# ПРИЈАВЕТЕ САЈБЕР НАПАДИ И ИНЦИДЕНТИ ЗА АВСТРАЛИЈА ДА БИДЕ БЕЗБЕДНА.

## ПРИЈАВЕТЕ СЕ

На нашата бесплатна услуга за предупредување,
**cyber.gov.au**

## ПРИЈАВЕТЕ

Сајбер криминал на REPORTCYBER:
**cyber.gov.au/report**

## КОНТАКТИРАЈТЕ НÈ

Јавете се на 1300 CYBER1 оили посетете ја веб-страницата **cyber.gov.au**

Овој број е достапен за користење само во Австралија.

## СЛЕДЕТЕ НÈ

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

## 5. ВНИМАВАЈТЕ НА ИЗМАМИ

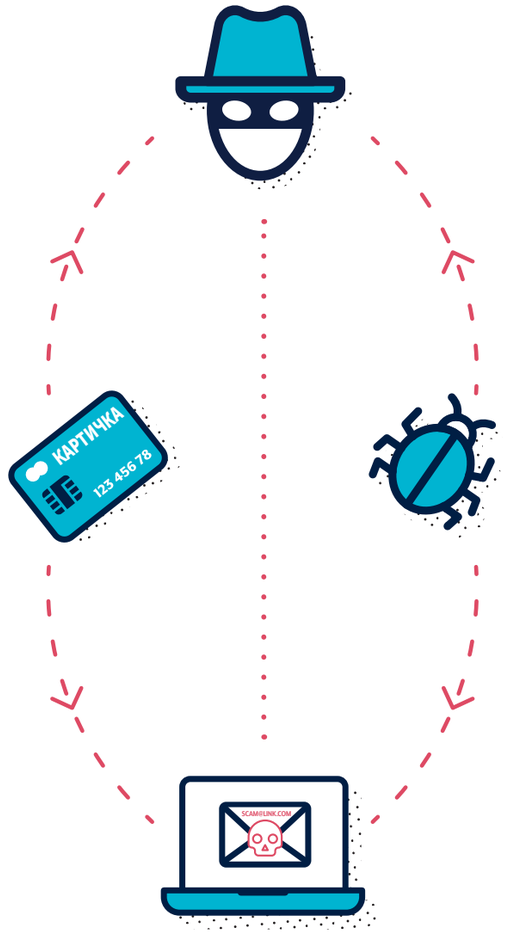
**Сајбер криминалците користат имејл, СМС пораки, телефонски повици и социјални медиуми за да ве прелажат да отворите прилог, да посетите веб-страница, да откриете детали за пријавување на сметка, да откриете чувствителни информации или да префрлите пари или подарок-картички. Овие пораки се направени да изгледаат како да биле испратени од поединци или организации кои мислите дека ги познавате или мислите дека треба да им верувате.**

За да откриете пораки кои се измами, застанете и размислете:

- **Авторитет:** Дали во пораката се тврди дека таа е од службено лице?
- **Итност:** Дали ви е кажано дека имате ограничено време да одговорите?
- **Чувства:** Дали пораката предизвикува да чувствувате паника, страв, надеж или љубопитност?
- **Реткост:** Дали пораката нуди нешто што тешко се наоѓа?
- **Тековни настани:** Дали пораката е за актуелни вести, големи настани или одредено време во годината (на пример, за пријавување на данок)?

За да проверите дали пораката е легитимна:

- Вратете се на нешто во кое имате доверба. Посетете ја официјалната веб-страница, пријавете се на вашата сметка или телефонирајте на нивниот огласен телефонски број. Не ги користете врските или податоците за контакт наведени во пораката што ви била испратена или дадена преку телефон.
- Проверете за да видите дали официјалниот извор веќе ви има кажано што нема никогаш да ве прашуваат. На пример, вашата банка можеби ви кажала дека никогаш нема да ја побара од вас вашата лозинка.




За повеќе информаци како да откриете лажни пораки, видете ја публикацијата Detecting Socially Engineered Messages (Откривање на пораки од социјален инженеринг) на Australian Cyber Security Centre (ACSC) (Австралиски центар за сајбер безбедност) и бидете информирани со тоа што ќе се пријавите на ACSC's Alert Service (Служба за предупредување на ACSC) на **cyber.gov.au.**

# ЛЕСНИ ЧЕКОРИ

## ДА ГИ ЗАШТИТИТЕ ВАШИТЕ УРЕДИ И СМЕТКИ

**СО СЛЕДЕЊЕ НА ОВИЕ ЧЕКОРИ НАМАЛЕТЕ ГО РИЗИКОТ ДА СТАНЕТЕ ЦЕЛ НА САЈБЕР КРИМИНАЛЦИ**

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

# 1. НАДГРАДУВАЈТЕ ГО СОФТВЕРОТ НА ВАШИТЕ УРЕДИ

**Сајбер криминалците незаконски влегуваат во уредите користејќи познати слабости на системите и апликациите. Новите верзии на софтвер имаат надградби за безбедност со цел отстранување на овие слабости. Вклучете го автоматското надградување за да не мора да го правите тоа рачно.**

Вклучете го автоматското надградување на сите ваши уреди:

- Мобилен телефон
- Лаптоп
- Десктоп

Редовно проверувајте за надградување на вашите:

- Апликации
- Програми
- „Паметни“ уреди


# 2. ВКЛУЧЕТЕ ЈА МУЛТИ-ФАКТОР АВТЕНТИКАЦИЈАТА (MFA)

**MFA ја подобрува вашата безбедност со тоа што повеќе им отежнува на сајбер криминалците да имаат пристап до вашите датотеки или сметка.**

Активирајте ја MFA, почнувајќи од вашите најважни сметки:

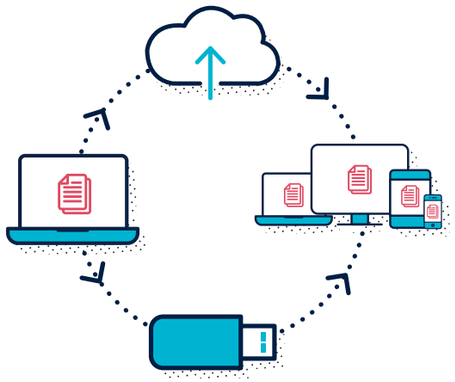
- Имејл сметки
- Онлајн банковни сметки и сметки со зачувани податоци за плаќање
- Сметки на социјални медиуми


# 3. ПРАВЕТЕ РЕЗЕРВНИ КОПИИ НА ПОДАТОЦИТЕ ВО ВАШИТЕ УРЕДИ

**Резервна копија (backup) е дигитална копија на зачуваните информации во вашиот уред, како што се фотографии, документи, видео-записи и податоци од апликации. Тие може да се зачуваат во надворешни уреди за чување на податоци или во облак. Правењето резервни копии значи дека можете да ги обновите вашите датотеки во случај вашиот уред некогаш да биде загубен, украден или оштетен.**

Редовно правете резервни копии на вашите уреди:

- Мобилен телефон
- Лаптоп компјутер
- Десктоп компјутер
- Таблет



# 4. КРЕИРАЈТЕ БЕЗБЕДНИ ЛОЗИНКИ ВО ФОРМА НА ФРАЗИ

**Во случаи кога не е достапна MFA, единствената работа што може да ги заштити вашите информации и сметки од криминалци е безбедна лозинка во форма на фраза (passphrase).**

За лозинка користете фраза од четири или повеќе случајно избрани зборови. Заменете ги вашите лозинки од единечни зборови со лозинки во форма на фрази и осигурете се тие да бидат:

- Долги: Колку е подолга фразата што ја користите како лозинка, толку подобро. Таа треба да има најмалку 14 букви
- Непредвидливи: Користете комбинација на случајно избрани зборови кои не се поврзани
- Единствена: Не ги користите лозинките во форма на фрази на повеќе сметки