Водич за дигитални права

Механизми за заштита и пријавување

Funded by
the European Union

BALKAN INVESTIGATIVE
REPORTING NETWORK

Reporting
Digital Rights
& Freedoms

Автор: м-р Лилјана Пецова-Илиеска

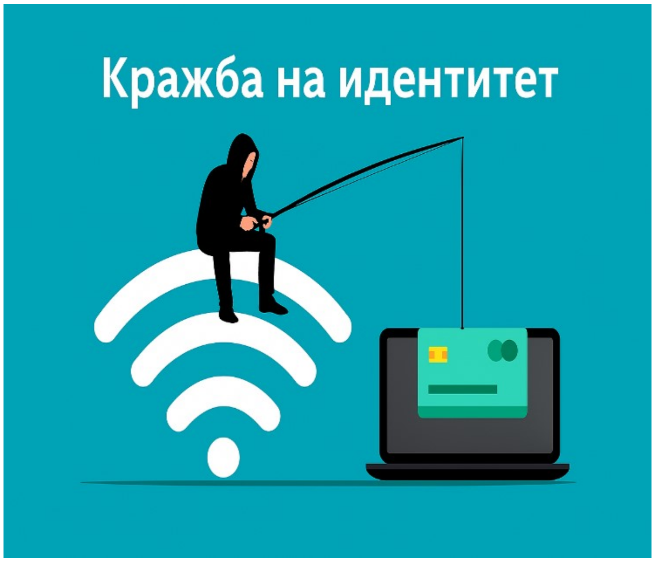
Оваа содржина а е изработена со финансиска поддршка од Европската Унија. Нејзината содржина е единствена одговорност на авторот и не ги одразува нужно ставовите на ЕУ.

Скопје
април, 2025

Кога твоите податоци се злоупотребени – како да се заштитиш и каде да пријавиш?

Во дигиталната ера, нашите лични податоци се сѐ повеќе изложени на ризици. Кражбата на идентитет, злоупотребата на платежни картички и онлајн измамите стануваат сѐ почести. Овој Водич ќе ви помогне да разберете како се случуваат овие злоупотреби, како да се заштитите и каде да ги пријавите.

Секојдневно се соочуваме со различни онлајн закани, како што се злоупотреба на идентитет, сајбер насилство, кражба на финансиски податоци и интернет измами. Овој краток Водич ви нуди практични совети за заштита, контакти за пријавување и организации што можат да ви помогнат за остварување на вашето право на заштита на личните податоци



🔍 1. Што значи „Кражба на идентитет“?

Кражба на идентитет претставува **неовластено** користење на **вашите лични податоци** за финансиска добивка или други злоупотреби.

Често, ова вклучува неовластен **пристап до банкарски сметки**, аплицирање за кредити во ваше име или создавање **лажни профили** со користење на ваши информации.

📌 **Како се случува?**

🔷 Инсталирање на злонамерен софтвер (вирус наречен „тројански коњ“, шпионски софтвер) кој ги краде вашите податоци.

🔷 „Погодување“ на матични броеви користејќи информации за вас од социјалните мрежи.

🔷 Користење на јавно објавени фотографии за создавање лажен профил.

🔷 Лажно спријателување на социјалните мрежи за да се добијат лични информации.

⚠️ **Пример:** Некој со вашите лични податоци отвора банкарска сметка или аплицира за кредит, стекнувајќи се со некаква корист и/или материјална штета.

📢 2. Кривични дела поврзани со злоупотреба на лични податоци

Кога вашите податоци се злоупотребени, тоа често доведува до кривични дела. Најчестите видови се**:**

🔷 **Изработка и употреба на лажна платежна картичка (Член 274-б)**

Крадците добиваат пристап до вашите банкарски податоци и вршат нелегални онлајн купувања.

🔷 **Злоупотреба на лични податоци (Член 149)**

Некој пристапува на вашиот профил и објавува содржина во ваше име, креира лажен профил, нарушувајќи ја вашата приватност и углед, користејќи притоа уцена, измама или ги злоупотребува за стекнување некаква корист.

🔷 **Производство и дистрибуција на детска порнографија (Член 193-а)**

Малолетници се присилуваат да создаваат или споделуваат нелегална содржина преку компјутерска мрежа, што претставува сериозно кривично дело.

🔷 Измама на интернет

Терминот измама на интернет општо се однесува на активности на компјутерски криминал што се одвива преку интернет (е-пошта, социјални мрежи, онлајн услуги), вклучувајќи кривични дела како кражба на идентитет, „фишинг"и други хакерски и измамнички активности со цел да се измамат луѓе, за да се украдат нивните лични податоци и пари.

🛡️ 3. Како да се заштитите од компјутерски криминал?

🔐 Зајакнете ја вашата онлајн безбедност со овие чекори:

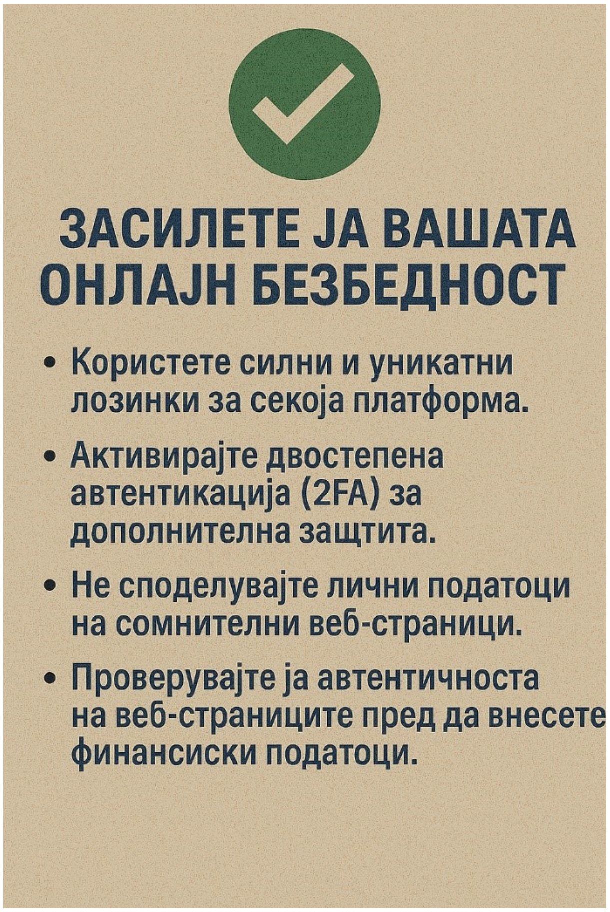
✅ Користете **силни лозинки** и активирајте двостепена автентикација (2FA).

✅ Внимавајте на **лажни веб страници** за интернет купување на електроника, автомобили, станови итн.

✅ Внимавајте на **„Фишинг"** напади каде целта е да ги украдат вашите лични податоци и да ги злоупотребат.

✅ Внимавајте на **лажни наградни игри** и „предобри да бидат вистинити" понуди.

✅ Доколку ве контактира „банка" и бара од вас лични податоци или да пополните нешто сега и веднаш, **повикајте некого од банката за да проверите дали** е вистински контакт. Верификувајте го барањето!



✅ Не споделувајте лични податоци на веб-страници кои се сомнителни и нема многу информации за истата.

✅ Внимавајте што **споделувате на социјалните мрежи**, информации за локација, податоци за вас и вашите блиски и слично.

✅ **Не отворајте** сомнителни линкови и прилози во е-пошта или пораки.

✅ Инсталирајте **антивирус** софтвер и VPN за дополнителна заштита.

✅ Редовно **ажурирајте ги** вашите уреди и софтвери за да избегнете безбедносни пропусти.

✅ Активирајте **SMS известувања** за извршени трансакции. Така ќе знаете за секоја транскација во реално време и ќе можете да спречите понатамошна злоупотреба.

✅ Никогаш не внесувајте финансиски податоци на несигурни веб-страници. Проверете ги фирмите пред онлајн купување.

4. 📢 ВНИМАНИЕ! Злоупотреба на идентитет со помош на АИ! 🤖🛑

Злоупотребата на идентитет со помош на вештачка интелигенција претставува сериозна закана при која напаѓачите користат напредни AI алатки за да креираат **лажни профили**, гласови или фотографии што изгледаат вистински, **со цел да измамат или наштетат** на поединци. Овие злоупотреби може да вклучуваат финансиски измами**, лажно претставување или нарушување на приватноста**.

Потребна е зголемена свесност и заштита на личните податоци за да се спречат ваквите дигитални злоупотреби.

Вештачката интелигенција сè почесто се користи за креирање лажни профили, гласови и фотографии кои изгледаат *вистински*, но се користат за измама, финансиски злоупотреби или нарушување на приватноста.

📌 Внимавајте каде ги оставате онлајн вашите лични податоци

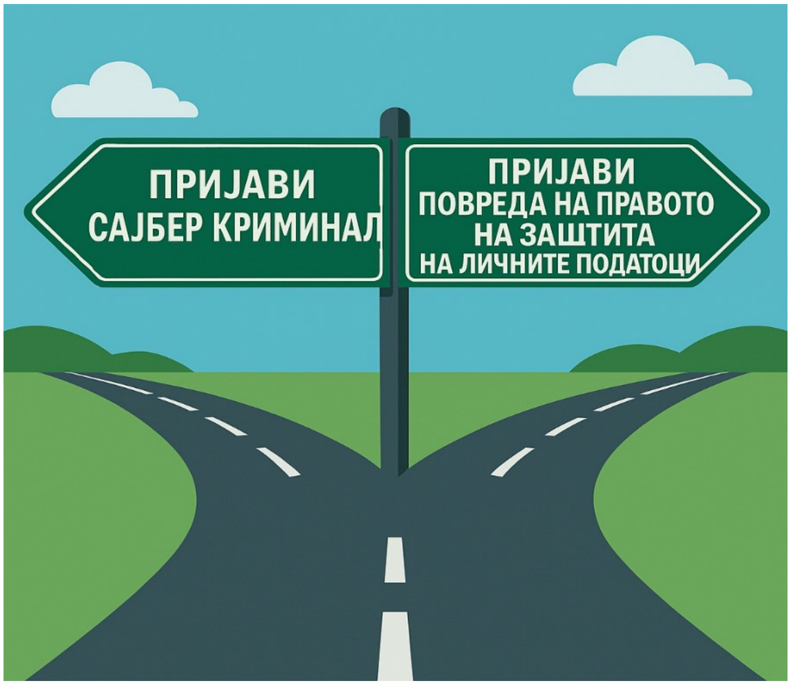
Секојдневно споделувате лични податоци со разни субјекти:

- ✔ Број на кредитна картичка при онлајн купување
- ✔ Податоци за здравствена состојба кај осигурителни компании
- ✔ Информации при аплицирање за кредити, попусти или членски карти
- ✔ Учествување во наградни игри и патувања

🚫 **Избегнувајте ги следниве ризици:**

- Бидете внимателни со **линкови и прилози во е-пошта** – можеби се фишинг обиди.
- Избегнувајте користење на **јавна Wi-Fi** мрежа за внесување на лични податоци.
- Никогаш не споделувајте **сензитивни информации** во јавни коментари или форуми.

📢 5. Каде да пријавите?



Ако сте жртва на сајбер (компјутерски) криминал, не молчете – пријавете го случајот во МВР!

Ако, пак, сметате дека ви е повредено правото на заштита на личните податоци, можете да пријавите во Агенцијата за заштита на личните податоци (АЗЛП).

📨 **Сектор за компјутерски криминал при МВР:** cybercrime@moi.gov.mk

📍 Локални оддели за сајбер криминал има во сите осум сектори на МВР:

- СВР Скопје, СВР Велес, СВР Штип, СВР Струмица, СВР Битола, СВР Охрид, СВР Тетово, СВР Куманово

📞 **Кривични пријави –** Секој граѓанин може да пријави кривично дело во Основното Јавно Обвинителство, писмено, усно, телефонски или по електронски пат:
🖂 Е-пошта: jorm@jorm.org.mk

🚨 **„Црвено копче" – Пријавување преку МВР за:**
🔶 Злоупотреба на деца
🔶 Криминал од омраза
🔶 Трговија со луѓе
📲 Апликација: http://redbutton.mvr.gov.mk/
📞 192

📲 **Дополнителна поддршка од невладини организации:**

📌 Хелсиншки комитет – Пријавување говор на омраза онлајн подразбира било која употреба на технологија на електронски комуникации за ширење антисемитски, расистички, ксенофобични, дискриминаторски, екстремистички или терористички содржини.

Доколку имате потреба од бесплатна правна помош, можете да се јавите на бесплатниот телефонските броеви **02 3119073** и **02 3290 469**. Доколку по разговорот ви е потребна понатамошна помош, можете да преземете и пополните **Барање за бесплатна правна помош**

Повеќе инфо: https://mhc.org.mk/baranje-za-besplatna-pravna-pomosh/

📌ИМПЕТУС – Центар за интернет, развој и добро управување – пријави лажни профили, сајбер насилство, прекршување на право на приватност, злоупотреба на твоите лични податоци и добиј советодавна помош што понатаму; contact@impetus.mk

📌 Прва детска амбасада „Мегаши" – СОС телефон за деца и млади 📞 0800 1 2222

Ало Бушавко - Бесплатно психосоцијално и правно советување, поддршка и насочување, упатување до државна институција која е надлежна за конкретниот проблем https://alobushavko.mk/mk/

📌 Центар за заштита на жртви на дигитално родово-базирано насилство
📧 coordinator@glasprotivnasilstvo.org.mk

---

6. 🛡 Вашите лични податоци – Ваше право, Ваша заштита!

Доколку сметате дека ви е повредено правото на заштита на личните податоци, можете да поднесете Барање за утврдување на прекршување на одредбите од Законот за заштита на личните податоци **до Агенцијата за заштита на личните податоци (АЗЛП)**.

За таа цел потребно е во Барањето да ги наведете вашите лични податоци и податоците за контролорот кој сметате дека го повредил вашето право на заштита на лични податоци.

Доколку не се остварени овие ваши права, пријавете во 📞 **Агенција за заштита на лични податоци info@privacy.mk;**

6.1. 📢 Ваши права според Законот за заштита на личните податоци

✓ Право на пристап до лични податоци

- Може да побарате **потврда** од институција или организација дали вашите податоци се обработуваат
- Имате право на **копија од вашите податоци** (пр. договор од банка, медицинско досие)

✓ Право на информираност

- Имате право да бидете информирани за обработката на вашите лични податоци од страна на оние кои ги собираат и чуваат

✓ Право на исправка на неточни податоци

- Доколку личните податоци се **неажурни или неточни**, имате право да барате исправка во рок од **15 дена**

  Пример: Ако болница има зачувано неточна е-мејл адреса и не ви пратила документи, може да барате да изврши корекција

✓ Право на ограничување на обработката на вашите лични податоци

- Во одредени околности имате право да го ограничите начинот на кој контролорот ги користи вашите лични податоци

  Пример: Личните податоци се веројатно неточни, обработката е незаконска, не постои валидна цел на обработката, сте се спротивставиле на обработката што се заснова на легитимен интерес на контролорот, итн.

✓ Право да поднесете Барање за утврдување прекршување на правото на заштита на личните податоци

- Доколку се сомневате дека некое физичко/правно лице врши незаконска обработка на вашите лични податоци

  Пример: Некоја организација/институција собира лични податоци без ваша согласност, без законски основ, или собира преголем обем на лични податоци, или пак нема известување за тоа кој врши видео надзор, или врши видео надзор во недозволени простории (гардероби, соблекувални, санитарни јазли, итн.)

🔐 **Засилете ја вашата онлајн безбедност:**

✅ Проверете кои лични податоци ги споделувате и за која цел се потребни

✅ Барајте јасно објаснување за **целта на обработката заради која ги собираат вашите лични податоци**

✅ Чувајте ги вашите податоци безбедни и не ги споделувајте на несигурни платформи

✅Не споделувајте **поголем обем на податоци отколку што е потребно** за постигнување на целта заради која се собираат

✅Водете сметка **каде сте дале согласност** за обработка на вашите податоци

7. Видови на онлајн злоупотреби и како да се заштитите

🔷 **Сајбер насилство кај младите:**

Сајбер насилство се случува кога децата и тинејџерите користејќи Интернет преку своите технолошки уреди (компјутери, телефони, таблети и сл.) објавуваат навредливи информации во вид на текст, слики или други видови содржини со намера да повредат или да посрамотат друга личност.

💻**Како да се заштитите:**

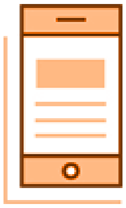
- Користете го делот на поставки за **ограничување на контактот** со насилници.
- Не реагирајте на навредливи пораки – **пријавете ги**!
- Обезбедето го материјалот, не го бришете, **снимете го како доказ**

- Може да пријавете во училиште, на платформите и во полиција доколку се работи за закани.

🛑 **Онлајн платформи за пријавување:**

- Facebook: www.facebook.com/help
- Instagram: www.instagram.com/help
- TikTok: www.tiktok.com/safety
- Google: www.support.google.com

Центар за побезбеден интернет на Македонија www.Mksafenet.mk



mksafenet@mdt.gov.mk

Tel: +389 2 3200 870

📍 **Како да го заштитите вашиот дигитален идентитет?**

🚨 Заштитете се – не дозволувајте вашите податоци да станат оружје во рацете на криминалците! 🔐 **Заштитете ги вашите лични податоци!**

Бидете информирани, споделете го овој водич и помогнете во борбата против кибер-криминалот.