na cyber.gov.au.

JESTE LI ZNALI:

Ažuriranja također mogu dodati nove značajke vašem uređaju i učiniti ga bržim.

Savjet 2: Uključite višefaktorsku autentifikaciju

Višefaktorska autentifikacija na Vašem računu je isto što i sigurnosna zaštita Vašeg doma.

Štiti Vas od kriminalaca koji pokušavaju provaliti.

S aktiviranom višefaktorskom provjerom autentičnosti morate dati više podataka da biste dobili pristup svom računu. Na primjer, možda ćete morati unijeti zaporku i kôd tekstualne poruke da biste se prijavili na svoj profil na društvenim mrežama.

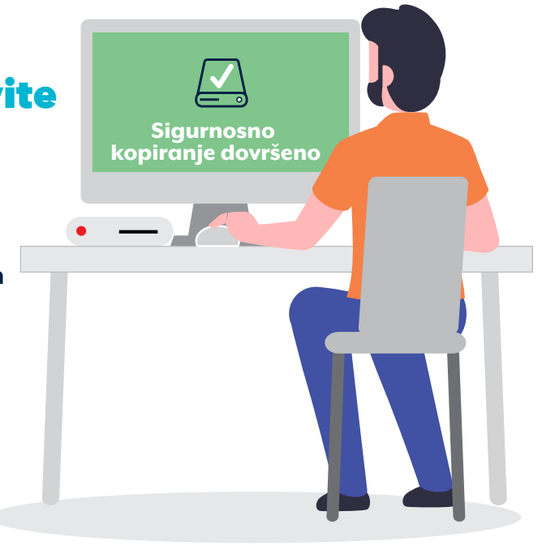
Višestruki slojevi otežavaju hakiranje kibernetičkih kriminalaca. Možda će uspjeti riješiti jedan dio, poput vaše lozinke, ali će i dalje morati pribaviti druge dijelove slagalice za pristup vašem računu.

Da biste pronašli više informacija, potražite 'Multi-factor authentication' ili 'MFA' na cyber.gov.au

ZAPAMTITE:

Ako vam je potrebna pomoć pri uključivanju višefaktorske autentifikacije, zatražite pomoć od prijatelja ili člana obitelji

Savjet 3: Napravite sigurnosnu kopiju uređaja



Izrada "sigurnosne kopije" je kada napravite kopiju svojih važnih datoteka i stavite ih na sigurno mjesto. To je poput fotokopiranja dragocjenih fotografija koje treba čuvati u sefu u slučaju da izgubite originale.

Prilikom izrade sigurnosne kopije računala, telefona ili tableta, kopije datoteka spremaju se na mreži ili na zaseban uređaj. Sigurnosna kopija važnih datoteka i dragocjenih fotografija pružit će Vam duševni mir.

Ako nešto pođe po zlu s Vašim uređajem ili Vas cyber kriminalci hakiraju, datoteke možete jednostavno vratiti iz sigurnosnih kopija.

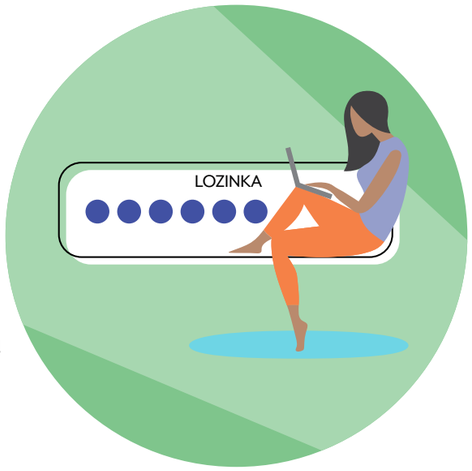
Za više informacija potražite 'Backups' na cyber.gov.au

JESTE LI ZNALI:

Redovito sigurnosno kopiranje uređaja znači da ćete uvijek imati pristup najnovijim datotekama.

Savjet 4: Upotrijebite zaporku-frazu

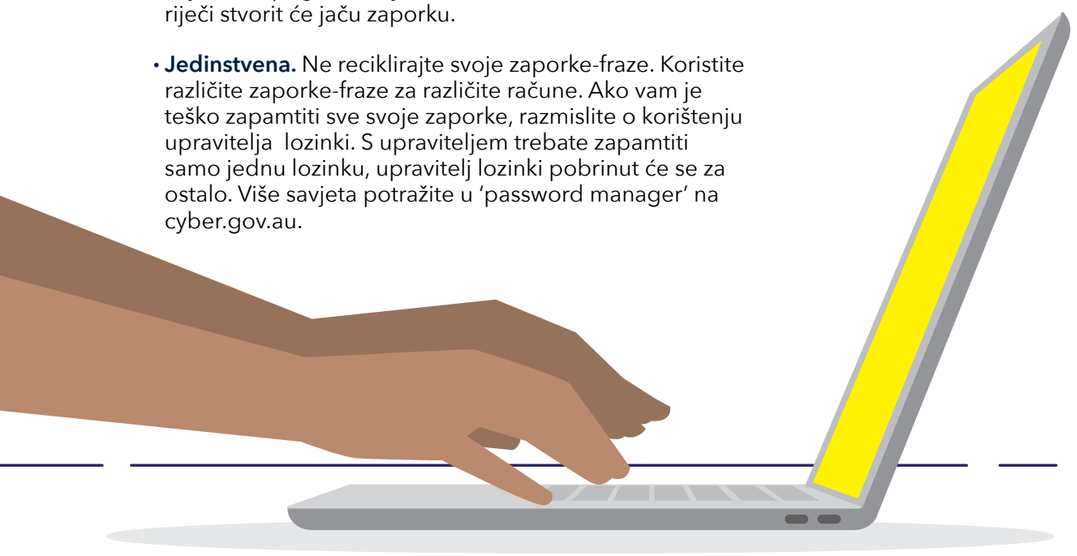
Ako lozinka na Vaš račun stavi lokot, zaporka-fraza mu daje vlastiti sigurnosni sustav! One su jače i sigurnije verzije lozinki.



Kad ne možete uključiti MFA, upotrijebite zaporku-frazu za zaštitu svog računa. Zaporke-fraze koriste četiri ili više slučajnih riječi kao Vašu lozinku. Zbog toga kibernetički kriminalci teško mogu pogoditi, ali Vama ih je lako zapamtiti.

Kad kreirate zaporku-frazu, neka bude:

- **Dugačka.** Što dulja, to bolje. Neka bude sa najmanje 14 znakova. Četiri ili više slučajnih riječi koje ćete zapamtiti je izvrsno. Na primjer, 'čamac od krumpira ljubičaste patke'.
- **Nepredvidljiva.** Što je vaša zaporka-fraza manje predvidljiva, to bolje. Rečenice mogu biti sjajne fraze, ali ih je lakše pogoditi. Mješavina četiri ili više nasumičnih riječi stvorit će jaču zaporku.
- **Jedinstvena.** Ne reciklirajte svoje zaporke-fraze. Koristite različite zaporke-fraze za različite račune. Ako vam je teško zapamtiti sve svoje zaporke, razmislite o korištenju upravitelja lozinki. S upraviteljem trebate zapamtiti samo jednu lozinku, upravitelj lozinki pobrinut će se za ostalo. Više savjeta potražite u 'password manager' na cyber.gov.au.



Saznajte više o stvaranju sigurnih zaporki pretraživanjem 'Passphrases' on cyber.gov.au

JESTE LI ZNALI:

Cyber kriminalci su lukavi i mogli bi koristiti poznato ime i adresu e -pošte. Budite oprezni ako:

- **od Vas se traži da hitno platite račun**
- **od Vas se traži da promijenite svoje podatke ili lozinku**
- **od Vas se traži da kliknete na poveznicu ili otvorite privitak.**

Savjet 5: Prepoznajte i prijavite prevare

Što brže prijavite prevaru, brže možemo djelovati.

Ako vjerujete da netko pokušava upotrijebiti internet da Vas prevari, bolje je biti proaktivan i oprezan nego riskirati da Vas netko iskoristi.

Ako zvuči previše dobro da bi bilo istinito, vjerojatno jest. Iako poruka može reći da ste osvojili nagradu ili da Vaše računalo sadrži virus, ta poruka nije svojstvena samo Vama.

Možda dolazi od prevaranata i oni Vas žele iskoristiti.

Imajte na umu da će se prevaranti često pretvarati da predstavljaju osobu ili organizaciju kojoj vjerujete. Budite sumnjičavi ako primite poruku koja izgleda kao da je od nekoga kome vjerujete, ali koristi novi telefonski broj, adresu e-pošte ili profil na društvenoj mreži. Prije nego što odgovorite, provjerite je li osoba ili organizacija koja vam šalje poruku stvarno ono za što se predstavlja tako da ih kontaktirate putem pouzdanih kanala. Na primjer, ako primite tekstualnu poruku koja izgleda kao da je od vašeg djeteta, ali dolazi s novog broja, nemojte odgovarati. Pošaljite im poruku na društvenim mrežama kako biste prvo provjerili jesu li stvarno promijenili broj telefona.

Zaključak

Sada kada ste naoružani znanjem za sigurnije korištenje interneta, možete s povjerenjem pregledavati i nastaviti uživati u vremenu na mreži.

Zapamtite, kibernetički kriminalci uvijek smišljaju nove načine da prevare ljude.

Nikad ne škodi povremeno doraditi svoje znanje o kibernetičkoj sigurnosti i naučiti nove načine da ostanete sigurni.

Bonus savjeti

Želite li saznati više načina da ostanete sigurni na mreži? Pogledajte sljedeće savjete.

Razmislite o tome što objavljujete.

Dobro razmislite o informacijama koje dijelite na internetu i tko će ih vidjeti. Prihvaćajte samo zahtjeve za prijateljstvo od ljudi koje poznajete u stvarnom životu.

Primajte upozorenja o novim prijetnjama.

Prijavite se za našu besplatnu uslugu upozorenja. To će Vas obavijestiti kad god pronađemo novu cyber prijetnju.

To će Vam također dati savjet što učiniti ako se napad dogodi.

Razgovarajte o cyber sigurnosti s obitelji i prijateljima.

Sada kada ste stekli vještinu u cyber sigurnosti, podijelite ono što ste naučili sa svojom obitelji i prijateljima. Vaše znanje moglo bi im pomoći da izađu iz nezgodne situacije!

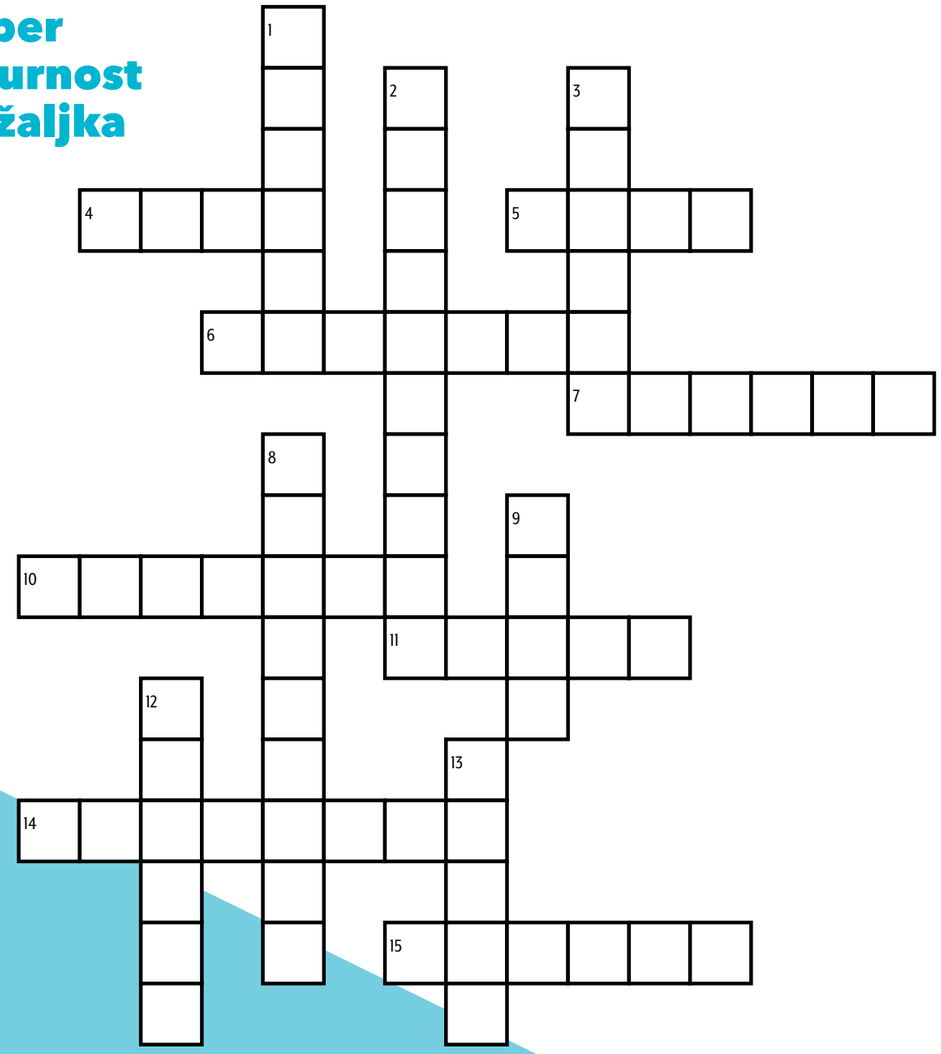
Izbjegavajte javni Wi-Fi kada bankarite ili kupujete na mreži.

Javni Wi-Fi odličan je za gledanje videozapisa ili čitanje web stranica, ali zadržavajte sve mrežne aktivnosti koje uključuju novac za kućnu internetsku vezu. Javni Wi-Fi može biti rizičan.

Prijavite cyber zločine i incidente kako biste zaštitili Australiju.

Ako mislite da ste bili žrtva kibernetičkog kriminala, djelujte brzo. Više savjeta nalazi se na cyber.gov.au

Cyber sigurnost križaljka



OKOMITO

1. Connected to the internet
2. A strong password
3. A person who uses computers to steal data
8. Software that destroys viruses
9. A deceptive scheme or trick
12. A copy of your computer's files
13. Relating to, or involving computers

VODORAVNO

4. Wireless networking technology
5. Australia's lead agency for cyber security
6. A document on the World Wide Web
7. To give information about something
10. New, improved or more secure versions of software
11. Electronic mail
14. The state of being free from danger or threat
15. A tool that can connect to the internet

Dopunski vodiči

Dodatne informacije potražite u našoj seriji *Osobna kibernetička sigurnost (Personal Cyber Security)*: tri vodiča osmišljena da pomognu običnim Australcima da razumiju osnove cyber sigurnosti i kako možete poduzeti mjere kako biste se zaštitili od uobičajenih cyber prijetnji.

Sva tri vodiča možete naći na **cyber.gov.au**

Odgovori u križaljki

1. online, 2. passphrase, 3. hacker, 4. Wi-Fi, 5. ACSC, 6. webpage, 7. report, 8. antivirus, 9. scam, 10. updates, 11. email, 12. backup, 13. cyber, 14. security, 15. device

Bilješke

Za više informacija ili prijavu incidenta cyber sigurnosti kontaktirajte nas

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Ovaj broj dostupan je za korištenje samo unutar Australije.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre