Преглед на онлајн презентација

Australian Government

Be Connected
Every Australian online.

Заштита на вашите лични податоци онлајн

Скоро секоја апликација, платформа за социјални медиуми или веб-страница бара од вас барем некои лични информации. Вашите лични податоци ги вклучуваат сите детали или податоци што може да се користат за да бидете идентификувани, како што се детали каде се наоѓате или каде живеете, како и други уникатни, специфични детали. Важно е секогаш добро да размислите во врска со споделувањето на лични податоци.

Заштитата на вашите лични податоци е важна

Заштитата на вашите лични податоци е многу важна бидејќи измамниците и крадците на идентитет можат да ги користат за да се преправаат дека сте вие. Тие можат да создадат лажни сметки во ваше име и да дејствуваат на начини кои би можеле да имаат влијание на вас сега или во иднина. Ова може да вклучува измама, како што е кражба на пари од вашата банкарска сметка или земање заем на ваше име.

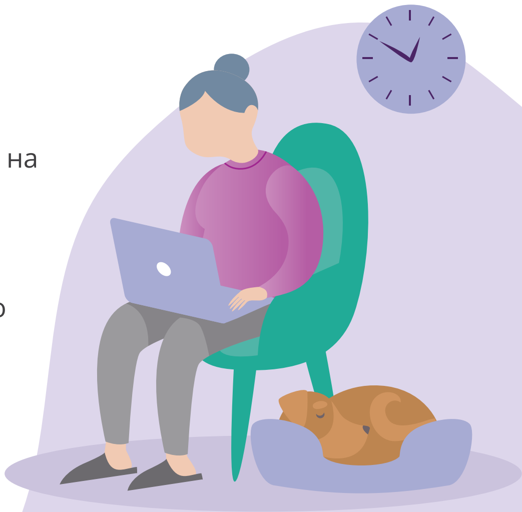
Измамниците може да ги користат вашите податоци самостојно или во контекст со други информации. Може да вклучува секојдневни работи што се специфични за вас, како што се вашите:

Лични податоци

- Име и презиме
- Домашна адреса
- Телефонски број
- Датум на раѓање
- Број на возачка дозвола
- Детали за банкарска сметка
- Имејл адреса
- Кориснички имиња и лозинки

Документи за идентификација

- Возачка дозвола
- Пасош
- Извод од матична книга на родените
- Medicare картичка
- Австралиска виза или потврда за државјанство
- ImmiCard



Бидете свесни за она што го споделувате

Социјални мрежи

Добра идеја е да избегнувате споделување лични податоци на вашите сметки на социјалните мрежи. Измамниците можат да научат многу за вас од деталите што ги споделувате онлајн. Понекогаш тие создаваат објави со квизови или прашања наменети да ве измамат да споделувате лични податоци. Тие ги користат овие податоци за да ги погодат лозинките на вашата сметка или да станете мета на други измами.

Користење на апликации

Преземајте апликации само од официјалните продавници за апликации и прочитајте ги правилниците за приватност и оценките од други корисници пред да преземете било што. Можете исто така да го ограничите бројот на податоци до коишто имаат пристап апликациите. Некои апликации бараат непотребен пристап до вашите списоци со контакти, камерата, просторот за складирање податоци, локацијата и микрофонот. Прегледајте ги и приспособете ги дозволите за апликациите во менито за поставки (settings menu) на вашиот паметен уред.

Запомнете: Прифаќајте барања за пријатели само од луѓе што ги познавате во вистинскиот живот, поставете ги вашите сметки на социјалните мрежи да бидат приватни и прегледајте кој може да види што споделувате.

Чувајте ги вашите податоци безбедни

Користете го обезбедувањето на уредот

Користењето безбедносен софтвер на вашиот компјутер е еден од наједноставните начини да се заштитите себеси и вашата приватност. Добрата компјутерска безбедност вклучува инсталирање на реномирани анти-шпионски софтвер, антивирусни скенери и „firewall“ софтвер. Исто така, треба да ги ажурирате вашите онлајн безбедносни алатки и апликации со овозможување автоматско ажурирање. Користете автоматско и временско заклучување на екранот или „screensavers“ заштитени со лозинка, и поставете автоматско заклучување по повеќе неуспешни обиди за пријавување.

Совет: Апликација за управување со лозинки исто така може да ви помогне да составите и чувате сложени фрази за лозинка што другите тешко можат да ги погодат или хакираат. На веб-страницата на Be Connected можете да најдете информации за **управувачи со лозинки (password managers)** и како да ги поставите.

Фрази за лозинка (Passphrases)

Чувајте ги вашите сметки безбедни со силни фрази за лозинка. Фрази за лозинка се посигурна верзија на лозинки и се составени од четири или повеќе случајни зборови.

Обидете се да смислите различни фрази за лозинка за секоја од вашите сметки и не рециклирајте делови од старите.

Кога ќе ја изберете вашата лозинка, направете ја:

- **Долга -** најмалку 14 знаци
- **Непредвидлива -** користете четири или повеќе случајни зборови со бројки, симболи и големи и мали букви
- **Уникатна –** немојте повторно да ги користите вашите фрази за лозинка

*На пример: Yellow So Hey Plant > Yell*w-S0heyPl@nt!*

Совет: Проверете ја јачината на лозинката користејќи го проверувачот за јачина на лозинката на владата на Нов Јужен Велс на веб-страницата **nsw.gov.au/id-support-nsw/be-prepared/passwords**

Повеќефакторска автентикација

Секогаш е добра идеја да вклучите повеќефакторска автентикација за вашите сметки. Повеќефакторската автентикација (исто така позната како автентикација во 2 чекора) додава дополнителен слој на безбедност. Ова значи дека кога ќе се најавите на сметка со вашата лозинка, можеби ќе биде побарано да направите дополнителен чекор за да потврдите дека сте вие - како на пример, да внесете код од текстуална порака или да користите идентификација со препознавање лице.

Купувајте безбедно онлајн

Кога купувате онлајн, погрижете се да користите доверливи продавници и разгледајте оценки од корисниците. Пред да ги внесете вашите лични податоци, проверете дали веб-страницата користи „https" на почетокот на името на нејзиниот домен или има безбедносна икона во прелистувачот, обично мал, заклучен катанец, што покажува дека е побезбедна веб-страница. Кога купувате, користете безбеден начин на плаќање како што се PayPal, BPAY или вашата кредитна картичка.

Користете сигурна конекција

Кога треба да пристапите до важни сметки, да испраќате чувствителни информации или да внесете лозинки, поврзете се на доверлива интернет конекција, како што е домашната, на работа или со користење на вашата сопствена податочна мрежа доколку е достапна. Јавниот Wi-Fi не е толку безбеден како вашиот Wi-Fi дома или на работа.

Измами и неовластен пристап до податоци (Scams and data breaches)

Заштитете се од измами

Бидете свесни за измамите и како тие функционираат - тоа е еден од важните чекори за нивно избегнување. Измамниците се преправаат дека се од организација или личност што ја познавате за да се обидат да ве измамат да им ги предадете вашите лични податоци. Овие измами се нарекуваат измами со имитирање.

Запомнете да:

Застанете – не давајте пари или лични податоци на никого ако не сте сигурни
Измамниците честопати бараат од вас да потврдите кои сте или бараат од вас да извршите плаќање.

Размислете - запрашајте се дали пораката или повикот можеби се лажни?
Пазете се од неочекувани повици, пораки и имејли. Ако не сте сигурни за пораката, јавете се во организацијата директно користејќи го телефонскиот број што се наоѓа на нивната веб-страница.

Заштитете се - дејствувајте брзо ако нешто не е во ред
Контактирајте ја вашата банка ако забележите некоја необична активност или ако измамник ги добие вашите пари или податоци.

Совет: Посетете ја веб-страницата Be Connected за нашиот бесплатен **водич за измами** со имитирање подготвен со Scamwatch.

Неовластен пристап до податоци (Data Breaches)

Неовластен пристап до податоци се случува кога до личните податоци што ги чува некоја организација се пристипи или се откриваат без овластување или се губат. Многу организации и владини агенции имаат законска одговорност да ви кажат дали вашите лични податоци се вклучени при нарушување на безбедноста на податоци, која веројатно ќе ви предизвика сериозна штета.

Ако вашите податоци се вклучени при неовластен пристап до податоци, погрижете се да дејствувате брзо и да добиете совет од **Канцеларијата на австралискиот комесар за информации (Office of the Australian Information Commissioner)**. Дејството што ќе го преземете зависи од податоците до кои е пристапено. Водете евиденција за тоа што го правите. Може да добиете и бесплатна поддршка и совет од **IDCARE**.

За да дознаете дали на веб-страницата или апликацијата што ја користите имало неовластен пристап до податоците, можете да ги проверите службите како што е **haveibeenpwned.com**. Ако тоа се случило, веднаш сменете ги лозинките.

Измама на идентитет

Ако знаете или се сомневате дека вашиот идентитет е украден:

- Поднесете пријава до Австралискиот центар за сајбер безбедност на Австралиската дирекцијата за сигнали (Australian Signals Directorate’s Australian Cyber Security Centre) на **ReportCyber**.
- Контактирајте ја полицијата на 131 444. Побарајте полициски извештај или референтен број како доказ дека сте поднеле пријава.
- Ако знаете или се сомневате каков вид на лични податоци се украдени, контактирајте со соодветната агенција или организација за да ги известите.
- Известете ја вашата финансиска институција што е можно поскоро.
- Поднесете пријава до Националниот центар против измама (National Anti-Scam Centre) во **Scamwatch** ако тоа било дел од измама.

Одвојте време да дознаете повеќе за Be Connected

Be Connected е сеопфатна веб-страница со бесплатни материјали специјално дизајнирани да им помогнат на постарите Австралијци безбедно да се поврзуваат онлајн и со сигурност да се движат низ дигиталниот свет. Веб-страницата е исто така корисна за семејствата и организациите во заедницата кои сакаат да им помогнат на постарите членови на заедницата да пристапат до сите придобивки на интернет.

Посетете ја веб-страницата beconnected.esafety.gov.au

Australian Government | eSafety Commissioner

Оваа програма е подготвена од eSafety како дел од иницијативата Be Connected.