Australian Government | Be Connected
Every Australian online.

Вовед во безбедност на интернет

Да ви помогнеме да бидете сигурни дека безбедно користите интернет.

Безбедност на компјутерот и имејлот

Некои од главните ризици на интернет вклучуваат:

- **Вируси** кои се пренесуваат преку интернет од компјутер на компјутер. Некои се само непријатни, други може и да ги избришат вашите податоци.
- **Trojans** („тројански коњи“) се програми што изгледаат безопасно и се обидуваат да ве измамат да ги инсталирате.
- **Spyware** („шпионски“ програми) се програми кои крадат информации како што се лозинки (passwords) или податоци од банковни сметки.

Постојат чекори за заштита од закани на интернет, и за вас и за вашиот компјутер.

1. Користете **антивирусни програми** кои помагаат да се откријат, спречат и отстранат вирусите.
2. Користете **антивирусни програми** кои помагаат да се спречи вашите податоци да бидат украдени.
3. Користете **firewall** (заштитен ѕид) кој помага вашиот компјутер да биде заштитен од неовластен пристап од интернет.
4. Одржувајте ја вашата програма за безбедност на интернет ажурирана.
5. Ако заедно со нов компјутер добиете антивирусна програма, обновете ја кога ќе помине пробниот (trial) период или инсталирајте бесплатна програма како што е AVG. Ве молиме имајте предвид дека Windows 10 доаѓа со ефикасна антивирусна програма наречена Windows Defender. Windows ќе ја одржува ажурирана наместо вас.
6. Ако не сте сигурни, побарајте совет на **https://www.staysmartonline.gov.au/.**

Вовед во безбедност на интернет

Треба да бидете многу внимателни вашиот компјутер да не го изложите на злонамерни програми.

1. Размислете двапати пред да отворите имејли и особено attachments (прилози на имејли) од луѓе кои не ги познавате.
2. На интернет работете со бизниси за кои знаете дека имаат добар углед. Побарајте информации за секоја компанија пред да купувате од неа.
3. Редовно правете копии (backups) на сите информации во вашиот компјутер. Ако тој се зарази со вируси, сеуште ќе ги имате сочувано вашите важни податоци.

Заштитете се себеси и вашиот компјутер од закани на интернет

Користење на лични податоци на интернет

Понекогаш на интернет треба да се дадат лични информации, но постојат граници колку информации треба да споделите и треба да сте свесни за вашите права.

- Ако треба да се провери вашиот идентитет, информации давајте само на веродостојни компании.
- Одбегнувајте да објавите лични информации (датум на раѓање, домашна адреса итн.) на јавни форуми како што е Facebook. Личните податоци можат од бидат искористени од криминалци за кражба на идентитетот.
- Користењето на лични податоци од страна на приватните компании е регулирано со закон. Во Австралија тоа е Законот за приватност од 1988 година (Privacy Act 1988).
- Законот за слобода на информациите може да важи во однос на информациите што ги давате на владините тела.
- Угледните компании имаат прописи за тоа како се грижат за личните податоци. Прочитајте ги нивните правилници за приватност на нивните интернет страници.
- За повеќе информации за правата на потрошувачите или за најновите информации како да се заштитите од измами (scams), ве молиме видете на интернет страницата ACCC: https://www.accc.gov.au/consumers.

Користењето на лични информации од страна на приватни компании во Австралија е регулирано со закон

Вовед во безбедност на интернет

Плаќање на интернет и безбедни подрачја

Бидете внимателни во однос на информациите што ги споделувате на интернет

Купувањето на интернет може да биде практично и постојат некои брзи проверки за да се осигура дека плаќањето е безбедно.

1. Дали компанијата со која имате работа има добар углед? На интернет страницата на компанијата проверете ги нејзините принципи за приватност и за враќање на парите. Користете интернет пребарувач (search engine) за да дознаете повеќе за компанијата.
2. Плаќајте со кредитна картичка или преку PayPal. Двата начина нудат извесни форми на заштита на купувачите.
3. Пред да ги внесете податоците од вашата кредитна картичка, проверете го просторот **Address bar** на вашиот пребарувач (browser). Безбедна страница треба да е означена со цртеж на катанец, а адресата на интернет страницата треба да почнува со **https:** (не само со **http:**).

Детска безбедност на интернет

Децата имаат помалку искуство за светот околу нив, па се изложени на поголем ризик од:

- Гледање несоодветни материјали.
- Откривање на лични информации.
- Насилничко однесување и малтретирање.

Chatrooms („соби за дрдорење“) и социјалните мрежи се места каде може да дојде до контакти. Никогаш не му дозволувајте на вашето дете да се сретне со некого што го „запознал“ на интернет, ако детето не е во придружба на возрасно лице.

Постојат заштитни чекори што може да ги преземете за вашето дете да биде безбедно на интернет.

1. На компјутерот креирајте корисничка сметка (user account) на детето.
2. Вклучете ја опцијата родителска контрола (parental controls) за таа корисничка сметка.
3. Во Google активирајте **SafeSearch**, а во Bing или Yahoo опцијата SafeSearch наместете ја на **strict**.
4. YouTube и сите други видео интернет страници (video sites) наместете ги на Restricted (Ограничено).
5. Разговарајте со вашето дете за опасностите со кои може да се соочи на интернет.

Ако некое дете случајно се најде во опасна ситуација на интернет, пријавете во Office of the eSafety Commissioner (Канцеларија на Началникот за електронска безбедност) на https://www.esafety.gov.au/complaints-and-reporting.