Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

OSOBNA KIBERNETIČKA SIGURNOST

PRVI KORACI

cyber.gov.au

Serija o osobnoj kibernetičkoj sigurnosti

Serija o osobnoj kibernetičkoj sigurnosti

Osobna kibernetička sigurnost: Prvi koraci vodič je koji je prvi u nizu od tri vodiča osmišljenih kako bi pomogli svakodnevnim Australcima razumjeti osnove načine kibernetičke sigurnosti. Saznajte kako možete poduzeti mjere da se zaštitite od uobičajenih kibernetičkih prijetnji.

Prvi koraci

Sljedeći koraci

Napredni koraci

Sadržaj

Uvod

Što je osobna kibernetička sigurnost?

U svijetu koji sve više pokreće tehnologija svakodnevno koristimo uređaje i račune koji su ranjivi na kibernetičke prijetnje:

- Vaši uređaji mogu uključivati: računala, mobilne telefone, tablete i druge uređaje povezane s internetom.
- Možda koristite i mrežne račune za e-poštu (email), bankarstvo, kupovinu, društvene medije, igrice i još mnogo toga.

Osobna kibernetička sigurnost sastoji se od kontinuiranih koraka koje možete poduzeti kako biste zaštitili svoje račune i uređaje od kibernetičkih prijetnji.

Kako me ovaj vodič može zaštititi od kibernetičkih prijetnji?

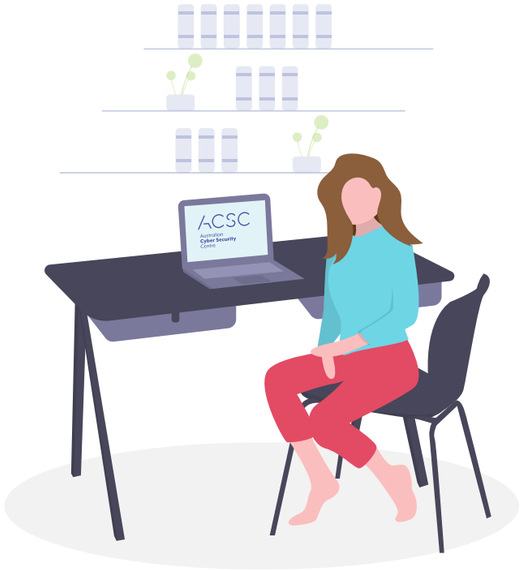
Ako ste tek saznali o kibernetičkoj sigurnosti ili želite biti u tijeku, ovaj vodič je izvrsno mjesto za početak. „Osobna kibernetička sigurnost: Prvi koraci“ prvi je u nizu od tri vodiča koji su osmišljeni da vam pomognu razumjeti osnove kibernetičke sigurnosti.

Što su kibernetičke prijetnje?

Glavne kibernetičke prijetnje koje pogađaju sve Australce su **prevarantski i malware softver**.

- **Malware softver je opći izraz koji se koristi za opisivanje zlonamjernog softvera** koji je osmišljen da nanese štetu. To može uključivati viruse, crve, spyware, trojance i ransomware. Kibernetički kriminalci koriste malware softver kako bi ukrali vaše podatke i novac te kontrolirali vaše uređaje i račune.
- **Prevarantski softver su poruke koje šalju kibernetički kriminalci** s namjerom da vas manipuliraju da odate osjetljive informacije ili da aktivirate malware softver na vašem uređaju.

Ovi napadi mogu imati značajan osobni i financijski učinak na žrtve, te im raste sofisticiranost i učestalost.



Uključite automatsko ažuriranje (updates)

Što je ažuriranje?

Ažuriranje je poboljšana verzija softvera (programa, aplikacija i operativnih sustava) koji ste instalirali na svoje računalo i mobilne uređaje.

- **Softverska ažuriranja pomažu u zaštiti vaših uređaja** ispravljanjem programskih grešaka (pogrešaka ili ranjivosti kodiranja) . Kibernetički kriminalci i malware mogu koristiti te greške za pristup vašem uređaju i krađu vaših osobnih podataka, računa, financijskih podataka i identiteta.
- Kibernetički kriminalci **neprestano pronalaze** i iskorištavaju **nove programske greške**. Ažuriranje softvera na vašim uređajima pomaže vašoj zaštititi od kibernetičkih napada.

Kako mogu postaviti automatsko ažuriranje?

Automatsko ažuriranje je zadana ili “postavi i zaboravi” postavka koja instalira nova ažuriranja čim su dostupna.

- Uključite i potvrdite automatsko ažuriranje na svim softverima i uređajima.
- Načini uključivanja automatskog ažuriranja mogu se razlikovati ovisno o softveru i uređaju.
- Ako je moguće, odredite prikladno vrijeme za automatsko ažuriranje, primjerice kada spavate ili obično ne koristite svoj uređaj.

Vaš uređaj mora biti uključen, priključen na napajanje i imati dovoljno neiskorištenog prostora za pohranu.

Savjet: ako dobijete upit za ažuriranje softvera na vašem uređaju, učinite to što prije.

Detaljnije informacije o načinu uključivanja automatskog ažuriranja možete pronaći pod ‘Updates’ na cyber.gov.au

Što ako postavka automatskog ažuriranja nije dostupna?

Ako postavka automatskog ažuriranja nije dostupna, trebali biste redovito provjeravati i instalirati nova ažuriranja putem vašeg softvera ili izbornika postavki uređaja.

Što ako postavka automatskog ažuriranja nije dostupna?

Ako su vaš uređaj, operativni sustav ili softver prestari,moguće je da ih proizvođač ili razvojni programer više ne podržava.

Kad dođu do faze "kraja podrške", proizvodi više neće primati ažuriranja. To vas može učiniti ranjivima na cyber-napade. Primjeri proizvoda za koje je podrška završena uključuju Operativni sustav Windows 7 i iPhone 7.

Ako je vaš uređaj, operativni sustav ili softver došao do kraja podrške, ACSC preporučuje nadogradnju što prije kako biste ostali zaštićeni.

Za više informacija potražite "Kraj podrške" (End of support) na cyber.gov.au

Aktivirajte autentifikaciju s više faktora (MFA)

Što je MFA?

Možete koristiti provjeru autentičnosti s više faktora (MFA) kako biste poboljšali sigurnost svojih najvažnijih računa. MFA zahtijeva da proizvedete kombinaciju dva ili više vrsta provjere autentičnosti prije odobravanja pristupa računu.

- **Nešto što znate** (npr. PIN, lozinka ili šifra)
- **Nešto što imate** (npr. pametna kartica, fizički znak (token), aplikacija za provjeru autentičnosti, SMS ili e-pošta)
- **Nešto što ste Vi** (npr. otisak prsta, prepoznavanje lica ili skeniranje šarenice oka)

MFA otežava kibernetičkim kriminalcima početni pristup vašem računu. Dodaje više slojeva provjere autentičnosti, zahtijevajući dodatno vrijeme, trud i resurse za probijanje.

Kako mogu aktivirati MFA da zaštitim svoje najvažnije račune?

Ovisno o računu, uređaju ili softver aplikaciji koraci za aktiviranje MFA su različiti Trebate odmah aktivirati MFA, počevši od važnih računa, kao što su:

- Svi internetski bankovni i financijski računi (npr. vaša banka, PayPal)
- Svi računi e-pošte (npr. Gmail, Outlook, Hotmail, Yahoo!)

Ako imate puno računa e-pošte, dajte prednost onima koji su povezani s vašim internetskim bankarstvom ili drugim važnim uslugama.

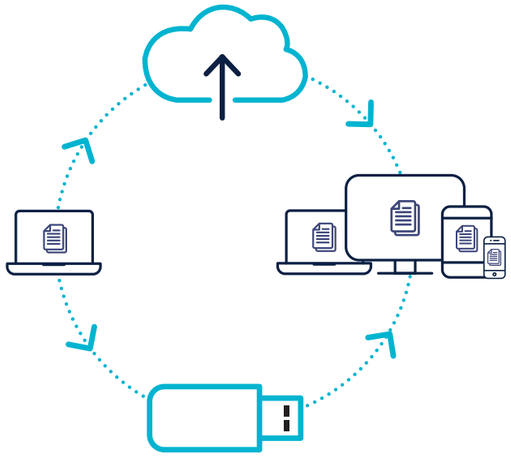
Više o tome kako aktivirati provjeru autentičnosti s više faktora možete pročitati na cyber.gov.au pretraživanjem 'Multi-factor authentication" or MFA.

Redovito provodite sigurnosno kopiranje svojih uređaja (backup)

Što je sigurnosna kopija?

Sigurnosna kopija je digitalna kopija vaših podataka. To može uključivati fotografije, financijske informacije ili zapise koje ste spremili na vanjski uređaj za pohranu ili u oblak.

Sigurnosno kopiranje podataka je mjera predostrožnosti kako bi se oni mogli vratiti ako se ikada izgube, ukradu ili oštete.



Kako mogu sigurnosno kopirati svoje uređaje i datoteke?

Trebali biste redovito sigurnosno kopirati svoje datoteke i uređaje. Kako će to biti, bilo da je svakodnevno, tjedno ili mjesečno, ovisit će o vama.

Koliko puta ćete sigurnosno kopirati može ovisiti o broju:

- novih datoteka koje učitate na svoj uređaj,
- promjena koje napravite u datotekama.

Savjet: redovito provjeravajte sigurnosne kopije kako biste bili upoznati s postupkom oporavka. Uvijek provjerite rade li sigurnosne kopije ispravno.

Detaljnije informacije o tome kako sigurnosno kopirati svoje podatke možete pronaći na 'Backups' on cyber.gov.au

Osobna kibernetička sigurnost: Prvi koraci

Koristite zaporke (passphrases) kako biste zaštitili svoje važne račune

Višefaktorska autentifikacija (MFA) jedan je od najučinkovitijih načina da zaštitite svoje račune od kibernetičkih kriminalaca. **Ako MFA nije dostupan**, jedinstvena jaka šifra može bolje zaštititi vaš račun u usporedbi s jednostavnom lozinkom.

Što je zaporka?

Zaporka koristi četiri ili više nasumičnih riječi kao svoju lozinku.

Na primjer: 'glineni perec od kristalnog luka'.

- **Zaporke su sigurnije** od jednostavnih lozinki (passwords).
- Kibernetičkim **kriminalcima** zaporke su teže za probijanje, **a** vama ih je **lakše zapamtiti**.

Kako mogu kreirati zaporku?

Napravite zaporke koje su:

- **Dugačke:** najmanje 14 znakova, koristeći četiri ili više nasumičnih riječi. Što je šifra duža, to je sigurnija.
- **Nepredvidive:** upotrijebite nasumičnu kombinaciju četiri ili više nepovezanih riječi. Nema poznatih fraza, citata ili stihova.
- **Jedinstvene:** ne koristi se ponovno na više računa.

Ako web stranica ili usluga zahtijeva složenu lozinku koja uključuje simbole, velika slova ili brojeve, možete ih uključiti u svoju zaporku. Vaša zaporka i bi dalje trebala biti dugačka, nepredvidiva i jedinstvena radi najbolje sigurnosti.

Koje račune trebam osigurati zaporkom?

Ako vaši najvažniji računi nisu zaštićeni s MFA, promijenite svoje lozinke u jedinstvene jake zaporke, počevši s:

- Online bankarstvom i financijskim računima
- Računima e-pošte

Ako imate puno računa e-pošte, dajte prednost onima koji su povezani s vašim internetskim bankarstvom ili drugim važnim uslugama.

Obično možete promijeniti svoju lozinku u jedinstvenu jaku šifru putem izbornika postavki računa.

Savjet: Ako vam je teško zapamtiti sve svoje zaporke, razmislite o korištenju upravitelja lozinki. Uz pomoć upravitelja lozinki, trebate zapamtiti samo jednu lozinku, upravitelj lozinki će se pobrinuti za ostalo. Za više savjeta potražite „password manager" na cyber.gov.au.

Detaljnije informacije o načinu stvaranja sigurnih zaporki možete pronaći pretražujući 'Passphrases' na cyber.gov.au

Zaštitite svoj mobilni uređaj

Danas se pametni telefoni i tableti koriste u svakodnevnom životu. Koristimo ih za povezivanje, kupnju, rad, bankarstvo, praćenje svoje kondicije i obavljanje stotina zadataka u bilo koje vrijeme i s bilo kojeg mjesta.

Što se može dogoditi ako je moj mobilni uređaj kompromitiran, izgubljen ili ukraden?

- Internetski kriminalci mogu ga koristiti za krađu vašeg novca ili identiteta. Oni to čine pomoću informacija pohranjenih na vašem uređaju, uključujući i društvene mreže i račune e-pošte.
- Možete izgubiti nezamjenjive podatke poput fotografija, bilješki ili poruka (ako nemate sigurnosnu kopiju).
- Internetski kriminalac može koristiti vaš telefonski broj za prijevaru drugih ljudi.

Kako mogu zaštititi svoj mobilni uređaj?

Sigurnost uređaja:

- **Zaključajte** svoj uređaj zaporkom, lozinkom, PIN-om ili šifrom. Neka bude teško pogoditi - datum rođenja i zaključavanje uzorkom je lako pogoditi. Koristite zaporku za optimalnu sigurnost (pogledajte stranicu 6). Također razmislite o upotrebi prepoznavanja lica ili otiska prsta za otključavanje uređaja.
- **Provjerite** je li vaš uređaj postavljen na automatsko zaključavanje nakon kratkog vremena neaktivnosti.
- **Ne** punite svoj uređaj na javnim stanicama za punjenje i izbjegavajte punjače trećih osoba.
- **Postavite se** prema svom telefonu kao prema svom novčaniku. Čuvajte ga na sigurnom i uz sebe u svakom trenutku.

Sigurnost softvera i aplikacija:

- **Koristite** značajku automatskog ažuriranja (updates) svog uređaja za instaliranje novih ažuriranja aplikacija i operativnog sustava čim budu dostupna.
- **Postavite** uređaj da zahtijeva zaporku/lozinku prije instaliranja aplikacija. Za to se također može koristiti roditeljski nadzor.
- **Pažljivo** provjerite dopuštenja privatnosti kada instalirate nove aplikacije na svoj uređaj, posebno za besplatne aplikacije. Instalirajte samo aplikacije renomiranih dobavljača.

Sigurnost podataka:

- **Omogućite** funkcije daljinskog zaključavanja i brisanja, ako ih vaš uređaj podržava.
- **Pobrinite se** da temeljito uklonite osobne podatke s vašeg uređaja prije prodaje ili odbacivanja.

Sigurnost povezivanja:

- **Isključite** Bluetooth i Wi-Fi kada ih ne koristite.
- **Osigurajte** da se vaš uređaj ne povezuje automatski s novim Wi-Fi mrežama.

Detaljnije informacije o tome kako osigurati da svoj mobitel možete pronaći potražite pod 'Secure your mobile phone' na cyber.gov.au

Osobna kibernetička sigurnost: Prvi koraci

Razvijte svoje cyber sigurno razmišljanje

Osobna kibernetička sigurnost nije samo promjena postavki, već i promjena vašeg razmišljanja i ponašanja.

Pazite na cyber prijevare

Poznato je da kibernetički kriminalci koriste e-poštu, poruke, društvene medije ili telefonske pozive kako bi pokušali prevariti Australce. Mogu se pretvarati da su pojedinac ili organizacija za koju mislite da vam je poznata i da joj možete vjerovati.

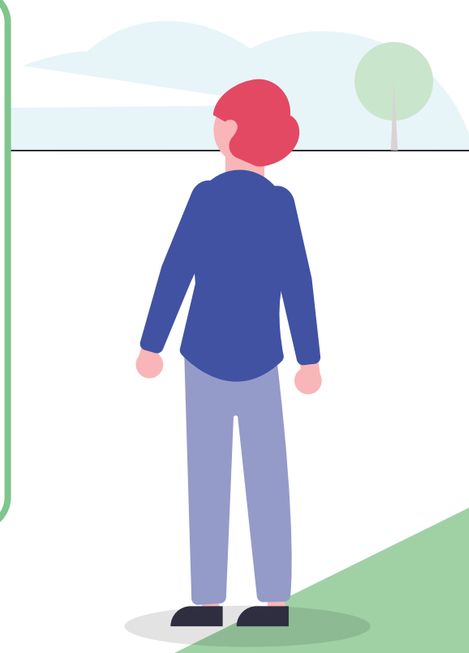
Putem poruka i poziva oni vas pokušavaju prevariti kako biste izvršili određene radnje, kao što su:

- Otkrivanje podataka o bankovnim računima, lozinkama i brojevima kreditnih kartica,
- Davanje daljinskog pristupa vašem računalu,
- Otvaranje privitka koji može sadržavati zlonamjerni softver,
- Slanje novca ili darovnih kartica.

Kako mogu prepoznati prijevarne poruke?

Prepoznati prijevarne poruke može biti teško. Kibernetički kriminalci često koriste određene metode prijevare. Njihove poruke mogu uključivati:

- **Autoritet:** tvrdi li se u poruci da dolazi od nekuda službeno, poput vaše banke?
- **Hitnost:** je li vam rečeno da postoji problem ili da imate ograničeno vrijeme za odgovor ili plaćanje?
- **Emocija:** tjera li vas poruka u paniku, nadu ili znatiželju?
- **Oskudica:** nudi li poruka nešto što je u nestašici ili obećava dobru ponudu?
- **Aktualni događaji:** je li poruka o aktualnoj vijesti ili velikom događaju?



Naučite kako uočiti krađu identiteta (phishing) ili prijevarne poruke tako da posjetite 'Learn the basics' na cyber.gov.au

Što trebam učiniti ako dobijem prijevarnu poruku?

Ako primite prijevarnu poruku ili telefonski poziv, trebali biste to zanemariti, izbrisati ili prijaviti ACCC-ovom Scamwatch na scamwatch.gov.au

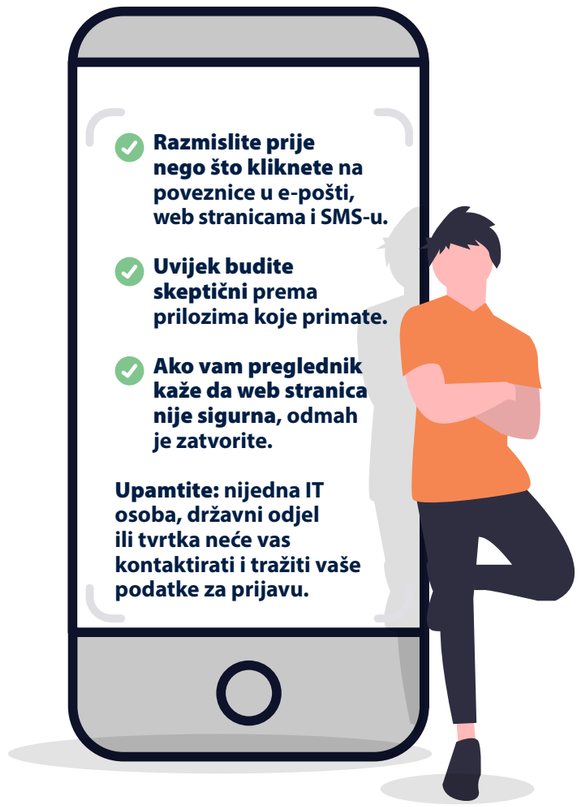
Možete također kontaktirati ACSC-ovu liniju za kibernetičku sigurnost na **1300 CYBER1** (1300 292 371) ako ste zabrinuti za svoju kibernetičku sigurnost.

Ako ste bili podvrgnuti prijevari i mislite da bi vaši bankovni računi, kreditne ili debitne kartice mogli biti ugroženi, odmah se obratite svojoj financijskoj instituciji. Možda će moći zatvoriti vaš račun ili zaustaviti transakciju.

Što ako ne znam zasigurno je li poruka prijevara?

Ako mislite da bi poruka ili poziv doista mogli biti od organizacije kojoj vjerujete (kao što je vaša banka), pronađite pouzdan način kontaktiranja. Potražite službenu web stranicu, nazovite njihov oglašeni telefonski broj, idite u direktno u trgovinu ili poslovnicu. Ne koristite poveznice ili podatke za kontakt u poruci koja vam je poslana ili dana putem telefona jer bi mogli biti lažni.

Savjet: Razmislite prije nego kliknete



Ako mislite da ste žrtva kibernetičkog kriminala, prijavite to putem ACSC-ovog ReportCyber na cyber.gov.au/report ili nazovite našu liniju za kibernetičku sigurnost na 1300 CYBER1 (1300 292 371).

Možete također biti u tijeku s najnovijim prijetnjama putem pretplate na ACSC-ovu besplatnu uslugu upozorenja. Potražite 'Subscribe to the ACSC alert service' na cyber.gov.au

Osobna kibernetička sigurnost: Prvi koraci

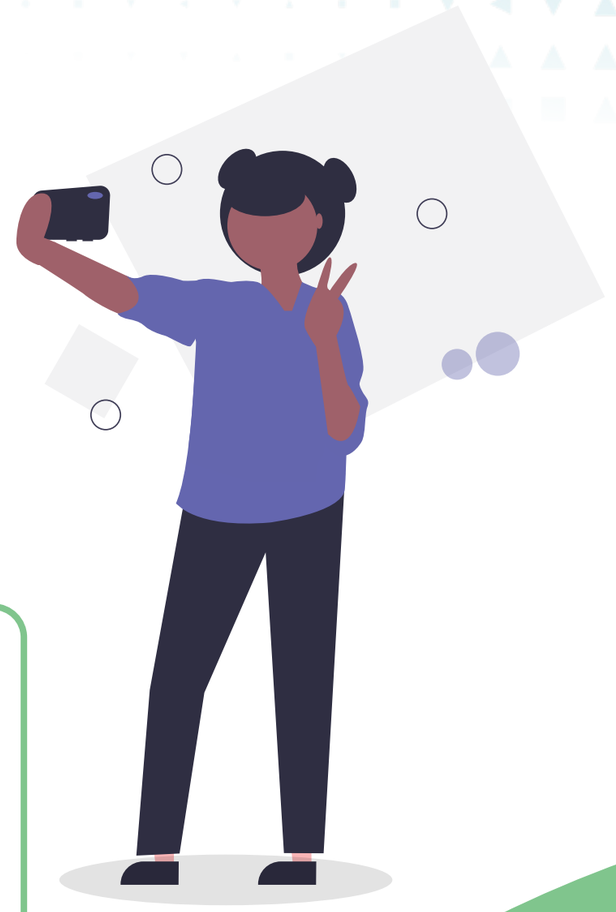
Stanite i razmislite prije nego što podijelite na društvenim mrežama

Informacije koje ste javno objavili na svojim računima društvenih medija kibernetički kriminalci mogu koristiti u svojim prijevarama i kibernetičkim napadima.

Imajte na umu da su informacije na internetu trajne i nikada ne možete u potpunosti ukloniti ono što je objavljeno.

Kako mogu stati i razmisliti prije objave?

- **Razmislite:** Kako bi kibernetički kriminalac mogao iskoristiti ove informacije da cilja na mene ili moje račune?
- **Razmislite:** Nebi li mi bilo nelagodno pokazati ovu informaciju ili sliku potpunom strancu izvan mreže?



Koje informacije trebam izbjegavati podijeliti?

Izbjegavajte dijeljenje informacija na internetu (uključujući fotografije) koje kibernetički kriminalci mogu upotrijebiti da vas identificiraju, manipuliraju prijevarom ili da pogode pitanja o oporavku vašeg računa. To može uključivati:

- Mjesto i datum rođenja.
- Adresu i broj telefona.
- Radnu povijest i poslodavce.
- Gdje ste išli u školu.
- Bilo koje druge osobne podatke koji se mogu upotrijebiti da vas uzmu na metu.

Sažetak kontrolnog popisa

Jeste li ispunili sve u ovom vodiču?

Upotrijebite ovaj praktični kontrolni popis kako biste pratili svoj napredak:

- **Uključeno je automatsko ažuriranje za sve moje uređaje:**
  - računalo (stolno i prijenosno).
  - mobitel.
  - tablet.
- **Aktivirana je provjera autentičnosti s više faktora na mojim najvažnijim računima:**
  - svi moji internetski bankovni i financijski računi (npr. banka, PayPal).
  - Svi moji računi e-pošte (npr. Gmail, Outlook, Hotmail, Yahoo!).
- **Redovito sigurnosno kopiram (back up) svoje uređaje:**
  - računalo (stolno i prijenosno).
  - mobitel.
  - tablet.
- **Koristim jedinstvene jake zaporke (passphrases) na svojim najvažnijim računima koji nisu zaštićeni više faktorskom autentifikacijom (MFA-om):**
  - Internetsko bankarstvo i financijski računi.
  - Računi e-pošte.
- **Provedene su sigurnosne mjere na mojim mobilnim uređajima:**
  - Prijenosnom računalu.
  - Mobitelu.
  - Tabletu.
- **Svaki dan koristim kibernetički sigurno razmišljanje:**
  - Mogu prepoznati prijevarne poruke.
  - Znam što učiniti ako primim prijevarnu poruku.
  - Znam kako provjeriti je li poruka prijevara ako nisam siguran/na.
  - Razmislim prije nego kliknem na poveznice i privitke.
  - Razmislim prije nego išta podijelim na društvenim mrežama.
- **Znam gdje potražiti pomoć ako sam žrtva kibernetičkog kriminala ili prijevare.**

Glosar

Aplikacija (App)
Također se naziva i mobilna aplikacija, a aplikacija je izraz za softver koji se obično koristi za pametni telefon ili tablet.

Aplikacija autentifikatora
Aplikacija koja se koristi za potvrdu identiteta korisnika računala da se dopusti pristup putem višefaktorske provjere autentičnosti (MFA).

Cyber kriminalac
Svaki pojedinac koji ilegalno pristupi računalnom sustavu ili računu kako bi oštetio ili ukrao informacije.

Daljinski pristup
Dobijte pristup i kontrolu nad uređajima i mrežama s druge lokacije.

Fizički token/privjesak
Fizički uređaj koji obično može stati na privjesak za ključeve, koji generira sigurnosni kod koji se koristi za potvrdu identiteta korisnika računala pomoću MFA.

Kraj podrške
Prestanak podrške odnosi se na situaciju u kojoj tvrtka prestaje podržavati proizvod ili uslugu. To se obično primjenjuje na hardverske i softverske proizvode kada tvrtka objavi novu verziju i prekine podršku za prethodne verzije.

Malware
Zlonamjerni softver koji se koristi za dobivanje neovlaštenog pristupa i kontrole nad korisničkim računalom, krađu informacija i ometanje ili onemogućavanje mreža.

Oblak
Mreža udaljenih poslužitelja koji pružaju masivnu, distribuiranu pohranu i procesorsku snagu.

Operacijski sustav
Softver instaliran na tvrdom disku računala koji omogućuje komunikaciju računalnog hardvera i pokretanje računalnih programa. Primjeri: Microsoft Windows, Apple macOS, iOS, Android.

Oporavak računa
Proces u kojem se skup pitanja ili druge metode provjere koriste za oporavak ili ponovni pristup računu ili za promjenu šifre/lozinke računa.

Privitak
Datoteka poslana uz poruku e-pošte.

Softver
Obično se nazivaju programima; zbirka uputa koje korisniku omogućuju interakciju s računalom, njegovim hardverom ili izvršavaju zadatke.

Uređaj
Računalni ili komunikacijski uređaj. Na primjer, računalo, prijenosno računalo, mobilni telefon ili tablet.

Izjava o odricanju odgovornosti
Materijal u ovom vodiču je općenite prirode i ne treba ga smatrati pravnim savjetom niti se na njega oslanjati za pomoć u bilo kojoj konkretnoj okolnosti ili hitnoj situaciji. O svim važnim stvarima trebali biste potražiti odgovarajući neovisni stručni savjet u odnosu na vlastite okolnosti.

Commonwealth ne prihvaća nikakvu odgovornost za bilo kakvu štetu, gubitak ili trošak nastao kao rezultat oslanjanja na informacije sadržane u ovom vodiču.

Za više informacija ili za prijavu incidenta kibernetičke 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