# Водич:

# ОСНОВИ НА ДИГИТАЛНАТА БЕЗБЕДНОСТ

# ВОВЕД

## ЗОШТО СЕ ВАЖНИ ПРИВАТНОСТА И БЕЗБЕДНОСТА НА ИНТЕРНЕТ?

## КОНЦЕПТОТ НА ПРИВАТНОСТ Е РЕЛАТИВНО ЈАСЕН ВО НЕДИГИТАЛНОТО ОПКРУЖУВАЊЕ. СЕКОЈ ЧОВЕК Е СВЕСЕН ЗА СВОЈАТА ПРИВАТНОСТ И СЕ ТРУДИ ДА ЈА ЗАШТИТА ДО СТЕПЕНОТ ДО КОЈ МУ ОДГОВАРА.

Ситуацијата е малку поинаква во дигиталното опкружување. Луѓето не се свесни кога се сами, а кога не додека се на интернет, па со самото тоа често не знаат дали се знае што правеле на интернет и кој може да дознае. Од друга страна, дигиталната безбедност е доста поширок концепт кој подразбира повеќе од само приватност. Попрецизно, дигиталниот систем кој не е безбеден не може да се смета за приватен, додека самото тоа што системот има обезбедена приватност не значи дека е потполно безбеден.

Постои цела низа фактори кои влијаат на тоа дали системот ќе биде безбеден или не. Пред сè, тука се технолошките фактори, односно дали е системот технолошки компромитиран или ранлив и кое е нивото на безбедност кое самите уреди и инсталирани програми го даваат. Потоа, постојат и нетехнолошки фактори, односно одредени навики на корисниците, кои се исто така многу важни. Општо правило е дека безбедноста не е вродена карактеристика на дигиталните системи, и за системот да биде бебеден, мора да се преземат одредени активности.

Секој корисник во текот на своите активности на интернет остава траги, „сенка“ која го следи додека се движи низ сајбер просторот. Во дигиталното опкружување, слично како и во недигиталното, овие сенки му даваат одредени карактеристики на сопственикот на сенката. Со анализа на сенката може да се дојде до одредени информации кои се од важност за напаѓачите чија цел е да влезат во одреден систем. Предноста на дигиталната средина е тоа што корисниците донекаде може да го контролираат обликот на нивната сенка доколку поведат сметка за одредени работи, што е и тема на овој прирачник.

## КЛУЧНИ ТЕРМИНИ

**ИНТЕРНЕТ ПРИВАТНОСТ** е вид лична приватност кој се однесува на чување, репродукција, споделување со трети лица и прикажување на информации кои припаѓаат на одредено лице, преку интернет.

**ИНТЕРНЕТ БЕЗБЕДНОСТ** е заштита на онлајн сметка, компјутер, датотека и систем од напад на надворешни субјекти.

**САЈБЕР ПРОСТОР** е апстрактна средина во која се одвива комуникацијата помеѓу компјутерски мрежи.

**ИНФОРМАЦИСКИ СИСТЕМ (ИС)** е систем составен од луѓе и компјутери во кој се обработуваат и толкуваат одредени информации.

**ОПЕРАТИВЕН СИСТЕМ (ОС)** е програмски систем кој им овозможува на корисниците на компјутери да работат, односно кој ги пренесува командите до на уредот кој извршува одредени операции.

**ХАКЕР** е лице кое пронаоѓа, искористува недостатоци и го прилагодува ИС и компјутерската мрежа на своите потреби.

**КРАКЕР(CRACKER)** е хакер кој пронаоѓа и искористува безбедносни недостатоци во ИС и компјутерските мрежи поради малициозност и лична корист (оттука, не се сите хакери лоши).

**КЛИЕНТ** или корисник во техничка смисла е компјутер кој се користи за пристап до интернет.

**СЕРВЕР** е еден вид компјутер кој има значително појака спецификација од клиентот и на кој се чуваат (хостираат) различни содржини, веб страници, датотеки (фајлови), е-мејл пораки, итн.

**WWW (WORLD WIDE WEB)** е ИС на меѓусебно поврзани веб сајтови кои се достапни преку интернет.

**ПРЕГЛЕДУВАЧ НА МРЕЖА (WEB BROWSER)** е програм чија намене е прегледување на содржините на **WWW** (на пр. Firefox, Chrome, Internet Explorer, Opera, Safari, итн.).

**ПРЕБАРУВАЧ НА МРЕЖА (SEARCH ENGINE)** е мрежен сервис кој е дел од WWW и кој овозожува полесно пребарување по WWW (на пр. Google, Bing, DuckDuckGo, итн.).

**URL (UNIFORM RESOURCE LOCATOR)** е референца на IP адреса на веб сајт. Стандардните URL имаат облик http://www.example.com.

**IP (INTERNET PROTOCOL)** адреса е основна ќелија на интернет адресирањето. Секој уред кој е поврзан на интернет мора да има барем една јавна IP адреса. Постојат две верзии на IP адреси кои се користат:

Пример на IPv4 адреса:
98.139.180.149

Пример на IPv6 адреса:
FE80:0000:0000:0000:0202:B3FF:-FE1E:8329

**МЕТАПОДАТОЦИ (METADATA)** се податоци кои автоматски се генерираат од страна на програмот и уредите кои се користат за поврзување на интернет. Метаподатоците подразбираат локација, датум, време, вид на уред кој се користи, итн.

**MALWARE (МАЛИЦИОЗЕН СОФТВЕР)** е општ термин за софтвер кој се користи за попречување на работата на компјутерот, собирање чувствителни информации или одбивање пристап до заштитен ИС.

**ОТВОРЕН КОД (OPEN SOURCE)** е вид на софтвер чиј изворен код (текстуален фајл кој го одредува функционирањето на софтверот) е јавно достапен и секој корисник има можност да врши ревизија и да го прилагодува на своите потреби. Софтверот со отворен код е во најголем број случаи бесплатен.

**CLOUD ТЕХНОЛОГИЈА (CLOUD COMPUTING)** е една од најновите интернет технологии која се темели на користење ресурси (проток на податоци, простор за складирање, работна меморија, итн.) на далечина и нивно споделување помеѓу различни апликации и корисници. Cloud може да биде приватен, јавен или хибриден.

# КАКО НАВИКИТЕ НА КОРИСНИКОТ ВЛИЈААТ НА НЕГОВАТА БЕЗБЕДНОСТ

## ЕНКРИПЦИЈА

### ЕНКРИПЦИЈАТА Е КРИПТОГРАФСКИ КОНЦЕПТ НА КОДИРАЊЕ НА ПОРАКИ ИЛИ ИНФОРМАЦИИ СО ШТО СЕ ОБЕЗБЕДУВА ДЕКА ЕДИНСТВЕНО ЛИЦАТА КОИ ИМААТ НАЧИН ДА ГИ ДЕКОДИРААТ (ДЕКРИПТИРААТ) МОЖАТ ДА ГИ ПРОЧИТААТ.

Енкрипцијата како концепт не е нова, постоела уште во стар Рим. Тогаш се користени примитивни алгоритми кои главно се однесуваат на креирање на нови комбинации на букви со користење на постоечките, со тоа што редоследот на буквите се модифицира на одреден начин.

Современата дигитална енкрипција произлегува од овој концепт, но толку е развиена што се издвоила како потполно нов и поинаков правец во криптографијата. Изворно, најголемиот дел од информациските системи не се енкриптирани, што значи дека енкрипцијата мора да се остави за да постои.

Голем број корисници кои немаат познавања од дигиталната безбедност ја занемаруваат енкрипцијата и со тоа се изложуваат на ризик самите себе, луѓето со кои комуницираат и организацијата во која работат. Енкрипцијата се имплементира на повеќе нивоа, т.е. енкрипција на врска и енкрипција на диск.

| | |
|---|---|
| LOREM IPSUM | оригинален текст |
| --- | |
| ERSPZHEBBZP73Z7YMBFFSA== | енкриптирано |

## БЕЗБЕДНО ПРЕБАРУВАЊЕ

### ЗА ПРЕБАРУВАЊЕ НА ИНТЕРНЕТ СЕ КОРИСТАТ ПРОГРАМИ КОИ СЕ ВИКААТ ИНТЕРНЕТ ПРЕГЛЕДУВАЧИ. ТЕХНИЧКОТО ПРЕБАРУВАЊЕ ПРЕТСТАВУВА ПРИСТАП ДО СОДРЖИНАТА НА ИНТЕРНЕТ СО ПОМОШ НА HTTP ИНТЕРНЕТ ПРОТОКОЛ

Постојат различни комерцијални решенија и сите на некој начин извршуваат иста функција, но за пребарувањето да биде безбедно, потребно е да се постават дополнителни параметри и да се инталираат дополнителни програми (plugins).

Основното ниво на безбедност подразбира користење на SSL или TLS. Овие технологии ја енкриптираат комуникацијата помеѓу клиентот и серверот и со тоа ефикасно штитат од MitM напади. На овој начин се овозможува безбеден пренос на чувствителни податоци преку интернет, како што се кориснички имиња, шифри, доверливи лични податоци, податоци за платежни картички, броеви на банкарски сметки, итн. SSL се инсталира на серверот, што значи дека не постои како опција за секој веб сајт. Веб сајтовите кои користат SSL во URL адресата содржат „https“ наместо стандардниот „http“.

При пребарување на интернет, покрај содржината која се праќа и презема од серверот по желба на корисникот, се разменуваат и метаподатоци. Со логично мапирање на метаподатоците и нивна анализа може да се отријат многу значајни податоци за корисникот, на пр. со кого, каде и од која географска локација комуницирал корисникот, кои содржини ги пребарувал, итн. Овој своевиден безбедносен „недостаток“ се користи за целно рекламирање, па затоа корисниците често при пребарувањето добиваат реклами кои се тематски слични со нивните претходни пребарувања. Притоа, рекламите кои се вчитуваат претставуваат содржини на трети страни и тие исто така собираат метаподатоци за корисникот. Постојат додатоци за блокирање на реклами кои се додаваат на прегледувачите и ја блокираат целата содржина на трети страни.

Сепак, конвенционалните прегледувачи не го решаваат до крај „проблемот“ со метаподатоците. Во моментот се актуелни три технологии кои се користат за да им се овозможи на корисниците да сокријат дел од метаподатоците кои се однесуваат на геолокацијата и видот на уредот кој се користи. Со тоа, овие хардверско-софтверско решенија нудат анонимност на интернет. Овие технологии се VPN, Proxy и TOR. Искуството покажало дека најконзистентно решение е употребата на TOR мрежа.

TOR мрежата е хибридно хардверско-софтверско решение кое им овозможува на корисниците анонимно поврзување на интернет. Оваа мрежа има карактеристики на VPN и Proxy, во смисла дека може да се користи и само во прегледувачот, но постои и можност сообраќајот да се пренасочи на TOR мрежа со посебна конфигурација на компјутерот.

## TOOL BOX:

Со користење на приклучокот (plugin) „**HTTPS EVERYWHERE“** прегледувачот автоматски секогаш вчитува безбедна верзија на веб страницата. Приклучокот е достапен на следниот линк: https://www.eff.org/https-everywhere

**PLUGIN ADBLOCK PLUS** е додаток за интернет прегледувачите кој блокира содржини на трети страни. Приклучокот е достапен на следниот линк: https://adblockplus.org/

**DUCKDUCKGO** е пребарувач кој собира многу малку додатоци за клиентите. Пребарувачот е достапен на следниот линк: https://duckduckgo.com/

Постои посебна верзија на Mozilla Firefox прегледувачот која е поставена така да користи TOR мрежа за прегледување на содржини на интернет. Прегледувачот може да се преземе од следниот линк: https://www.torproject.org/dowload/download-easy.html.en

## INFO BOX:

**HTTP (HYPERTEXT TRANSFER PROTOCOL)** е протокол низ кој се одвива сообраќај кој се однесува на пребарување на World Wide Web (WWW). Со овој протокол е регулирана комуникацијата помеѓу корисникот и серверот на кој се наоѓа содржината.

**SSL (SECURITY SOCKET LAYER)** е посебен слој на заштита на HTTP интернет протоколот.

**TLS (TRANSPORT LAYER SECURITY)** е унапредена и подобра верзија на SSL.

**MITM (MAN IN THE MIDDLE)** напад е вид технички напад во кој клиентот и серверот не се нужно компромитирани, но врската помеѓу нив е, при што напаѓачот ги користи недостатоците на врската за да добие пристап до комуникацијата со цел да ја компромитира.

**BACKDOOR (СПОРЕДЕН ВЛЕЗ)** во ИС е механизам на заобиколување на стандардната форма на автентикација и добивање неовластен пристап до заштитениот ИС, при што специфично е тоа што натрапникот останува незабележан.

**СОДРЖИНА НА ТРЕТИ СТРАНИ (THIRD PARTY CONTENT)** е содржина која корисникот не ја барал директно, но му е прикажана поради тоа што сопственикот на бараната содржина отстапил дел од својот сајт на трети страни (реклами на Google, коментари на Facebook, итн.).

**VPN (VIRTUAL PRIVATE NETWORK)** е интернет услуга која овозможува поврзување на приватна мрежа преку јавна мрежа како што е интернетот. VPN им овозможува на корисниците безбедно да примаат и испраќаат доверливи податоци преку интернет.

**PROXY** е сервис кој овозможува поврзување на сервер на далечина преку кој потоа се пристапува на интернет. Суштинската разлика помеѓу Proxy и VPN е во тоа што низ Proxy минува само сообраќајот кој се однесува на прегледувачот, додека VPN го покрива целиот сообраќај кој произлегува од тој компјутер (вклучувајќи Skype, е-мејл клиенти, итн.).

(Забелешка: Не се препорачува користење на TOR мрежа за симнување големи датотеки поради тоа што мрежата се оптоварува и тоа влијае на нејзината брзина. Исто така, во случај програмот кој се користи да не е сигурен, TOR не може да гарантира анонимност).

## АЖУРИРАЊЕ НА СОФТВЕР

## СЕКОЈДНЕВНО СЕ РАЗВИВААТ НОВИ ВИДОВИ НА ТЕХНОЛОШКИ НАПАДИ И МАЛИЦИОЗНИ СОФТВЕРИ, ПОРАДИ ШТО ANTI-MALWARE АПЛИКАЦИИТЕ СЕКОЈДНЕВНО ГИ АЖУРИРААТ СВОИТЕ ЛИСТИ СО ШТО ОВОЗМОЖУВААТ ПРОГРАМОТ ДА ГИ ДЕТЕКТИРА НАЈНОВИТЕ ВИДОВИ НА МАЛИЦИОЗЕН СОФТВЕР

Ниту еден софтверски или хардверски систем не е потполно совршен, односно секој систем има недостатоци кои може да се искористат за да се оствари неовластен пристап во системот. Кракерите константно работат на пронаоѓање и истражување на овие недостатоци, со чија експлоатација би се овозможил упад во системот.

Затоа е важно редовно да се ажурираат сите видови на апликации во рамките на системот, почнувајќи од оперативниот систем, преку anti-malware апликациите до апликациите кои корисникот ги користи секојдневно. Важно е да се напомене дека се препорачува единствено инсталирање на апликации од проверени и сигурни производители поради тоа што многу кракери лажно го претставуваат својот малициозен софтвер како ажурирана верзија на програмот. За корисниците полесно да препознаат кои апликации не се ажурирани, и за да бидат сигурни дека ќе ги преземат вистинските ажурирани верзии на програмот, може да користат различни апликации. Во секој случај се препорачува да се користат апликации кои само го известуваат корисникот дека треба да ажурира одреден софтвер, а да не се дозволува автоматско преземање на ажурирани верзии на програмот.

## TOOL BOX:

Корисниците на Windows и iOS може да користат FileHippo App Manager кој е достапен на следниот линк: http://www.filehipp.com/download_app_manager/

Корисниците на Linux може да користат Synaptic manager за ажурирања, кој е достапен на следниот линк: http://www.nongnu.org/synaptic/

## МАЛИЦИОЗЕН СОФТВЕР (MALWARE)

### MALWARE Е НАЈЕДНОСТАВНО КАЖАНО СОФТВЕР КОЈ ГО КРЕИРААТ КРАКЕРИТЕ ЗА НАМЕРНО ДА ПРИЧИНАТ ШТЕТА НА ОДРЕДЕН ИС

Најпрепознатлив вид на malware се компјутерските вируси, но постојат и други видови како што се тројанци, adware, spyware и црви (“worms”). Секој вид на malware има свој начин на функционирање, па оттука штетата која секој од нив ја нанесува е од различен степен.

И покрај тоа што постојат одредени дефиниции и поделби на malware-от, категориите не можат дефинитивно да се разграничат, па често се случува еден malware да врши активности кои се карактеристични за други видови malware-и. Malware-от може да врши различни операции, почнувајќи од пренасочување на лажни веб сајтови до дестабилизирање на целиот систем. Посебен вид malware-и се key logger-ите, кои го забележуваат секој внес преку тастатурата и ги праќаат записите на трети лица. Исто така, постои и вид на malware кој има можност да праќа и по неколку илјади е-мејл пораки од заразениот компјутер.

Malware-от се дистрибуира на различни начини. Најчесто корисниците сами го преземаат malware-от со некоја своја активност, но бидејќи инсталираните програми комуницираат на интернет на различни начини поради своите активности, а секој од нив има по некој недостаток кој напаѓачот може да го искористи, во најголемиот број случаи овие недостатоци се решаваат, па затоа е важно програмите да се ажурираат.

Не е секогаш едноставно да се препознае malware; често се случува корисникот на почетокот воопшто да не е свесен дека неговиот компјутер/систем е заразен. Понекогаш

активноста на malware-от може да се примети поради спонтаното влошување на перформансите на системот. Просечниот корисник секако не може сам во целост да го отстрани malware-от без употреба на одреден anti-malware програм. Овие програми вршат мониторинг на системот, ги скенираат фајловите кои ги преземаат од интернет и е-мејл пораките, и доколку најдат malware го стават во карантин или го бришат, во зависност од поставките.

Сепак, не е доволно само да се инсталира одреден програм кој ќе се бори против malware-от, битно е и корисниците да не инстаираат аликации кои не се проверени и сигурни, да не кликаат на сомнителни линкови, да не отвораат сомнителни е-мејл пораки и да не посетуваат несигурни веб сајтови.

## TOOL BOX:

Avira е еден од најдобрите бесплатни anti-malware програми. Програмот е достапен на следниот линк: http://www.avira.com/en/avira-free-antivirus

## INFO BOX:

**ВИРУС** е вид на malware кој сам се размножува во постоечките фајлови, програми, па дури и во самиот оперативен систем. Најчесто ја модифицира содржината на фајловите или ги брише, што може да доведе до пад на системот доколку вирусот избрише некој системски фајл.

**ТРОЈАНЕЦ (TROJAN)** е вид на malware кој кога ќе се инсталира во ИС врши операции кои се дефинирани од страна на напаѓачот, а тоа е најчесто бришење или модифицирање на податоци, но често може да дојде и до оштетување на целиот систем. Најчесто личат на нормални и корисни инсталациони датотеки, па оттука го добиле и името.

**ADWARE (ADVERTISING SOFTWARE)** кој кога ќе зарази ИС, автоматски прикажува реклами при пребарување на интернет што му носи приход на огласувачот кој го креирал. (Компаниите им плаќаат на огласувачите според бројот на прикажувања на одредени реклами).

**SPYWARE (SPYING SOFTWARE)** е вид на malware кој собира податоци од заразен ИС и истите ги проследува до трети лица (најчесто до инстанцата која го креирала). Со овој malware, неовластени лица може да дојдат до шифри, лични податоци, коресподенција, итн.

**ЦРВ (WORM)** е вид на malware кој сам се размножува. Тоа значи дека доколку е заразен еден компјутер во рамките на системот, голема е веројатноста дека сите компјутери поврзани со него ќе бидат заразени по одредено време. Најчесто нанесува штета на мрежата и системот со тоа што го успорува протокот на податоци во мрежата. Црвите се самостоен malware, т.е. за разлика од вирусите, тие не мора да бидат поврзани за постоечки програм за да се пренесуваат.

**ШИФРИ**

## КАКО ДА СЕ КРЕИРААТ БЕЗБЕДНИ И КОМПЛЕКСНИ ШИФРИ КОИ ЛЕСНО СЕ ПАМЕТАТ

## ШИФРИТЕ СЕ НАЈРАСПРОСТРАНЕТИОТ МЕТОД НА АВТЕНТИКАЦИЈА И ЗАТОА Е ВАЖНО ДА БИДАТ ШТО Е МОЖНО ПОКОМПЛЕКСНИ

Основно правило при креирањето шифри е тие да не содржат фактографски податоци за корисникот и цели зборови на природниот јазик, бидејќи така можат полесно да се откријат со методата на обиди и грешки. Постојат генератори на комплексни, случајни шифри, но тие шифри многу тешко се паметат. Добро решение е креирање на наизглед случајни шифри кои тешко можат да се откријат но лесно се паметат. На пример, се составува одредена реченица и се земаат првите букви од секој збор и на тој начин се креира шифрата. Исто така, битно е да се конфигурираат и добри безбедносни прашања за ресетирање на шифрата. Треба да се води сметка одговорот на безбедносните прашања да не е општопознат и да биде наизглед случаен.

Покрај комплексните шифри, добра пракса е и да се активира автентикација на две нивоа секаде каде што е тоа можно. Автентикацијата на две нивоа (two step authentication) е начин на автентикација која покрај внесот на шифри бара и дополнителен чекор, а тоа е најчесто внес на код кој се добива преку СМС порака.

Квалитетот на шифрата и останатите механизми на заштита е неминовен на патот кон безбеден систем, но подеднакво важен е и начинот на чување. Никако не се препорачува шифрите да се запишуваат во тетратки, на ливчиња или да се чуваат во телефон, како што е често пракса. Безбеден начин на чување се софтверски решенија кои чуваат шифри и бази на податоци во енкриптиран формат, така што во случај на напад врз компјутерот на кој се чуваат шифрите, тие нема да го загубат својот интегритет.

## TOOL BOX:

Автентикација на две нивоа може да се конфигурира за следните платформи:

**GOOGLE:** http://www.google.com/landing/2step/

**FACEBOOK** (Login Approvals):
https://www.facebook.com/settings?tab=security&section=approvals

**TWITTER:** https://support.twitter.com/articles/20170388-using-login-verification

**DROPBOX:** https://www.dropbox.com/en/help/363

**LINKEDIN:** https://blog.lonkedin.com/2013/05/31/protecting-your-linkedin-account-with-two-step-verification/

Добар програм за чување шифри е **KEEPASS**, кој е достапен на следниот линк:
http://keepass.info@download.html

## ЕНКРИПЦИЈА НА ДИСКОВИ

## ЕНКРИПЦИЈА НА ДИСКОВИ

## ЕНКРИПЦИЈАТА Е ГЕНЕРАЛЕН КОНЦЕПТ КОЈ ИМА РАЗЛИЧНА ИМПЛЕМЕНТАЦИЈА, А ЕДНА ОД НИВ Е ЕНКРИПЦИЈА НА ДИСКОВИ ИЛИ ЛОКАЛНА ЕНКРИПЦИЈА

Технолошки постојат различни видови на дискови, но две општи групи се релевантни кога е во прашање енкрипција: тоа се локални дискови и преносни уреди.

Енкрипција на диск подразбира создавање на слој на заштита кој им неовозможува на неовластени лица да пристапат до содржината која се наоѓа на дискот. За да се пристапи на содржината, потребен е внес на шифра, а понекогаш и дополнителни параметри како што се автентикација на две нивоа, дигитален сертификат или биометриски податоци.

Секој имплементација на енкрипција е различна бидејќи потребите се разликуваат во зависност од тоа како се користат податоците кои се енкриптираат, т.е. дали се работи за пренос или складирање на податоци. SSL е класичен пример на енкрипција на пренос на податоци, додека енкрипција на локален диск на компјутер е пример на енкрипција на податоци кои се чуваат на тој диск.

Во поединечни случаи, се јавува потреба од хибридна енкрипција, на пример кај USB флеш меморијата, во една трансакција се јавува потреба да се енкриптира пренос од некој диск до флеш меморијата и тогаш енкрипцијата се врши на самата меморија. Cloud технологијата од друга страна исто така условува посебни механизми на енкрипција бидејќи самата технологија е хибрид на пренос и складирање.

## TOOL BOX:

**VERACRYPT** е модифицирана верзија на порано популарниот TrueCrypt чиј развој е прекинат и со самото тоа тој престанал да биде потполно безбеден. VeraCrypt е програм кој локално енкриптира податоци и достапен е на следниот линк:
https://veracrypt.codeplex.com/

**BOXCRYPTOR** е софтверско решение кое воглавно се користи за енкрипција на датотеки и фајлови на cloud. Достапен е на следниот линк:
https://www.boxcryptor.com/en/download

## INFO BOX:

**ДИГИТАЛЕН СЕРТИФИКАТ (DIGITAL CERTIFICATE)** е посебен сертификат кој служи за докажување на идентитетот во текот на различни видови на комуникација во сајбер просторот и го издаваат организации кои имаат овластувања за издавање на дигитални сертификати.

**БИОМЕТРИСКИ ПОДАТОЦИ** се биолошки карактеристики кои може да се дигитализираат, како на пример отпечаток од прст и дланка, скен на зеница и ретина, итн.

## ЕНКРИПЦИЈА НА КОМУНИКАЦИЈА

## Е-МЕЈЛ

## И ПОКРАЈ РАЗВОЈОТ НА ПОСОВРЕМЕНИ НАЧИНИ НА КОМУНИКАЦИЈА, Е-МЕЈЛОТ ОСТАНА КОНВЕНЦИОНАЛНО И НАЈЧЕСТО КОРИСТЕНО РЕШЕНИЕ ВО ОФИЦИЈАЛНАТА КОМУНИКАЦИЈА ПРЕКУ ИНТЕРНЕТ

Со тоа, и понатаму голем број важни и чувствителни информации се пренесуваат преку е-мејл. Од друга страна, самата технологија која стои за е-мејлот не е потполно безбедна, т.е. има многу безбедносни недостатоци, па корисникот нема контрола кој сè може да им пристапи на метаподатоците и содржината на неговата е-мејл комуникација, особено кога се користат јавни е-мејл сервиси како Gmail, Live, Yahoo Mail, и сл.

Делумно решение за проблемот со метаподатоците е секако користење на TOR мрежа, како и блокирање на активната содржина како што се слики и различни други потенцијално ризични елементи во е-мејл пораките. Во секој случај, содржината на овој начин не е енкриптирана. Еден од најдобрите начини за енкриптирање на содржината на е-мејл пораките е PGP. Недостатокот на PGP е можеби во неговата имплементација која не е во целост водена од корисничкото искуство. Исто така, потребно е двете страни во комуникацијата да користат PGP за тој да може да се воспостави како механизам на заштитена комуникација.

## TOOL BOX:

**THUNDERBIRD** е клиент за е-мејл кој поддржува датотеки за поедноставна примена на PGP енкрипција. Програмот е достапен на следниот линк: https://www.mozilla.org/en-US/thunderbird/

**ENIGMAIL** е додаток за Thunderbird кој овозможува поедноставна примена на PGP енкрипцијата. Додатокот е достапен на следниот линк: https://addons.mozilla.org/en-us/thunderbird/addon/enigmail/

## INFO BOX:

**PGP (Pretty Good Privacy)** е метод на енкрипција и декрипција кој се користи за end-to-end заштита на содржина.

**END-TO-END ЕНКРИПЦИЈА (E2EE)** е парадигма во криптографската наука која означува непрекината енкрипција на содржината од изворот до крајот на комуникацијата.

## CHAT

### ПОКРАЈ Е-МЕЈЛ КОМУНИКАЦИЈАТА, ГОЛЕМ ДЕЛ КОРИСНИЦИ НА ИНТЕРНЕТ КОРИСТАТ И РАЗЛИЧНИ CHAT УСЛУГИ

Овие услуги главно се користат за неформална и лична комуникација, па се често предмет на преписка на доверливи информации за корисниците кои не би требало да бидат достапни на трети страни. Постојат апликации кои овозможуваат енкриптирана комуникација преку chat услуги.

СМС комуникацијата е слична на chat комуникацијата, со единствена разлика што во chat комуникацијата се користи интернет како медиум за пренос на податоци, додека кај СМС пораките се користи стандардната мрежа на мобилните телефони (GSM, 2G, 3G, 4G, итн.). Поради тоа, механизмот за енкрипција на СМС пораки е малку поразличен од енкрипцијата на chat пораките. Во обата случаи се работи за E2EE, така што е важно да се нагласи дека двете страни мора да користат енкрипција за системот да биде безбеден. Постојат посебни апликации за сите ОС на паметни телефони кои овозможуваат енкрипција на комуникацијата преку СМС порака.

## TOOL BOX:

**PIDGIN** е програм кој нуди можност за енкрипција на chat комуникацијата. Достапен е на следниот линк: https://www.pidgin.im/

**TELEGRAM** апликација за безбеден chat за паметни телефони и компјутери. Апликацијата е достапна на следниот линк: https://telegram.org/apps

**TEXTSECURE** е апликација за енкриптирање на СМС комуникација за Android паметни телефони. Апликацијата е достапна на следниот линк: https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms&hl=en

**SIGNAL** е апликација за енкриптирани текстуални, сликовни и видео пораки за iPhone. Апликацијата е достапна на следниот линк: https://itunes.apple.com/us/app/signal-private-messenger/id874139669?mt=8

## ДОБРИ И ЛОШИ ПРАКТИКИ НА ИНТЕРНЕТ БЕЗБЕДНОСТ

## ДОБРИ ПРАКТИКИ

1. Бидете многу внимателни со вашите лични податоци.
2. Почитувајте ја приватноста на другите на интернет.

3. Преземајте само фајлови и инсталирајте само програми од познати извори во кои имате доверба.
4. Ажурирајте ги сите програми и ОС за да го намалите ризикот од напади.
5. Креирајте комплексни шифри кои лесно се паметат а тешко се пробиваат.
6. Активирајте автентикација на повеќе нивоа секаде каде што е можно.
7. Користете anti-malware програм.
8. Енкриптирајте сè што може да се енкриптира.
9. Доколку користите јавен компјутер, обидете се да не оставите никакви траги зад вас.
10. Доколку вашата USB меморија била во јавен или незаштитен компјутер, секогаш скенирајте ја со anti-malware програм пред да ја користите.
11. Се препорачува преносните уреди да се скенираат секогаш кога ќе се поврзат на комјутер.
12. Внимавајте на ризиците кои ги носи секоја ваша постапка на интернет. Приватноста не значи помала одговорност.
13. Макар и набрзина прочитајте ги условите за користење пред да кликнете „Прифаќам“.

## ЛОШИ ПРАКТИКИ

1. Никогаш не праќајте шифри, лични податоци или финансиски информации по електронска пошта.
2. Немојте да пристапувате на мрежи за кои немате овласување, дури и да сте дошле до одредени login детали (корисничко име, шифра). Тоа не значи дека сте добиле овластување.
3. Немојте да инсталирате сомнителни додатоци и ажурирани верзии на програмата.
4. Немојте да кликате на сомнителни линкови кои сте ги добиле по пат на електронска пошта, колку и интересно да делува пораката.
5. Избегнувајте користење на јавни и незаштитени компјутери.
6. Избегнувајте користење на туѓи мобилни телефони.
7. Не ги запишувате вашите шифри на ливчиња. Навистина немојте!
8. Не ставајте имиња или датуми на раѓање на вам блиски луѓе како шифри.
9. Не ги оставајте вашите уреди без надзор и отклучени.
10. Не занемарувајте сомнителни активности. Понекогаш е подобро да се биде параноичен.
11. Не користете пиратски софтвер. Доколку не сакате да плаќате за софтвер, побарајте варијанта со отворен код.
12. Немојте да живеете во вашата зона на комфор. Понекогаш вреди да се вложи малку труд и напор и да се научат основните работи за тоа како да се биде безбеден на интернет.

# ИНТЕРЕСНИ РЕСУРСИ

**MYSHADOW:**
https://myshadow.org/

Интересна интерактивна платформа која се фокусира на концептот на приватност на интернет. Содржи доста едукативен материјал, но и интерактивни квизови со помош на кои корисниците може да одредат колку се ранливи на интернет.

**WOLFRAMALPHA FACEBOOK REPORT**
http://www.wolframalpha.com/facebook

Интересен начин корисниците на друштвената мрежи Facebook да дознаат кои лични податоци ги споделиле со оваа друштвена мрежа и со целиот свет. За да се генерира извештај, корисникот мора да биде најавен на својот Facebook профил во рамките на ист прегледувач.

**LIGHBEAM**
https://addons.mozilla.org/en-us/firefox/addon/lightbeam/

Додаток за Mozilla Firefox кој прикажува мрежа на сајтови кои собираат податоци за корисникот по пат на содржини на трети страни (third party content).

**TERMS OF SERVICE DIDN`T READ**
https://tosdr.org/

Интересен додаток за прегледувачи кој ги анализира условите за користење на интернет сервисот и ги издвојува најважните делови, односно деловите на кои корисникот треба да обрне внимание.

**SHARECONFERENCE.NET**

Страница на Фондацијата SHARE, корисен извор на вести и информации за состојбата во сајбер просторот во Србија, регионот и Европа.

**EFF.ORG**

Страница на Фондацијата Electronic Frontier, корисен извор на информации, софтверски решенија и различни упатства и насоки во областа на интернет безбедноста.

Забелешка: Фондацијата SHARE не фаворизира одредени програми во однос на други. Програмите кои се споменуваат во овој прирачник се избрани врз основа на нивниот рејтинг и оценките на заедницата. Фондацијата SHARE нема да сноси никаква одговорност доколку некоја од овие апликации не ја извршува функцијата која се очекува од неа. Препорачуваме одговорно користење на апликациите.