Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

ЛИЧНА САЈБЕР БЕЗБЕДНОСТ

ПРВИ ЧЕКОРИ

cyber.gov.au

Серија за лична сајбер безбедност

Серија за лична сајбер безбедност

Овој водич, ***„Лична сајбер безбедност: први чекори“***, е прв во серијата од три водичи наменети да им помогнат на обичните Австралијци да ги разберете основите на сајбер безбедноста. Научете како можете да преземете мерки за да се заштитите од вообичаените закани.

Први чекори

Следни чекори

Напредни чекори

Содржина

Вовед

Што е лична сајбер безбедност?

Во свет кој сè повеќе го води технологијата, секојдневно користиме уреди и сметки кои се чувствителни на сајбер закани:

- Вашите уреди може да вклучуваат компјутери, мобилни телефони, таблети и други уреди поврзани на интернет.
- Можеби исто така користите онлајн сметки за имејл, банкарски услуги, пазарење, социјални мрежи, видео игри и други работи.

Личната сајбер безбедност се однесува на постојаните чекори кои можете да ги преземете за да ги заштитите вашите сметки и уреди од сајбер закани.

Како овој водич може да ми помогне да се заштитам од сајбер закани?

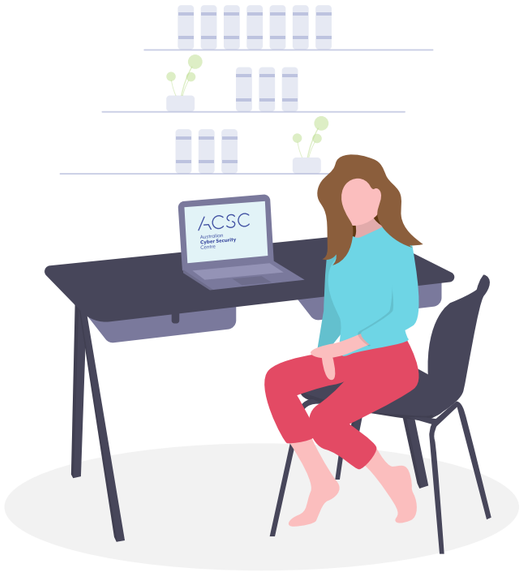
Ако за првпат се запознавате со сајбер безбедноста или сакате да бидете во тек со работите, овој водич е одлично место за почеток. Водичот „Лична сајбер безбедност: први чекори“ е прв во серијата од три водичи наменети да ви помогнат да ги разберете основите на сајбер безбедноста.

Што се сајбер закани?

Главните сајбер закани кои ги засегаат обичните Австралијци се **измамите и злонамерниот софтвер**.

- **Злонамерен софтвер е општ термин кој се користи да се опише злобен софтвер** дизајниран да предизвика штета. Ова може да вклучува вируси, црви, шпионски софтвер, тројански коњи и уценувачки програми. Сајбер криминалците користат злонамерен софтвер за да гу украдат вашите податоци и пари, а и да ги контролираат вашите уреди и сметки.
- **Измамите се пораки кои ги испраќаат сајбер криминалци** наменети да ве манипулираат да дадете чувствителни податоци или да активираат злонамерен софтвер на вашиот уред.

Овие напади можат да имаат значително лично и финансиско влијание на жртвите. Тие исто така стануваат пософистицирани и почести.



Вклучете го автоматското ажурирање на софтверот

Што е ажурирање?

Ажурирање е подобрена верзија на софтвер (програми, апликации и оперативни системи) кој сте го инсталирале на вашиот компјутер и мобилни уреди.

- **Ажурирањето на софтверот помага да ги заштитите вашите уреди** така што ќе ги отстраните софтверските „бубачки“ (грешки во кодирањето или слабости). Сајбер криминалците и злонамерниот софтвер можат да ги користат овие „бубачки“ за да пристапат до вашиот уред и да ги украдат вашите лични податоци, сметки, финансиски податоци и идентитет.
- Сајбер криминалците **постојано наоѓаат и злоупотребуваат нови „бубачки“**. Ажурирањето на софтверот на вашите уреди помага да се заштитите од сајбер напади.

Како да поставам автоматско ажурирање?

Автоматското ажурирање е стандардна или т.н. „постави и заборави“ поставка со која се инсталираат нови ажурирани верзии на софтвер веднаш штом се достапни.

- **Вклучете и потврдете го автоматското ажурирање** на сите софтвери и уреди.
- **Вклучувањето на автоматското ажурирање може да се разликува** во зависност од софтверот и уредите.
- Ако е можно, **одредете погодно време за автоматско ажурирање**, на пример, додека спиете или кога обично не го користите вашиот уред.

Вашиот уред мора да е вклучен, поврзан на струја и да има неискористен простор за складирање.

Совет: Ако ви биде побарано да го ажурирате софтверот на уредот, треба да го направите тоа што е можно поскоро.

Подетални информации како да го вклучите автоматското ажурирање може да најдете ако побарате „Ажурирање“ (Updates) на cyber.gov.au

Што ако поставката за автоматското ажурирање не е достапна?

Ако поставката за автоматско ажурирање не е достапна, треба редовно да проверувате за нови ажурирања и да ги инсталирате преку вашиот софтвер или менито за поставки на вашиот уред.

Што ако мојот постар уред и софтвер не примаат никакви ажурирања?

Ако вашиот уред, оперативен систем или софтвер се премногу стари, тие можеби повеќе нема да бидат поддржувани од производителот или развивачот на софтвер.

Кога производите ќе стигнат до оваа фаза кога „поддршката прекинува“, тие повеќе нема да добиваат ажурирања. Ова може да предизвика да станете ранливи на сајбер напади. Примери на производи кај кои поддршката прекинува ги вклучуваат оперативниот систем Windows 7 и iPhone 7.

Ако поддршката на вашиот уред, оперативен систем или софтвер завршува, ACSC препорачува надградба што е можно поскоро за да останете безбедни.

За повеќе информации, побарајте „Поддршката прекинува“ (End of support) на cyber.gov.au

Активирајте ја мулти-фактор автентикацијата (MFA)

Што е MFA?

Можете да ја користите мулти-фактор автентикацијата (MFA) за да ја подобрите безбедноста на вашите најважни сметки. MFA бара да создадете комбинација од два или повеќе видови на автентикација пред да се одобри пристап до сметката.

- **Нешто што знаете** (на пример, ПИН, лозинка или лозинка во форма на фраза)
- **Нешто што имате** (на пример, паметна картичка, физички токен, апликација за автентикација, СМС или имејл)
- **Нешто што е дел од вас** (на пример, отпечаток од прст, препознавање на лице или скен на шареница од око)

MFA им отежнува на сајбер криминалците да добијат почетен пристап до вашата сметка. Таа додава повеќе слоеви за автентикација за кои за да се пробијат е потребно повеќе време, напор и помагала.

Како можам да ја активирам MFA за да ги заштитам моите најважни сметки?

Чекорите за активирање на MFA се разликуваат во зависност од сметката, уредот или софтверската апликација. Треба да ја активирате MFA сега, почнувајќи со вашите важни сметки:

- Сите онлајн банковни и финансиски сметки (на пример, од вашата банка, PayPal)
- Сите имејл сметки (на пример, Gmail, Outlook, Hotmail, Yahoo!)

Ако имате многу имејл сметки, дадете им приоритет на оние кои се поврзани со вашите банкарски или други важни услуги.

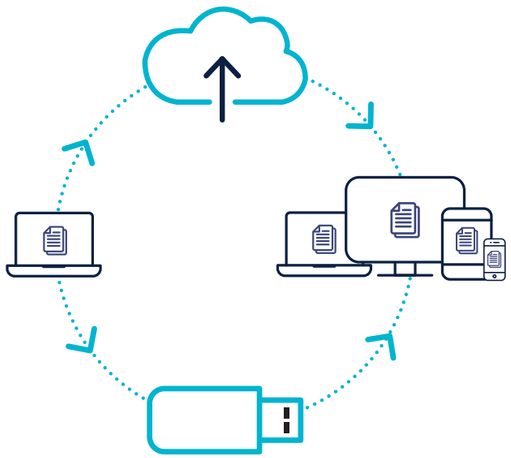
Можете да прочитате повеќе како да ја вклучите мулти-фактор автентикацијата ако побарате „Мулти-фактор автентикација“ (Multi-factor authentication) или „MFA“ на cyber.gov.au

Редовно правете резервни копии на вашите уреди

Што е резервна копија?

Резервна копија е дигитална копија на вашите податоци. Ова може да вклучува работи како што се фотографии, финансиски податоци или извештаи што сте ги зачувале на надворешен уред за складирање на податоци или во облакот.

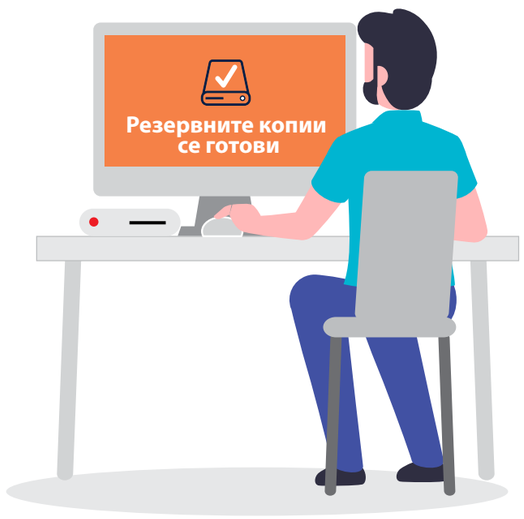
Правењето резервни копии од вашите податоци е мерка на претпазливост за тие да можат да се обноват доколку било кога се изгубат, украдат или оштетат.



Како да направам резервни копии на моите уреди и датотеки?

Треба редовно да правите резервни копии на вашите датотеки и уреди. Како тоа изгледа, без разлика дали го правите дневно, неделно или месечно, на крајот од краиштата зависи од вас. Колку пати ќе правите резервни копии може да зависи од бројот на:

- новите датотеки што ги вчитувате на вашиот уред,
- измените што ги правите на датотеките.



Совет: Редовно проверувајте ги вашите резервни копии за да се запознаете со постапката за обновување. Секогаш проверувајте дали вашите резервни копии работат правилно.

Подетални информации како да направите резервни копии од вашите податоци може да најдете ако побарате „Резервни копии“ (Backups) на cyber.gov.au

Користете лозинки во форма на фрази за да ги заштитите вашите важни сметки

Мулти-фактор автентикацијата (MFA) е еден од најефикасните начини да ги заштитите вашите сметки од сајбер криминалци. **Ако MFA не е достапна**, уникатна силна лозинка во форма на фраза може подобро да ја заштити вашата сметка во споредба со едноставна лозинка.

Што е лозинка во форма на фраза?

За лозинка се користи фраза од четири или повеќе случајно избрани зборови.

На пример: „глинен перек од кристален кромид“.

- **Лозинките во форма на фраза се побезбедни** од едноставните лозинки.
- На **сајбер криминалците име тешко** да ги пробијат лозинките во форма на фрази, но **лесно за вас** да ги запомнете.

Како можам да креирам лозинка во форма на фраза?

Креирајте лозинки во форма на фрази кои се:

- **Долги:** најмалку 14 букви, користејќи четири или повеќе случајно избрани зборови. Колку е подолга вашата лозинка во форма на фраза, толку е посигурна.
- **Непредвидливи:** користете комбинација од четири или повеќе случајно избрани или неповрзани зборови. Не користете познати фрази, цитати или стихови.
- **Уникатни:** неискористени за различни сметки.

Ако веб-страницата или услугата бара сложена лозинка која вклучува симболи, големи букви или бројки, можете да ги вклучите во вашата лозинка во форма на фраза. Таа сепак треба да биде долга, непредвидлива и уникатна за најдобра безбедност.

Кои сметки треба да ги заштитам со лозинка во форма на фраза?

Ако вашите најважни сметки не се заштитени со MFA, променете ги вашите лозинки со уникатни јаки лозинки во форма на фрази, почнувајќи со:

- Онлајн банковните и финансиските сметки
- Имејл сметките

Ако имате многу имејл сметки, дадете им приоритет на оние кои се поврзани со вашите банкарски или други важни услуги.

Обично можете да ја смените лозинката во уникатна силна лозинка во форма на фраза преку менито за поставки на вашата сметка.

Совет: Ако ви е тешко да ги запомните сите ваши лозинки во форма на фрази, размислете да користите управувач на лозинки. Со управувачот на лозинки треба да запомните само една лозинка, а за останатото ќе се погрижи тој. Барајте „управувач на лозинки“ (password manager) на cyber.gov.au за повеќе совети.

Подетални информации како да креирате безбедни лозинки во форма на фрази можете да најдете ако побарате „Лозинки во форма на фрази“ (Passphrases)’ на cyber.gov.au

Заштитете го вашиот мобилен уред

Денес паметните телефони и таблетите се користат во секојдневниот живот. Ги користиме за поврзување со другите, пазарување, работа, банкарски услуги, следење на нашата физичка кондиција и извршување на стотици задачи во секое време и од каде било.

Што може да се случи ако мојот мобилен уред е компромитиран, изгубен или украден?

- Може да го користат сајбер криминалци за да ги украдат вашите пари или идентитет. Тие го прават ова користејќи податоци складирани во вашиот уред, вклучително на сметките на социјалните мрежи и имејл.
- Може да изгубите незаменливи податоци како што се фотографии, белешки или пораки (ако немате резервни копии од нив).
- Сајбер криминалец може да го користи вашиот телефонски број за да измамува други луѓе.

Како да го заштитам мојот мобилен уред?

Безбедност на уредот:

- **Заклучете го** вашиот уред со лозинка во форма на фраза, обична лозинка, ПИН или шифра. Направете да биде тешко да се погоди – сајбер криминалците лесно можат да ги погодат вашиот датум на раѓање и шемите за заклучување. За оптимална заштита, користете лозинка во форма на фраза (видете на страница 6). Можеби исто така ќе сакате да размислите да користите препознавање на лице или отпечаток од прст да го отклучите вашиот уред.
- **Осигурете се** вашиот уред автоматски да се исклучува после кратко време на неактивност.
- **Не** го полнете уредот на јавни станици за полнење и избегнувајте да користите полначи од трети странки.
- **Третирајте го** вашиот телефон како вашиот паричник. Чувајте го безбеден и со вас во секое време.

Безбедност на софтвер и апликации:

- **Користете ја** функцијата за автоматско ажурирање на вашиот уред за да инсталирате нови апликации и ажурирање на оперативниот систем кога тие ќе бидат достапни.
- **Поставете го** уредот да бара лозинка во форма на фраза/обична лозинка пред да се инсталираат апликации. За оваа цел може да се користи и родителска контрола.
- **Проверете ги** дозволите за приватност внимателно кога инсталирате нови апликации на вашиот уред, особено бесплатни апликации. Инсталирајте апликации само од реномирани продавачи.

Безбедност на податоци:

- **Овозможете ги** функциите за далечинско заклучување и бришење, доколку вашиот уред ги поддржува.
- **Погрижете се** целосно да ги отстраните личните податоци од вашиот уред пред да го продадете или отстраните.

Безбедност на врската:

- **Исклучете ги** Bluetooth и Wi-Fi кога не ги користите.
- **Погрижете се** вашиот уред да не се поврзува автоматски на нови Wi-Fi мрежи.

Подетални информации за тоа како можете да го заштитите вашиот мобилен телефон можете да најдете ако барате „Заштитете го вашиот мобилен телефон“ (Secure your mobile phone) на cyber.gov.au

Научете да размислувате за вашата сајбер безбедност

Личната сајбер безбедност не се однесува само на менувањето на вашите поставки, туку исто така и на менување на начинот на кој размислувате и се однесувате.

Внимавајте на сајбер измами

Познато е дека сајбер криминалците користат имејл, пораки, социјални мрежи или телефонски повици за да се обидат да ги измамат Австралијците. Тие можат да се преправаат дека се поединец или организација за кои мислите дека ги знаете или треба да им верувате.

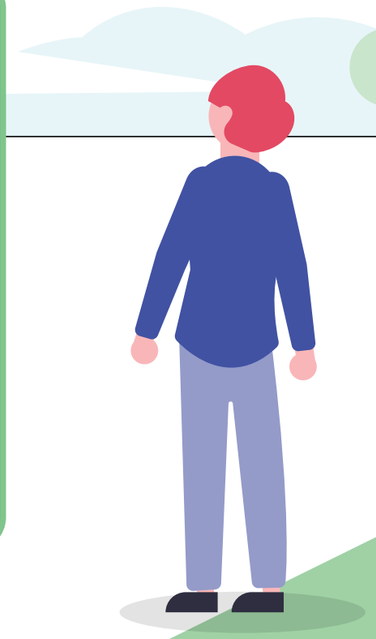
Со нивните пораки и телефонски повици, тие се обидуваат да ве измамат да направите одредени работи, на пример:

- Да ги дадете деталите за вашите банковни сметки, лозинки и броевите на кредитни картички,
- Да овозможите далечински пристап до вашиот компјутер,
- Да отворите прилог кој содржи злонамерен софтвер,
- Да испратите пари или подарок-картички.

Како можам да препознаам лажни пораки?

Може да биде тешко да преознаете лажни пораки. Сајбер криминалците често користат одредени методи да ве измамат. Нивните пораки може да вклучуваат:

- **Авторитет:** дали во пораката се тврди дека е од службено лице, на пример, од вашата банка?
- **Итност:** дали ви се кажува дека постои проблем или дека имате ограничено време да одговорите или платите?
- **Емоции:** дали пораката предизвикува да чувствувате паника, надеж или љубопитност?
- **Оскудност:** дали пораката нуди нешто што е во мали залихи или ветува добра зделка?
- **Тековни настани:** дали пораката се однесува на актуелни вести или голем настан?



Научете како да препознаете пораки со лажно претставување (phishing) или измама со посета на „Научете ги основите“ (‘Learn the basics) на cyber.gov.au

Што треба да направам ако добијам лажна порака?

Ако добиете лажна порака или лажен телефонски повик, треба да ги игнорирате, избришете или пријавите на Scamwatch на ACCC на scamwatch.gov.au

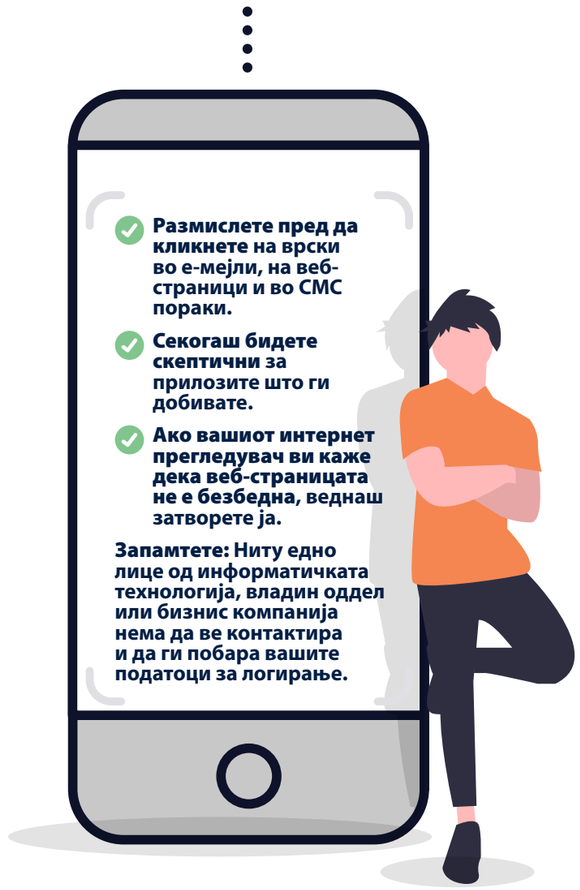
Исто така, ако сте загрижени за вашата сајбер безбедност, можете да се јавите на дежурната линија за сајбер безбедност на ACSC (ACSC's Cyber Security Hotline) на **1300 CYBER1** (1300 292 371).

Ако сте биле жртва на измама и верувате дека вашите банковни сметки, кредитни или дебитни картички можеби се изложени на ризик, веднаш контактирајте ја вашата финансиска институција. Можеби ќе можат да ја затворат вашата сметка или да ја запрат трансакцијата.

Што ако не сум сигурен/сигурна дека пораката е измама?

Ако мислите дека пораката или повикот всушност може да се од организација на која и верувате (како што е вашата банка), најдете кредибилен начин за контакт. Побарајте ја официјалната веб-страница, јавете се на нивниот огласен телефонски број или посетете физичка продавница или филијала. Немојте да ги користите врските или контактните податоци во пораката што ви е испратена или дадена преку телефон, бидејќи тие може да биде лажни.

Совет:
Размислете пред да кликнете.



Ако мислите дека сте жртва на сајбер криминал, пријавете го тоа преку ReportCyber на ACSC на cyber.gov.au/report или јавете се на нашата дежурна телефонска линија за сајбер безбедност на 1300 CYBER1 (1300 292 371).

Можете исто така да бидете во тек со најновите закани ако се претплатите на бесплатната услуга за предупредување на ACSC. Барајте „Претплатете се на услугата на ACSC за предупредување" (Subscribe to the ACSC alert service) на cyber.gov.au. Ќе ви испратиме предупредување кога ќе идентификуваме нова сајбер закана.

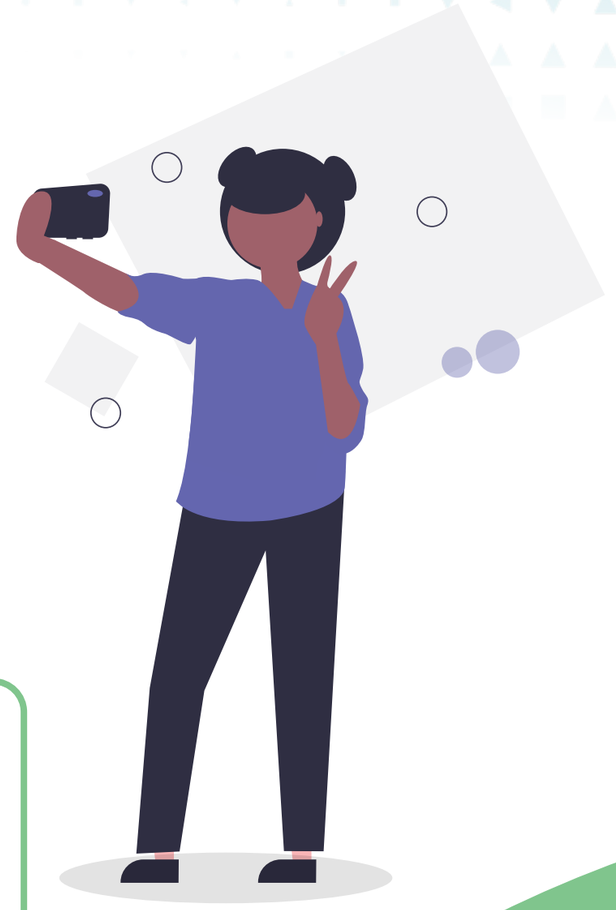
Застанете и размислете пред да споделите нешто на социјалните мрежи

Во нивните измами и сајбер напади, сајбер криминалците можат да ги користат информациите што сте ги објавиле јавно на вашата/вашите сметка/сметки на социјалните мрежи.

Запамтете дека информациите на Интернет се трајни и никогаш не можете целосно да го отстраните тоа што е објавено.

Како можам да застанам и да размислам пред да објавам нешто?

- **Размислете:** Како може сајбер криминалецот да ги искористи овие информации за да ме стави на мета мене или моите сметки?
- **Размислете:** Дали би ми било пријатно да му ги покажам овие информации или слика на лице кое воопшто не го познавам кога не сум на интернет?



Кои информации треба да избегнувам да ги споделувам?

Избегнувајте да споделувате информации (вклучително фотографии) онлајн кои сајбер криминалците можат да ги користат за да ве идентификуваат, да ве манипулираат преку измама или да ги одгатнат прашањата за повторно воспоставување на вашата сметка. Ова може да ги вклучува:

- Вашето место и датум на раѓање.
- Вашата адреса и телефонски број.
- Вашиот работодавец и работната историја.
- Училиштето во кое сте посетувале настава.
- Било какви други лични податоци кои може да се користат за да бидете мета.

Краток список за проверка

Дали сте направиле сè според овој водич?

Користете го овој практичен список за проверка за да следите како напредувате:

- **Го вклучив автоматското ажурирање на сите мои уреди:**
  - Компјутер (статичен и лаптоп)
  - Мобилен телефон
  - Таблет
- **Ја активирав мулти-фактор автентикацијата на моите најважни сметки:**
  - Сите мои онлајн банковни и финансиски сметки (на пример, од вашата банка, PayPal)
  - Сите мои имејл сметки (на пример, Gmail, Outlook, Hotmail, Yahoo!)
- **Редовно правам резервни копии на моите уреди:**
  - Компјутер (статичен и лаптоп)
  - Мобилен телефон
  - Таблет
- **Користам уникатни силни лозинки во форма на фрази на моите најважни сметки кои не се заштитени со MFA:**
  - Онлајн банковни и финансиски сметки
  - Имејл сметки
- **Ги заштитив сите мои мобилни уреди:**
  - Лаптоп
  - Мобилен телефон
  - Таблет
- **Секој ден внимавам на сајбер безбедноста:**
  - Можам да препознавам лажни пораки
  - Знам што да правам ако примам лажна порака
  - Знам како да проверам дали некоја порака е лажна ако не сум сигурен/сигурна
  - Размислувам пред да кликнам на врски и прилози
  - Размислувам пред да споделам нешто на социјалните мрежи
- **Знам каде да се обратам за помош ако сум жртва на сајбер криминал или измама**

Речник

Повторно воспоставување на сметка (Account recovery)
Процес во кој се користат група прашања или други методи на потврдување на идентитет за повторно воспоставување или повторно добивање на пристап на сметка или за менување на лозинката во форма на фраза/обичната лозинка.

Злонамерен софтвер (Malware)
Злобен софтвер кој се користи за да се добие неовластен пристап и контрола врз компјутерот на корисникот, да се украдат податоци и да се попречат или исклучат мрежите.

Апликација (App)
Исто така наречена мобилна апликација, терминот „ апликација“ се однесува на софтвер што обично се користи на паметен телефон или таблет.

Прилог (Attachment)
Датотека испратена со е-мејл порака.

Оперативен систем (Operating system)
Софтвер инсталиран на компјутерскиот хард диск кој овозможува компјутерскиот хардвер да комуницира и да раководи со компјутерски програми. Примери: Microsoft Windows, Apple macOS, iOS, Android.

Физички токен (Physical token)
Физички уред кој вообичаено може да се стави на привезок за клучеви и кој создава безбедносен код што се користи да се потврди идентитетот на корисникот на компјутер кој користи MFA.

Апликација за автентикација (Authenticator app)
Апликација што се користи да се потврди идентитетот на корисникот на компјутер за да се дозволи пристап преку мулти-фактор автентикација (MFA).

Облак (Cloud)
Мрежа на далечински сервери кои имаат моќ да врши масовна дистрибуција на складирање и обработка на податоци.

Далечински пристап (Remote access)
Овозможува пристап и контрола на уреди и мрежи од друга локација.

Сајбер криминалец (Cybercriminal)
Секое лице кое незаконски пристапува до компјутерски систем или сметка за да направи штета или украде податоци.

Уред (Device)
Компјутерски или комуникациски уред. На пример, компјутер, лаптоп, мобилен телефон или таблет.

Софтвер (Software)
Обично познат како програми, збир на упатства кои му овозможуваат на корисникот да работи со компјутер, неговиот хардвер или да извршува задачи.

„Поддршката прекинува“ (End of support)
Терминот „поддршката прекинува“ се однесува на ситуација кога некоја компанија престанува да дава поддршка за некој производ или услуга. Ова обично се однесува на хардверски и софтверски производи кога компанијата објавува нова верзија и ја прекинува поддршката за претходните верзии.

Одрекување од одговорност
Материјалот во овој водич е од општ карактер и не треба да се смета како правен совет или материјал на кој можете да се потпирате за помош во било кои одредени околности или итни ситуации. За сите важни работи треба да побарате совети од соодветно независно професионално лице за вашите сопствени околности.

Комонвелтот не прифаќа никаква одговорност или обврска за каква било штета, загуба или трошоци кои произлегуваат поради доверба на информациите во овој водич.

За повеќе информации или да пријавите инцидент во врска со сајбер безбедноста, контактирајте не на:

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

Овој број е достапен за користење само во Австралија.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre