ЗАШТИТИТЕ СВОЈУ
ФИРМУ И ЗАПОСЛЕНЕ

https://pixabay.com/vectors/hack-fraud-card-code-computer-6077545/

# ФИШИНГ (PHISHING)

ПРИЈАВИТЕ СВАКИ ИНЦИДЕНТ
НА НАШЕМ ПОРТАЛУ:
HTTPS://WWW.CERT.RS/PRIJAVA.HTML

СРБ-ЦЕРТ

# УВОД

Фишинг (енг. *phishing*) је тип преваре која има за циљ прикупљање и злоупотребу поверљивих података корисника, попут бројева банковних рачуна, лозинки налога на друштвеним мрежама или приступа електронској пошти.

Жртва овог типа сајбер напада добија поруку путем електронске поште, друштвених мрежа, телефона или СМС-а у којој се од ње захтева да посети линк или отвори документ и упише личне и поверљиве податке.

Тренутно су на првом месту у начину извођења фишинг превара поруке путем електронске поште, уз очекивање да ће тако бити и у будућности. Међутим већ је приметан пораст употребе друштвених мрежа и апликација за инстант слање порука попут *WhatsApp*, *Viber* и осталих, у извођењу напада. Промена која се очекује у извођењу ових напада јесте да ће методе које се користе за слање порука бити све софистицираније.[1] Недавна студија је показала да је 88% светских организација доживело фишинг нападе, док је 86% њих имало сусрет са компромитовањемпословне електронске поште.[2]

Један број фишинг напада има за циљ крађу креденцијала, док други имају за циљ дистрибуцију злонамерног софтвера. Фишинг напади реализују се када жртва предузме радње из упутства датог у тексту поруке, које су најчешће креиране тако да упућују на брзу реакцију. Неки од примера захтеваних радњи у фишинг нападима су следећи:

- Клик на одређени линк;
- Ажурирање лозинке;
- Клик на „*Enable Content*“ или „*Enable Editing*“ у документу из прилога;
- Прихватање захтева за повезивањем на друштвеним мрежама;
- Коришћење нових приступних тачака за бежично спајање на интернет (*wi-fi hotspot*).

Фишинг поруке су креиране са намером да изгледају као да су послате из поузданих извора, док је текст поруке такав да ствара осећај знатижеље, страха или хитности с циљем навођења примаоца поруке да брзо реагује – кликом на одређени линк или преузимањем докумената из прилога. Клик на линк води на лажну страницу, која личи на легитимну, и креирана је у циљу прикупљања података као што су адресе електронске поште и лозинке. Клик на „*Enable Content*“ или „*Enable Editing*“ у документу из прилога, аутоматски покреће злонамерни софтвер који убризгава одређене процесе у оперативни систем примаоца, како би онемогућио детекцију од стране антивируса и других безбедносних софтверских решења.


*Слика 1. Начини реализације фишинг напада*

[1]ENISA Threat Landscape 2020 - Phishing — ENISA (europa.eu)
[2] 2020 ‘State of the Phish’: Security Awareness Training, Email Reporting More Critical as Targeted Attacks Spike”. January 23, 2020. Proof Point

# ВРСТЕ ФИШИНГ НАПАДА[3]

Најпрепознатљивије врсте фишинг напада су: *Spear phishing, Microsoft 365 phishing, Business email compromise, Whaling, Social media phish, Vishing i Smishing*.

***Spear phishing*** – Циљана верзија напада, којом нападач бира одређене групе појединаца, организацију или предузеће, уместо широке групе корисника. Циљ напада је најчешће крађа података, али може бити и инсталација злонамерног софтвера на рачунар циљаног корисника. За разлику од уобичајеног фишинга који представља напад усмерен ка већем броју корисника, spear фишинг као мету има тачно одређену жртву. На тај начин нападачи комуникацију могу прилагодити тако да изгледа аутентично, јер истраживањем могу доћи до одређених података о жртви као што су адреса електронске поште, листа пријатеља, локације које често посећује и сл.

***Microsoft 365 phishing*** – Нападачи за приступ налогу *Microsoft 365* електронске поште користе методе које су једноставне и најчешће подразумевају облик лажне поруке е-поште од компаније *Microsoft*. Порука је креирана тако да садржи захтев да се примаоци поруке улогују и промене лозинку наводећи да је то неопходно, најчешће јер се одређено време није приступало налогу или зато што постоји проблем са налогом који захтева додатну пажњу.

***Business email compromise (BEC)*** – Компромитовање пословне електронске поште је врста напада, односно преваре, у којој нападач користећи лажне налоге е-поште има као крајњи циљ наношење штете компанији. Често ће нападач користити налог са адресом е-поште која је скоро идентична као на корпоративној мрежи, ослањајући се на претпостављено поверење између жртве и пошиљаоца поруке са тог налога. Злонамерни нападач се представља као неко коме прималац такве поруке треба да верује – обично као колега, шеф или компанија са којом, посредно или непосредно, сарађују. Злонамерни нападач шаље поруку е-поште за коју се чини да долази од познатог извора, и који поставља легитиман захтев, као нпр. да изврши трансфер новца са једног на други рачун, преусмери платни списак, промени банкарске детаље за будућа плаћања и сл.

***Whaling*** – Напади који су усмерени ка вишим руководиоцима и најчешће се извршавају кроз е-поруке које изгледају легитимно. Из тог разлога ови напади су од посебног значаја јер виши руководиоци имају приступ великом броју осетљивих информација о компанији. Уместо слања порука широј групи људи, нападачи идентификују једну особу од које могу добити све жељене податке.

***Social media phish*** - Нападачи често истражују своје жртве на друштвеним мрежама и другим веб локацијама с циљем прикупљања детаљних информација, након чега у складу са тим планирају напад.

***Vishing (Гласовни фишинг)*** - Vishing је заправо форма фишинга, односно гласовни фишинг и представља сваку врсту напада посредством телефонских позива и *Skype*-а , а као циљну групу има кориснике *Voice Over Internet Protocol – VoIP* услуге. За време телефонског позива, нападач користи социјални инжењеринг да би жртву натерао да дели личне и финансијске податке, као што су бројеви рачуна и лозинке. Нападач се обично представља као представник полиције, особа која нуди помоћ у инсталирању софтвера (упозорење: То је вероватно злонамерни софтвер), или најчешће као представник банке говорећи жртви да јој је рачун компромитован.

***Smishing (СМС фишинг)*** – Врста фишинг напада који се шаље путем СМС-а (*Short Message Service*) и користи методе социјалног инжењеринга како би се жртва навела да подели личне податке. *Smishing* порука садржи претњу или примамљиву понуду како би жртва кликнула на линк или позвала број и поделила поверљиве информације у одређеном року. Понекад нападачи поруком могу захтевати инсталацију и неког безбедносног софтвера за који ће се касније испоставити да је злонамеран.

---

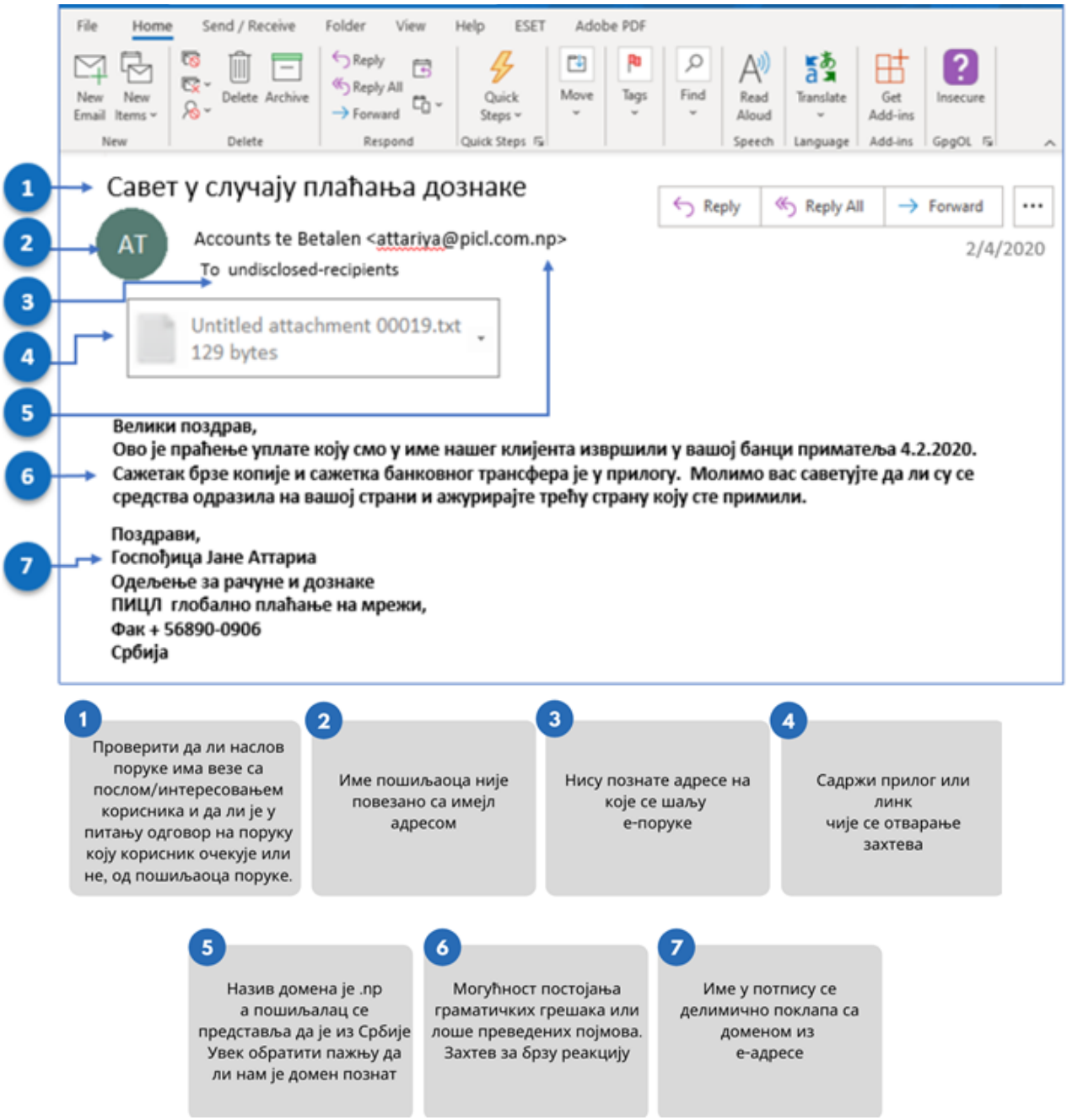
[3] What Is Phishing? Examples and Phishing Quiz - Cisco

# КАКО ПРЕПОЗНАТИ ФИШИНГ НАПАД?

У одређеним ситуацијама може бити тешко да се препозна фишинг напад, јер се поруке креирају тако да изгледају аутентично и зато је први корак одбране постојање свести о могућности преваре.

Да би били сигурни потребно је не журити са отварањем прилога у поруци, кликом на линкове или слањем одговора. Карактеристике које могу указати да је реч о фишинг превари су:[4]

- Прилози и линкови;
- Правописне грешке;
- Непотребна хитност у вези са верификацијом адресе е-поште или других личних података;
- Општи уводни поздрави попут „Поштовани клијенту“ уместо личног имена.



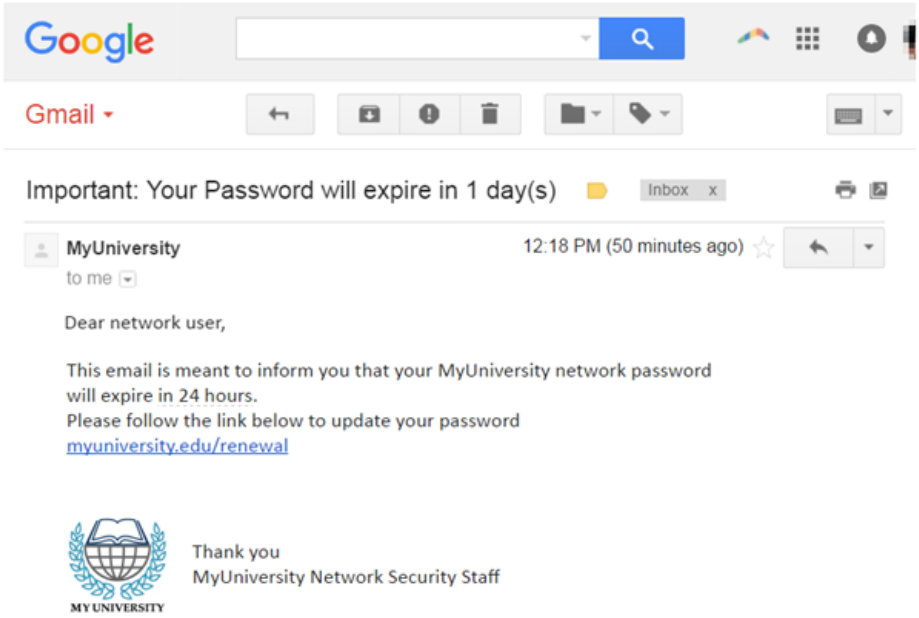

*Слика 2. Савети како препознати фишинг напад*

[4] https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips

Приликом пријема е-поруке у којој се захтева унос личних података, препорука Националног ЦЕРТ-а је детаљно анализирање **имена и адресе пошиљаоца**, као и садржај поруке. Највећи број организација имају сопствени **домен е-поште**, на пример за *Google* ће бити *@google.com.* Ако се назив домена (део иза симбола @) подудара са пошиљаоцем, порука је највероватније легитимна, а најбољи начин да се провери назив домена организације је уношење назива компаније у претраживач. Када нападачи креирају своје лажне е-адресе, односно email, они имају могућност да изаберу „име за приказ" (*From* поље) које уопште не мора да се подудара са адресом е-поште. Нападачи могу користити називе организација у локалном делу адресе е-поште да би се приликом пријема исте као име пошиљаоца појавило име организације коју нападачи користе да би извршили напад или могу да креирају лажне домене, нпр. да користе '*r*' и '*n*' једно поред другог '***rn***' уместо '***m***', или коришћење „-" уместо „." у називу домена, а све у циљу да створе осећај код жртве да је у питању легитимна организација.

Следећи пример илуструје ток фишинг напада креирањем лажне URL адресе[5]:

- Лажна адреса е-поште, наводно са *myuniversity.edu* дистрибуира се масовно што већем броју чланова факултета;
- У е-поруци се наводи да корисничка лозинка истиче, уз упутство да се приступи наведеном линку да би креирали нову лозинку у року од 24 часа, а која упућује на фишинг сајт.




*Слика 3. Пример Phishing е-поруке у којој се захтева промена шифре у кратком року*

У овом примеру URL адреса **myuniversity.edu/renewal** је промењена у **myuniversity.edurenewal.com.**


*Слика 4. Пример лажне URL адресе*

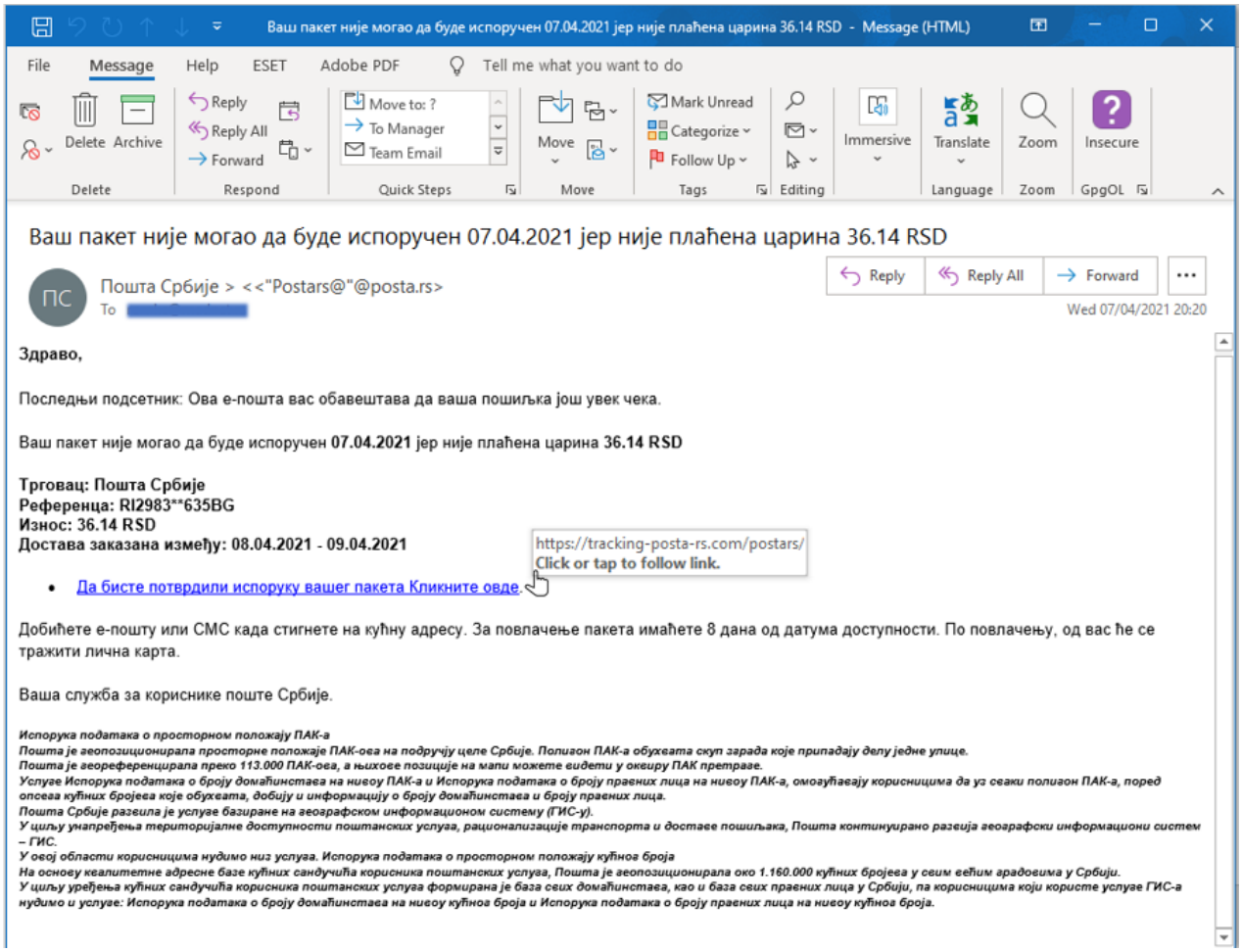
[5]https://www.imperva.com/learn/application-security/phishing-attack-scam/

Сличност између ове две адресе, корисника може да наведе на мисао да је у питању безбедна адреса интернет странице чинећи га мање свесним да је у питању сајбер напад.

Препорука је да у случају пријема поруке која садржи захтев попут промене лозинке, коју је потребно спровести у неком кратком периоду, наводећи корисника на брзу реакцију због истека времена и стварајући осећај хитности да се захтев испуни, увек накнадно провери URL адреса на којој се тражи промена шифре. Препорука је да се легитимна адреса претражи путем интернет претраживача, а не кликом на линк из е-поруке. Компарацијом адреса, често се могу уочити недоследности, и на тај начин се потенцијална превара може избећи.

Приликом пријема порука е-поште у којима се захтева да се приступи одређеном линку, да се верификује лозинка и слично, иако порука може изгледати као да стиже из поузданог извора, мале грешке у куцању или недоследности у домену често могу открити праву природу дате поруке, односно потенцијалног напада.

Следећи пример илуструје фишинг кампању која је била усмерена на кориснике поштанских услуга. У овом примеру, корисници су добијали е-пошту са обавештењем да је пристигао пакет корисника, али да није могао бити испоручен јер није уплаћен износ од 36,14 динара за царинске трошкове. Порука је стизала са лажне адресе: Поште Србије *''Postas@"@posta.rs*, са насловом: Ваш пакет није могао да буде испоручен 07.04.2021 јер није плаћена царина 36.14 РСД.

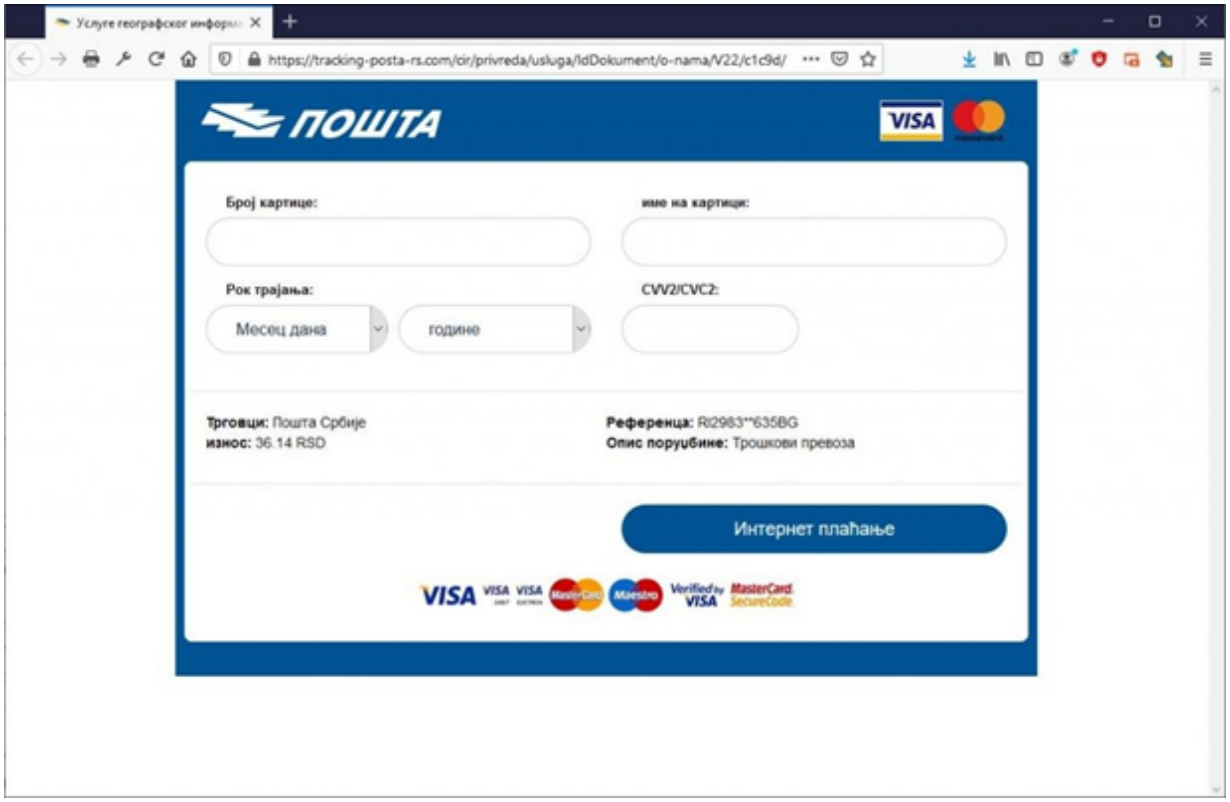



*Слика 5. Пример Phishing е-поруке за Пошту Србије уз линк на ком се захтева плаћање*

Препорука Националног ЦЕРТ-а је да се пре приступа линку, прво провери адреса пошиљаоца, обзиром да се адреса може лажирати, што се може видети у овом примеру ''*Postas@"@posta.rs*, иако је као име за приказ назначена „Пошта Србије“. Такође, савет је обратити пажњу на граматичке грешке, које су такође један од показатеља да је у питању фишинг превара.

Даље у тексту, преласком курсора преко линкованог текста (линка), види се линк који може изгледати легитимно, и отварањем истог, приказује се фишинг страница која садржи лого Поште Србије и има садржај хитности како би пошиљка била достављена. Иако интернет страница може изгледати као легитимна страница сајта Поште Србије, она то заправо није. На врху екрана се може видети потпуно нетачна URL адреса, што се може проверити претрагом званичне странице Поште Србије путем претраживача.

Отварањем линка, корисник се преусмеравао на лажну страницу за интернет плаћање Поште Србије, у којој се захтевао унос података: Број платне картице, Име и Презиме, Рок трајања, као и *CVV2/CVC2* број картице. Уносом тражених података, нападач би дошао у посед информација на основу којих би могао да преузме новац са рачуна лица које је оставило податке.




*Слика 6. Пример Phishing сајта са формом за унос података за платне картице*

Препоруке Националног ЦЕРТа за превенцију од фишинг напада јесу:

- Обратити пажњу на поље „*From*“ и да ли је пошиљалац познат;
- Проверити да ли постоје правописне грешке у тексту поруке;
- Уколико постоји непотребна хитност за реакцију, не журити са отварањем линкова и прилога из поруке;
- Проверити легитимност *URL* адресе, провером адресе у интернет претраживачу;
- Упоредити да ли је име пошиљаоца повезано са адресом е-поште;
- Обратите додатно пажњу када се тражи унос података о банковној картици, посебно када је реч о *CVV2/CVC2* број картице;
- Ако примите сумњиву поруку електронске поште означите је као *Spam/Junk* или је одмах избришите.

Ако сте кликнули на линк или документ предузмите следеће кораке:

- Ако користите службени телефон или лаптоп одмах контактирајте ИТ службу;
- Ако сте дали своје податке о банковном рачуну одмах обавестите банку;
- Активирајте антивирус и кликните на „*full scan*“;
- Ако сте оставили своју лозинку, одмах промените лозинке на свим налозима;
- Ако сте изгубили новац одмах контактирајте своју банку и пријавите полицији на vtk@mup.gov.rs;

*Национални ЦЕРТ Републике Србије не промовише или фаворизује било који од коришћених јавних извора, међу којима су и комерцијални производи и услуге. Све препоруке, анализе и предлози дати су у циљу превенције и заштите од безбедносних ризика.*

РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНА АГЕНЦИЈА ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

#odbraniseznanjem

СРБ-ЦЕРТ

# Рансомвер као модел пружања услуга

(Ransomware-as-a-Service)

СРБ-ЦЕРТ

Рансомвер представља једну од најзаступљенијих интернет претњи. Статистички подаци Европске агенције за мрежну и информациону безбедност *(ENISA)** указују да је током 2022. године забележен пад броја изнуђених плаћања жртава рансомвер напада, док се у 2023. години поново бележи њихов пораст, баш као и пораст броја наплаћених изнуда. Узрок пораста је увођење тзв. "Дупле изнуде" као додатног облика изнуђивања. Уколико узмемо у обзир и чињеницу присуства вештачке интелигенције и могућности њене злоупотребе, то нам јасно може указати да ће рансомвер напад и даље бити у самом врху листе најзаступљенијих сајбер напада и да је примена превентивних мера једна од најбољих метода заштите од рансомвер напада.

Рансомвер (енг. *Ransomware*), је тип малвера (малициозни програмски код) који је усмерен на неовлашћено приступање информационим системима или уређају, са задатком да кориснику лимитира приступ, или да закључа одређене фајлове и датотеке и на тај начин у потпуности онемогући приступ нападнутом информационом систему или уређају. Крајњи циљ нападача је противправно стицање имовинске користи, али може бити злоупотребљен и за остваривање политичких, односно хактивистичких циљева. Након неовлашћеног приступа и закључавања фајлова или датотека, нападачи шаљу поруку која се појављује на монитору жртве која садржи инструкције за откуп декрипционих кључева (програмски код за откључавање), који би жртви требало да омогући поновни приступ инфицираним фајловима или датотекама.

Током свог развоја, рансомвер је представљао тип сајбер напада који је, пре свега, био усмерен на физичка лица, односно појединце. Разлог томе је био низак ниво сајбер културе појединца, која се најпре огледала у креирању само једне и често једноставне лозинке за приступ интернет налозима, као и неадекватна заштита уређаја у виду одсуства лиценцираних антивирусних софтвера. Малициозни програмски код за откључавање енкриптованих фајлова и датотека је често био лошег квалитета и није откључавао све инфициране датотеке. Са друге стране чест проблем је представљала и немогућност брзе реализације изнуде захтеване суме новца. То су била два основна  изазова са којима су се суочавале жртве, али и нападачи приликом коришћења рансомвера.

Са унапређењем малициозног програмског кода, растао је и ниво софистицираности напада, што је хакерима омогућило да усмере своје нападе на мала и средња предузећа, а затим и на веће и боље заштићене системе. Онемогућавање рада великих система представља велики изазов како за конкретно правно лице, тако и за све оне који користе услуге или производе нападнуте организације.

Организовање сајбер напада на правна лица је нападачима омогућило и већу зараду, што је касније водило ка организовању већег броја хакера у „корпоративни модел пословања", као и развоја *RaaS (Ransomware-as-a-Service)* услуга.

*RaaS* услуге заправо представљају нови бизнис модел дизајниран од стране већих и озбиљнијих хакерских група које креирају одређени тип рансомвера и нуде га на продају

* https://www.enisa.europa.eu/publications/enisa-threat-landscape-²0²³

заинтересованим купцима, било да је реч о другим хакерским групама, било да говоримо о потенцијалним купцима који немају техничка знања, али из одређених интереса желе да покрену рансомвер напад на неки информациони систем. Хакерске групе своје RaaS услуге најчешће нуде заинтересованим купцима путем реклама на *Dark Web*-у. Купац се може одлучити за различити „пакет услуга" које су доступне у одговарајућем ценовном рангу - од једнократне услуге, па све до месечних или других одговарајућих модела „претплате".

У продужетку се налази кратак опис основних десет корака за извршавање Рансомвер напада:

1. анализа и одабир потенцијалне жртве,
2. анализа одбрамбених капацитета информационог система жртве,
3. уколико жртва има квалитетну заштиту система, приступа се анализи одбрамбених капацитета информационог система повезаних компанија са којима жртва има остварену пословну сарадњу, како би се упало преко тих система који имају слабију одбрану,
4. упад у систем жртве (најчешће то може бити помоћу фишинга, компромитације пословне кореспонденције – *BEC*, искоришћавања рањивости система који није ажуриран, или RDP приступа) који нападачима омогућава приступ информационом систему жртве,
5. копирање података из система жртве на систем нападача за потребе „Дупле изнуде",
6. анализа пословних процеса и података на основу преузетих информација из система жртве,
7. активирање одговарајућег рансомвер програмског кода који закључава датотеке на информационом систему жртве,
8. захтевање откупа декрипционих кључева у крипто валути,
9. претња јавним објављивањем прекопираних пословних и личних података путем медија („Дупла изнуда"),
10. достављање декрипционих кључева (у случајевима када жртва плати изнуђену суму новца).

Вођени „корпоративним моделом пословања" хакерске групе се данас углавном организују и раде у тимовима. Једна група ради анализу финансијских и пословних података приликом одабира жртве, док други тимови могу радити на анализи повезаних компанија у намери да злоупотребом ресурса повезане компаније омогуће нападачима лакши приступ систему крајње жртве рансомвер напада.

За потребе напада, хакери се најчешће одлучују за финишг напад, као улазни вектор, али то може бити и искоришћавање неке од рањивости информационог система жртве, као и злоупотреба RDP *(Remote Desktop Protocol)* приступа систему.

Након упада у систем жртве, хакери раде детаљну анализу пословних процеса и података, како би на основу те анализе могли да организују напад и дефинишу који је реални износ откупа који могу захтевати од жртве. Уовом кораку хакери такође преузимају одређену количину количину података из информационог система жртве и копирају их на своје системе.

Тако прикупљени подаци им служе за каснију претњу којом желе додатно да присиле жртву да плати износ откупа. Уколико би жртва одбила плаћање откупа, нападачи би запретили објављивањем прикупљених пословних и личних података целокупној јавности, путем медија, што представља тзв. „Дуплу изнуду".

Препорука Националног ЦЕРТ-а Републике Србије је да се откупни износ не плаћа, јер се на тај начин финансира криминално деловање хакерских група, при чему нема никаквих гаранција да ће жртва добити декрипционе кључеве, или да ће добијени кључеви у потпуности омогућити приступ и коришћење података који су били закључани рансомвером током напада. Са друге стране, уколико се плати откупни износ, хакерске групе се често опредељују да и у будућности понове напад на исту организацију или компанију, без обзира на поруку да ће, уколико им се први пут уплати тражени износ, заувек нестати из система те жртве и неће се више враћати.

Последице рансомвер напада могу имати веома негативан утицај на пословање, профит, али и репутацију организације или компаније, због чега је значај примене превентивних мера заштите у интересу свих запослених у једној организацији или компанији, као и повезаних пословних партнера са којима је остварена добра сарадња. Такође, значај примене превентивних мера се може односити и на све кориснике којима се нуде услуге одређене организације или компаније.

Превентивне мере, које се могу предузети у циљу заштите од рансомвер напада, су:

1. редовно ажурирање оперативних и апликативних софтвера, како би биле примењене све доступне закрпе за откривене рањивости,
2. сегментирање мреже којим се једна велика мрежа претвори у скуп мањих делова мреже, чиме се онемогућава брзо потенцијално ширење малвера по целокупној мрежи,
3. инсталација лиценцираног програма за заштиту рачунара од вируса и малвера,
4. редовно креирање резервних копија свих важних датотека и фајлова,
5. редовно тестирање резервних копија,
6. увођење и примена мултифакторске аутентификације као додатног слоја заштите,
7. контрола приступа информационом систему са удаљених локација,
8. континуиран рад на подизању свести запослених о безбедносним претњама, који се најпре огледа у:

    - креирању комплексних лозинки,
    - примена принципа: један налог – једна лозинка
    - коришћењу службених имејл налога искључиво у корпоративне сврхе,
    - избегавању клика на линк или отварање прилога у имејлу који стигне од непознатог пошиљаоца, јер се фишинг често користи као улазни вектор за рансомвер нападе,

- чувању личних или финансијских података, односно да их не треба делити путем: имејла, СМС или чет порука, телефонског позива или у директном разговору са непознатим особама,
- провери домена интернет страница које се посећују, имајући у виду да се на интернету налази велики број компромитованих интернет страница путем којих се шире малициозни садржаји.

Остале мере превенције, превасходно усмерене на пословне кориснике, можете погледати у нашој публикацији „Препоруке за заштиту од рансомвер напада”.


# КАКО ПОСТУПИТИ УКОЛИКО ДОЂЕ ДО КОМПРОМИТОВАЊА ЕЛЕКТРОНСКЕ ПОШТЕ И КАКО ЗАШТИТИТИ НАЛОГЕ

ПРИЈАВИТЕ СВАКИ ИНЦИДЕНТ
НА НАШЕМ ПОРТАЛУ:
HTTPS://WWW.CERT.RS/PRIJAVA.HTML

СРБ-ЦЕРТ

Комуникација посредством електронске поште (*e-mail*) одвија се годинама уназад и представља ефикасан и једноставан начин размене порука како у циљу личне тако и професионалне комуникације.

Масовност употребе електронске поште, коришћење налога електронске поште за приступ друштвеним мрежама (*Facebook*, *Instagram*, *LinkedIn* itd.) или за пријем извода стања на банковном рачуну као и за приступ различитим апликацијама и сајтовима, за нападаче представља вредан ресурс, јер приступом налогу електронске поште (корисничком имену и лозинки) могу доћи у посед личних и поверљивих података о кориснику.

Када се одређени корисник интернета нађе у ситуацији да су нападачи неовлашћено приступили његовом налогу електронске поште, постоје кораци које је могуће предузети а који би кориснику омогућили поновни приступ налогу који је претходно био компромитован, као и смернице о начинима заштите налога како се корисник не би нашао у ситуацији да остане без приступа свом налогу електронске поште.

## РАЗЛОЗИ ЗБОГ КОЈИХ ЈЕ ЕЛЕКТРОНСКА ПОШТА МЕТА НАПАДАЧА

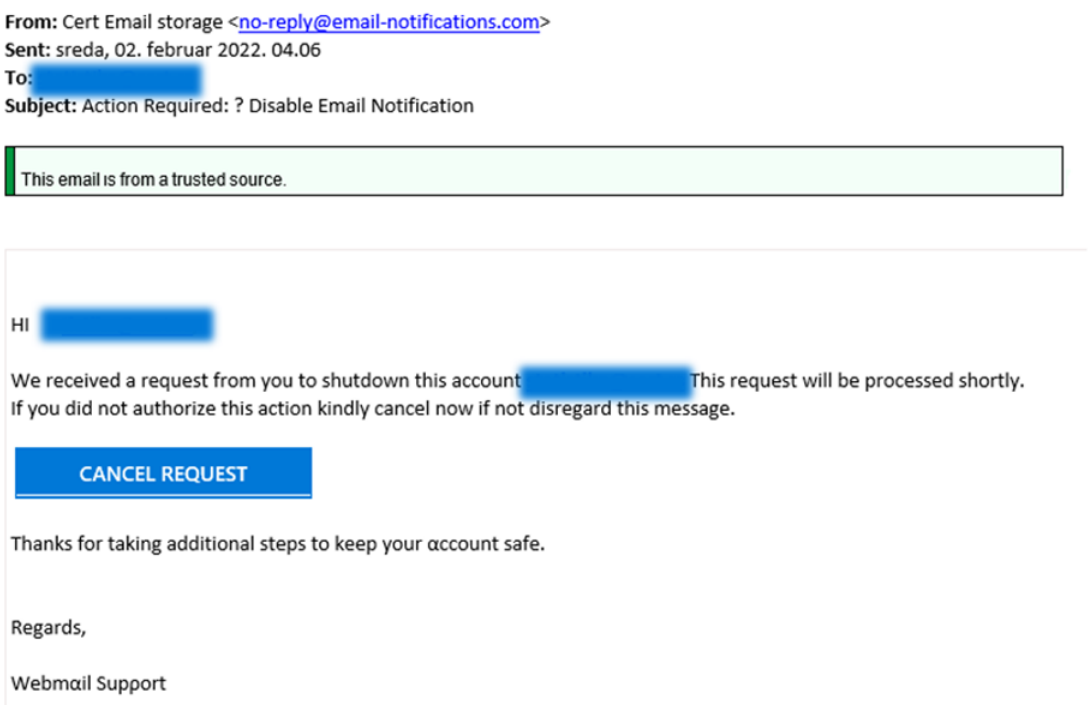
Најчешћи разлози због којих је електронска пошта мета нападача су:

- Уколико нападач преузме налог електронске поште корисника то му може омогућити приступ подацима на другим налозима, на пример може доћи до података корисника на друштвеним мрежама ако је налог креиран на основу те адресе или може приступити свим приватним фајловима корисника на *Dropbox-u*, *Google Drive-y* и другим сервисима за складиштење фајлова, и на тај начин нападач добија приступ личним информацијама корисника.
- Неовлашћеним приступањем налогу електронске поште корисника, нападачи имају могућност да ресетују лозинке и приступе свим другим налозима корисника, обзиром да већина интернет сајтова и апликација на адресу електронске поште шаље линк за ресетовање лозинке, чиме једним кликом нападачи могу променити лозинке свих других налога корисника.
- Када нападач приступи налогу електронске поште корисника, то му омогућава увид у преписке и листу контаката (чланови породице, пријатељи или пословни партнери) што нападачи даље могу искористити за слање нежељене електронске поште, најчешће кроз фишинг поруке, са циљем компромитовања што већег броја налога.

## КОЈИ СУ НАЧИНИ НА КОЈЕ НАПАДАЧИ МОГУ НЕОВЛАШЋЕНО ПРИСТУПИТИ ЕЛЕКТРОНСКОЈ ПОШТИ?

Нападачи најчешће користе следеће начине како би неовлашћено приступили електронској пошти корисника:

- Слањем порука посредством електронске поште која је креирана тако да изгледа као да је послата из легитимног извора, нпр. од стране провајдера електронске поште (*Gmail*, *Yahoo*, *Microsoft Outlook* itd.), где се од корисника захтева да се опет пријави на налог. Најчешће је та порука креирана са елементима хитности, где се у кратком року захтева пријава на налог, на пример како би корисник избегао губитак података, гашење налога или како би променио лозинку јер је наводно друга особа покушала да приступи налогу корисника.



**From:** Cert Email storage <no-reply@email-notifications.com>
**Sent:** sreda, 02. februar 2022. 04.06
**To:** [redacted]
**Subject:** Action Required: ? Disable Email Notification

This email is from a trusted source.

HI [redacted]

We received a request from you to shutdown this account [redacted] This request will be processed shortly.
If you did not authorize this action kindly cancel now if not disregard this message.

CANCEL REQUEST

Thanks for taking additional steps to keep your account safe.

Regards,

Webmail Support

Слика 1 – Пример е-поште о наводном гашењу налога корисника

- *Brute Force* напади који подразумевају покушај приступа систему жртве непрекидним логовањем различитим комбинацијама слова, бројева и симбола са циљем идентификације корисничког имена и лозинке.
- Када корисник приступа електронској пошти коришћењем јавне бежичне мреже (*Wi-Fi*), нападачи могу да пресретну њихов приступ интернету чиме добијају увид у комплетан саобраћај и могу да преузму поверљиве податке или идентитет корисника.
- Преузимањем злонамерног софтвера (малвера) кроз поруке електронске поште из непроверених извора (најчешће су у питању фишинг поруке).

# КАКО КОРИСНИК МОЖЕ ПРОВЕРИТИ ДА ЛИ ЈЕ НЕКО НЕОВЛАШЋЕНО ПРИСТУПИО ЊЕГОВОМ НАЛОГУ ЕЛЕКТРОНСКЕ ПОШТЕ?

Следећи примери илуструју ситуације у којима је највероватније дошло до неовлашћеног преузимања налога електронске поште од стране нападача:

- Очигледан показатељ да је налог компромитован јесте уколико корисник не може да приступи налогу уз обавештење да је лозинка промењена;
- Пријатељи и колеге примају нежељену пошту која долази са адресе електронске поште корисника који сумња да му је налог компромитован;
- Пријем више узастопних захтева за променом лозинке са других интернет страница и апликација;
- Провајдер електронске поште (*Gmail*, *Yahoo*, *Microsoft Outlook* itd.) обавештава корисника о вишеструким пријавама са непознатих *IP* адреса и локација.

# КОРАЦИ КОЈЕ ЈЕ МОГУЋЕ ПРЕДУЗЕТИ УКОЛИКО ЈЕ ДОШЛО ДО НЕОВЛАШЋЕНОГ ПРЕУЗИМАЊА НАЛОГА ЕЛЕКТРОНСКЕ ПОШТЕ

Уколико корисник има и даље приступ налогу, потребно је у најкраћем року:

- Променити лозинку компромитоване електронске поште као и све лозинке на налозима где се ова адреса користила као и пратећа сигурноса питања која су везана за конкретан налог;
- Активирати антивирус, кликом на „*full scan*";
- У оквиру секције подешавања проверити да ли су промењени претходно дефинисани параметри.

Ако корисник нема приступ налогу, и лозинка је промењена од стране нападача, потребно је започети процедуру опоравка. У одређеним случајевима налог је могуће опоравити користећи методе враћања налога као што су коришћење секундарне адресе електронске поште, броја телефона или одговором на сигурносна питања. Провајдер електронске поште ће кориснику омогућити линк са лозинком за враћање налога на секундарну адресу електронске поште, или поруку на мобилни телефон са циљем враћања налога.

Процедуре за опоравак налога електронске поште, за различите провајдере, се налазе на следећим линковима:

- Gmail
- Microsoft Outlook
- Yahoo

Међутим, уколико су нападачи изменили податке за приступ налогу, потребно је контактирати подршку у циљу добијања информација о додатним корацима доказивања идентитета корисника што може бити дуготрајан процес, а не мора се увек завршити успешно – односно враћањем налога кориснику. Из тог разлога неопходно је предузети све кораке да се електронска пошта заштити од неовлашћеног приступа.

# КАКО ЗАШТИТИТИ ЕЛЕКТРОНСКУ ПОШТУ ОД НЕОВЛАШЋЕНОГ ПРИСТУПА?


Слика 2 - Кораци заштите налога електронске поште

**1. Креирање комплексних лозинки**

Један од начина заштите налога, који смањује могућност неовлашћеног приступа личним и осетљивим подацима корисника јесте креирање комплексних лозинки.

Основне смернице за креирање сигурних лозинки су:

- Коришћење најмање 9 алфанумеричких карактера и то:

  - малих слова (a-z)

  - великих слова (A-Z)

  - бројева (0-9)

  - знакова (!@#$%^&*)

- Лозинка не би требало да садржи личне податке (име, презиме, надимак, датум рођења, име кућног љубимца итд.)
- Приликом креирања лозинки не користити секвенце са тастатуре (део реда на тастатури као што су qwerty, 123456 итд.)
- Не користити исту лозинку за више налога.

Лозинка треба да садржи сваки од препоручених словних или знаковних карактера, како би сложеност лозинке била што већа чиме би се отежао неовлашћени приступ.

**2. Коришћење двофакторске аутентификације**

Коришћењем двофакторске аутентификације обезбеђује се додатан ниво безбедности што се налога тиче, обзиром да подразумева постојање више корака провере како би корисник доказао идентитет, односно да је заправо корисник тај који приступа налогу. На пример, за пријаву на налог електронске поште поред лозинке, корисник ће добити сигурносни код путем СМС поруке чијим уношењем доказује идентитет и приступа налогу. Двофакторска аутентификација подразумева комбиновање два начина од следећа четири:

- Оно што знам (лозинка, ПИН)
- Оно што имам (токен, картице, мобилни телефон)
- Оно што јесам (отисак прста, препознавање лица, ока...)
- Оно што радим (говор)

**3. Приликом коришћења отвореног бежичног интернета (*Wi-Fi*), односно јавно доступних тачака за приступ интернету треба бити додатно обазрив**

Бесплатан приступ бежичном интернету представља све распрострањенију услугу која се нуди корисницима угоститељских објеката, хотела, тржних центара, аеродрома, чак и возила јавног превоза. Велики број корисника свакодневно користи бесплатан приступ бежичном интернету за различите потребе - за приступ друштвеним мрежама, електронској пошти или на пример за „рад на даљину“ у омиљеном кафе бару. Већина корисника није свесна да су на тај начин изложени ризику од губитака података, као што су фотографије, поруке, лични подаци, лозинке и информације о банковним рачунима. Веома распрострањен тип сајбер напада приликом коришћења јавних бежичних мрежа јесте тзв. „човек у средини“ (енг. ***Man-in-the-middle - MITM***), где је нападачима циљ да буду у истој мрежи са другим корисницима и пресретну њихов приступ интернету чиме добијају увид у комплетан саобраћај и могу да преузму поверљиве податке или идентитет корисника.

Нападачи такође могу лако креирати лажно приступно место (*hotspot*) за бежичну јавну мрежу, која имитира мрежу неког угоститељског или другог објекта - где је најчешће слободан приступ или су шифре лако доступне и ретко се мењају. То омогућава нападачу да постави замку са називом мреже која личи на назив угоститељског објекта, или називом као што је “Бесплатан *Wi-Fi*“. Када се корисник повеже на приступну тачку, креирану на овакав начин, за бесплатан бежични интернет, тада нападач добија приступ осетљивим подацима корисника.

Најбољи начин да се заштите поверљиви подаци приликом коришћења јавних бежичних мрежа је да се избегава приступање налозима електронске поште, друштвених мрежа или обављање финансијских трансакција.

**4. Водити рачуна приликом пријема порука које у себи садрже прилоге или линкове**

Фишинг је тип преваре која за циљ има прикупљање и злоупотребу поверљивих података корисника, попут бројева банковних рачуна, лозинки налога на друштвеним мрежама или приступа електронској пошти. Један број фишинг напада има за циљ крађу креденцијала, док други имају за циљ дистрибуцију злонамерног софтвера. Фишинг поруке најчешће се дистрибуирају путем порука електронске поште и креиране су са намером да изгледају као да су послате из поузданих извора, док је текст поруке такав да ствара осећај знатижеље, страха или хитности с циљем навођења примаоца поруке да брзо реагује – кликом на одређени линк или преузимањем докумената из прилога. Клик на линк води на лажну страницу, која личи на легитимну, и креирана је у циљу прикупљања података као што су адресе електронске поште и лозинке. Додатно је важно водити рачуна о пошиљаоцу поруке, о самом тексту поруке - да ли постоје граматичке или правописне грешке и бити посебно обазрив код порука које садрже прилоге или линкове. Више о фишинг преварама можете прочитати овде.

### 5. Редовно ажурирање оперативног система и софтвера

Редовно ажурирање оперативних система, софтвера и апликација поможе у превенцији да до безбедносних ризика уопште дође, обзиром да је главна сврха ажурирања да додају новине, поправе или побољшају софтвер који се користи. Препорука је да се укључи аутоматско ажурирање за оперативни систем као и за све апликације које имају ту опцију јер нападачи могу користити уочене и познате рањивости система или апликација у току спровођења напада. Редовним ажурирањем обезбеђују се закрпе за уочене рањивости, што за нападача отежава посао у извођењу напада.

Национални ЦЕРТ препоручује свим корисницима електронске поште да пријаве инцидент уколико дође до неовлашћеног преузимања налога, док применом свих наведених превентивних мера корисници имају могућност да се сами заштите од оваквих видова малициозних активности нападача.

Шта је Phishing?

Пхисхинг (пецање) је метод преваре где вам нападачи пошаљу садржај представљајући се као нека стварна фирма, а у циљу отварања фајлова или остављања поверљивих информација.

Како препознати Phishing емаил?

Најпознатији пример пхисхинг мејла је Принц од Нигерије који је тражио да му се уплати новац, а мејлови су почињали са текстом "Salutations from the son of the deposed Prince of Nigeria…" и било је релативно лако препознати да се ради о лажном емаилу. Међутим временом су пхисхинг мејлови постали све сличнији стварним мејловима и знатно их је теже детектовати.
Ово су само неке од најбитнијих **карактеристика** пхисхинг емаилова:

1. Мејлови се не шаљу са домена са кога се наводи
2. Користе генеричне поздраве
3. Линкови унутар мејла воде на неки трећи сајт
4. Траже вам поверљиве податке путем мејла
5. Шаљу вам фајлове са чудним називима

**Примери Phishing емаилова:**

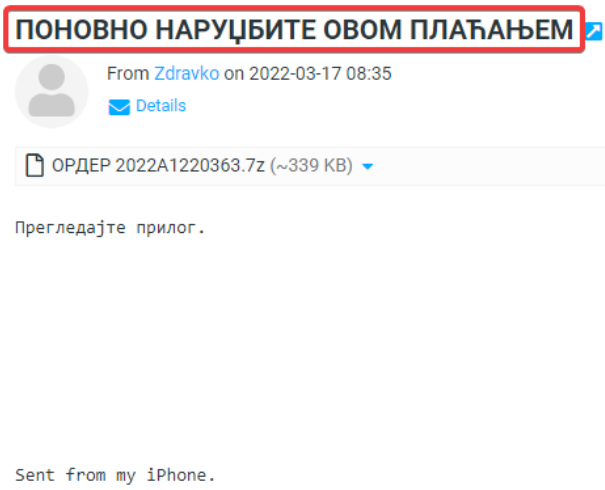
Издвојили смо 7 примера стварних Phishing мејлова, напомињемо да су сви подаци укључујући и емаил адресе и домене на сликама измењени.

1. Траже вам податке путем емаила
Уколико сте добили емаил од банке која тражи да преузмете фајл из прилога који садржи листу трансакција, измените га и пошаљете назад, велика је вероватноћа да је реч о СПАМ / Phishing мејлу.
Стварне фирме вам никада неће тражити поверљиве информације попут лозинки, броја рачуна или кредитне картице, већ ће вам послати линк до форме на њиховом сајту где се морате претходно пријавити како бисте унели те информације.

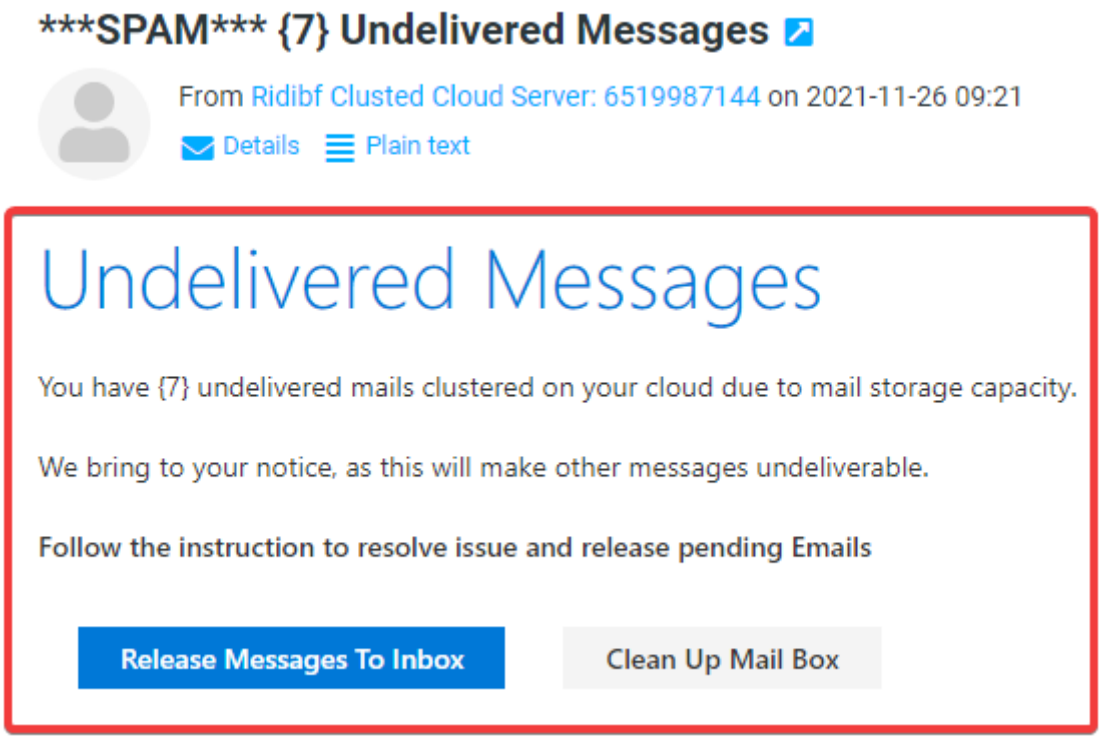
2. Не ословљавају вас по имену
Phishing мејлови углавном почињу са генеричним поздравима, нпр. “Драги господине” или “Поштовани корисниче”. Ово би требало да вам буде прва црвена застава јер фирме код којих имате направљене налоге имају ваше податке и знају ваше име, те ће вас у већини случајева ословљавати по имену, нпр. Драга Слађана.


3. Не шаљу емаил са свог домена
Важно је напоменути да Фром адреса у хеадеру мејла није нужно и адреса са које се заиста шаље мејл. Фром адреса је само адреса која се приказује да са ње долази мејл, док је Сендер адрреса заправо она са које се заиста врши слање. Добра пракса је да обе адресе буду исте, међутим пошто већина емаил програма као што су нпр. Гмаил или Вебмаил, приказују само Фром адресу, ово се често злоупотребљава.
Уколико сумњате да мејл долази са неке друге адресе можете кликом на Детаилс, а затим на Алл хеадерс.. видети хеадер поруке где су наведене и Фром и Сендер адресе.

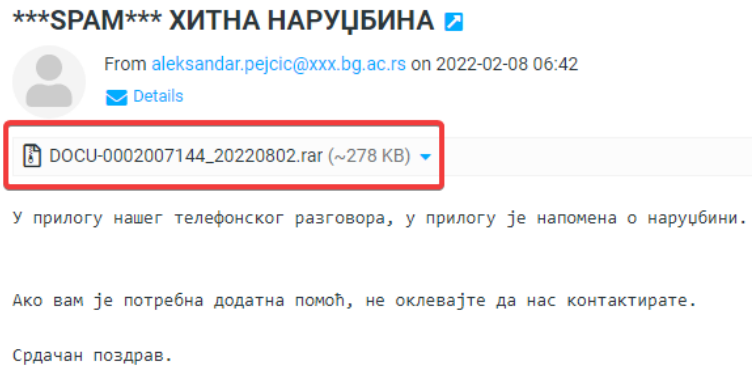
4. Словне или правописне грешке
Следећи мејл на први поглед делује легитимно, међутим наслов мејла је “ПОНОВО НАРУЏБИТЕ ОВОМ ПЛАЋАЊЕМ” као да је аутоматски преведен са неког другог језика на Српски језик.
Наравно то можда некада и јесте случај, али овакве словне или правописне грешке у већини случајева су знак да се ради о аутоматском превођењу текста и најчешће и јесте реч о СПАМ мејловима.



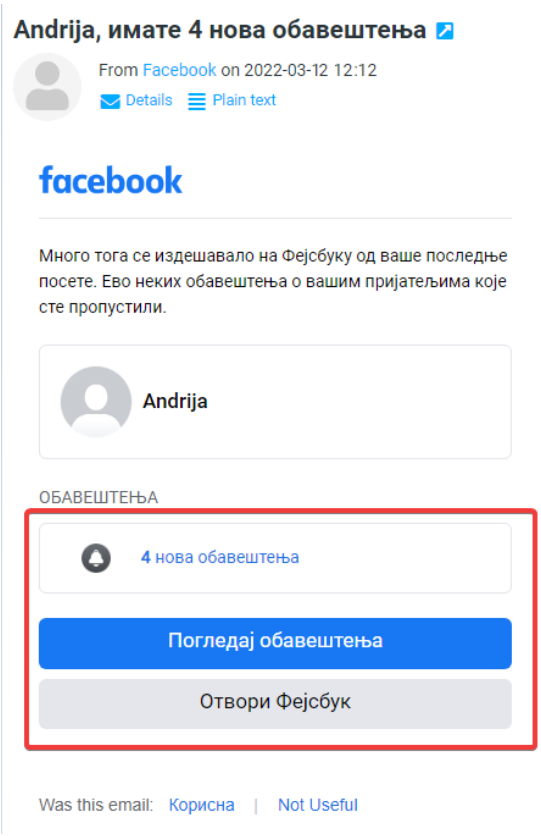

5. Терају вас на свој сајт
Пхисхинг мејлови који су најефектнији су они који траже хитне акције од примаоца под претећим изговорима: Ваш налог ће бити суспендован, Прешли сте квоту за мејлове те неће радити док не обришете кликом на дугме у мејлу, Неко вам је послао поруку кликните да је видите и сл..



6. Шаљу вам фајлове за преузимање
Ово је такође још један од знакова пхисхинг мејлова, типично институције као што су банке вам неће слати аттацхменте у мејловима како бисте попунили податке и вратили их назад, већ ће вам послати линкове ка свом сајту где можете преузети или попунити документе уколико сте улоговани на свој налог.
Наравно и овде постоје изузеци и неке фирме ће вам слати фајлове као што су рачуни или изводи, међутим и ту обратите пажњу да ли се ради о .exe, .pap или .зип екстензијама које најчешће садрже малициозне фајлове.




7. Линкови се не слажу са сајтом
У овом примеру мејла наводи се да он долази са адресе фацебоок.цом међутим кликом на линк из потписа мејла отвара се страница која уопште није на овом домену: хттпс://хф2а6-2иааа-аааад-qбх7а-цаи.иц.флеек.цо/
Али не морате кликнути на линк да бисте то проверили, на рачунару када пређете мишем преко линка у доњем левом углу можете видети линк који би се отворио ако бисте кликнули.



# Šta je ransomware?

Ransomware je zlonamerni tip programa koji zaključava vaš kompjuter, tablet ili pametni telefon – ili enkriptuje vaše fajlove i zatim zahteva otkup za njihovo bezbedno vraćanje. Postoje u suštini dva tipa ransomware-a.

Prvi tip su kriptori, koji enkriptuju fajlove i tako ih čine nedostupnim. Za dekripciju fajlova potreban je ključ korišćen prilikom enkripcije – za to plaćate otkup.

Drugi tip su blokeri; oni jednostavno blokiraju kompjuter ili drugi uređaj, čineći ga neupotrebljivim. Blokeri zapravo predstavljaju bolji scenario od kriptora; žrtva ima veće šanse za oporavak blokiranog pristupa nego kod enkriptovanih fajlova.

# Koliko obično iznosi otkup?

Ne postoji uobičajena cifra. Ipak, 300 dolara je prosečan otkup koji iznuđivači traže od svojih žrtava da plate kako bi povratili pristup enkriptovanim fajlovima ili zaključanim kompjuterima. Ali, neki ransomware programi traže i samo 30 dolara. Pojedini zahtevaju desetine hiljada dolara. Preduzeća i druge velike organizacije, koje se obično inficiraju kroz fišing, imaju veće šanse da dobiju više otkupne zahteve.

Međutim, trebalo bi da imate u vidu da plaćanje otkupa ne obezbeđuje sigurno i pouzdano vraćanje fajlova.

# Mogu li da dekriptujem enkriptovane fajlove bez plaćanja otkupa?

Ponekad. Većina ransomware programa koristi otporne kripto algoritme, što znači da bi bez ključa za enkripciju njihovo dekriptovanje moglo potrajati godinama.

Ponekad kriminalci koji stoje iza ransomware napada čine greške, omogućavajući predstavnicima zakona da oduzmu napadačke servere koji sadrže ključeve za enkripciju. Kada se to dogodi, dobri momci su u mogućnosti da razviju dekriptor.

# Kako se plaća otkup?

Obično se otkup zahteva u kripto valuti, odnosno bitkoinima. Ova elektronska valuta ne može biti falsifikovana. Istorija transakcija je dostupna svima, ali vlasnik novčanika ne može lako biti praćen. Zato sajber kriminalci preferiraju bitkoine. Tako uvećavaju svoje šanse da ne budu uhvaćeni.

Neki tipovi ransomware-a koriste anonimne onlajn novčanike ili čak mobilna plaćanja. Najveće iznenađenje do sada je bio zahtev za iTunes karticama od 50$.

# Kako ransomware završi na mom kompjuteru?

Najčešće putem e-maila. Ransomware se može predstaviti kao koristan ili važan attachment (hitna faktura, zanimljiv članak ili besplatna aplikacija). Kada otvorite prilog, vaš računar se zarazi.

Međutim, ransomware se može infiltrirati u vaš sistem i dok samo surfujete po internetu. Da bi preuzeli kontrolu nad vašim sistemom, iznuđivači koriste slabosti operativnog sistema, browsera ili aplikacija. Zato je od presudnog značaja da vaš softver i operativni sistem budu uvek ažurirani – update-ovani.

Neki ransomware programi mogu se samostalno širiti kroz lokalne mreže. Na primer, ako Trojanac inficira jednu mašinu ili uređaj u vašoj kućnoj ili korporativnoj mreži, i drugi korisnici bi na kraju mogli da se zaraze. Ali to je redak slučaj.

Naravno, postoje scenariji infekcije koji su predvidljiviji. Skinete torent, zatim instalirate plugin… i tako sve počinje.

# Koje vrste fajlova su najopasnije?

Najsumnjiviji fajlovi su izvršni (poput EXE ili SCR), a ne zaostaju puno ni Visual Basic ili Java skripte (.VBS i .JS ekstenzije). Oni su vrlo često upakovani u ZIP ili RAR arhive, kako bi sakrili svoju zlonamernu prirodu.

Još jedna opasna kategorija fajlova su MS Office datoteke (DOC, DOCX, XLS, XLSX, PPT i tako dalje). One mogu da sadrže ranjive makroe; ako se traži da omogućite makroe u Word dokumentu, razmislite dvaput pre nego što to uradite.

Budite oprezni i kod fajlova sa prečicama (.LNK ekstenzija). Windows može da ih predstavi kao bilo koju ikonu koja, u kombinaciji sa nevinim nazivom fajla, može da vas namami u nevolju.

Važna napomena: Windows otvara fajlove sa poznatim ekstenzijama bez pitanja korisnika, a podrazumevano skriva ove ekstenzije u Windows Exploreru. Dakle, ako vidite fajl sa nazivom poput Important_info.txt, to bi zapravo mogao biti Important_info.txt.exe, fajl koji instalira malware. Podesite Windows da prikazuje ekstenzije kako biste bili bezbedniji.

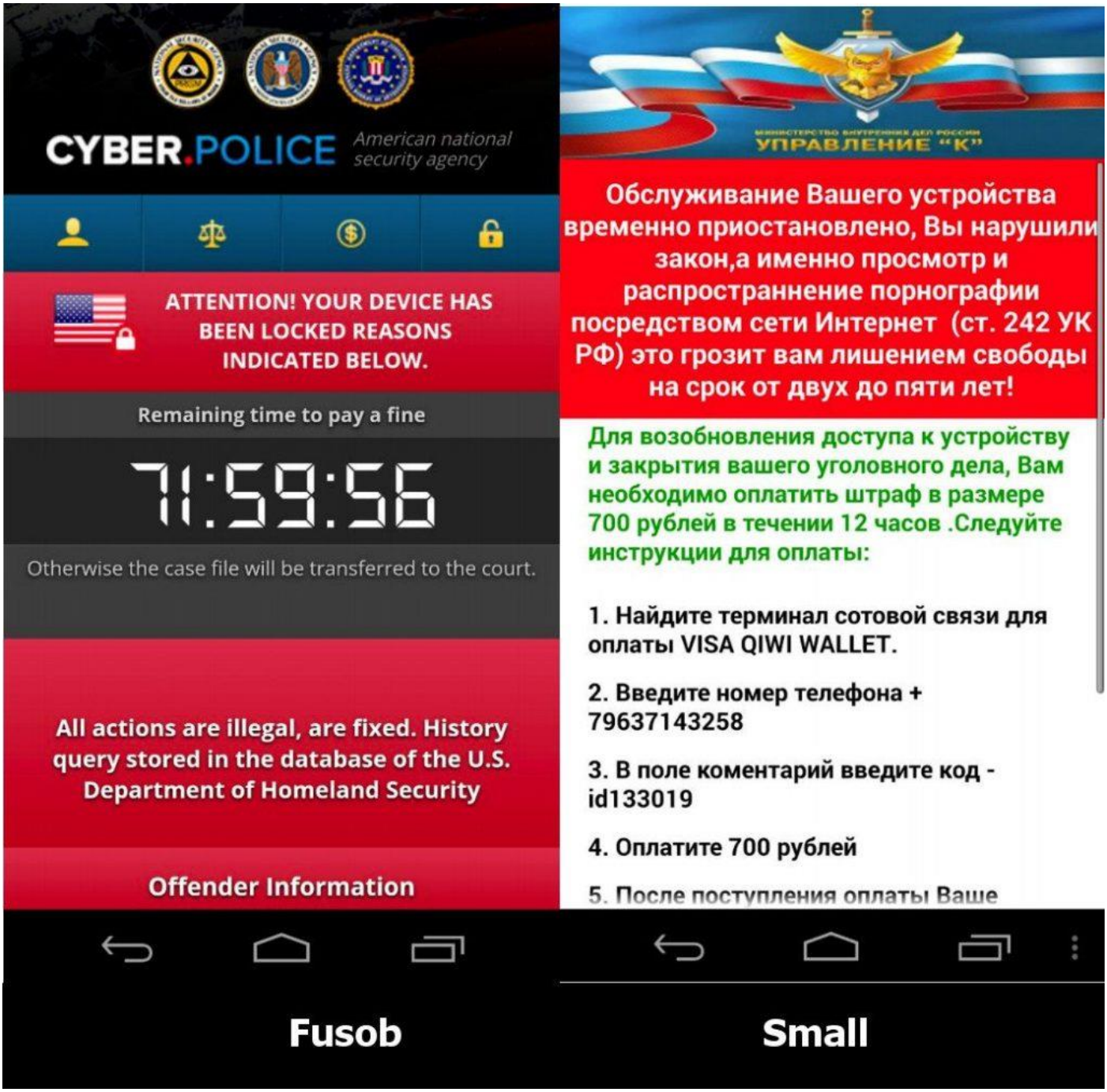
# Mogu li da izbegnem infekciju ako se držim dalje od nevaljalih web sajtova ili sumnjivih attachmenta?

Na žalost, čak i oprezni korisnici mogu da budu inficirani ransomware-om. Na primer, moguće je da zarazite svoj računar dok čitate vesti na velikom, uglednom medijskom veb sajtu.

Naravno, sam veb sajt neće distribuirati malware posetiocima – osim ako je hakovan, što je druga priča. Umesto toga, mreže oglašivača napadnute od strane sajber kriminalaca služe kao distributeri, jer njihova nezakrpljena ranjivost može dozvoliti učitavanje malware-a. I da ponovimo još jednom, redovno ažurirani softver i potpuna nadogradnja (**zakrpe**) operativnog sistema su ključni.

# Koristim telefon za surfovanje. Da li bi trebalo da brinem zbog ransomware-a na Androidu?

Da, trebalo bi. Na primer, postoje kriptori i blokeri za Android uređaje, s tim što preovlađuju ovi drugi. Imati antivirus na pametnom telefonu nije paranoično.



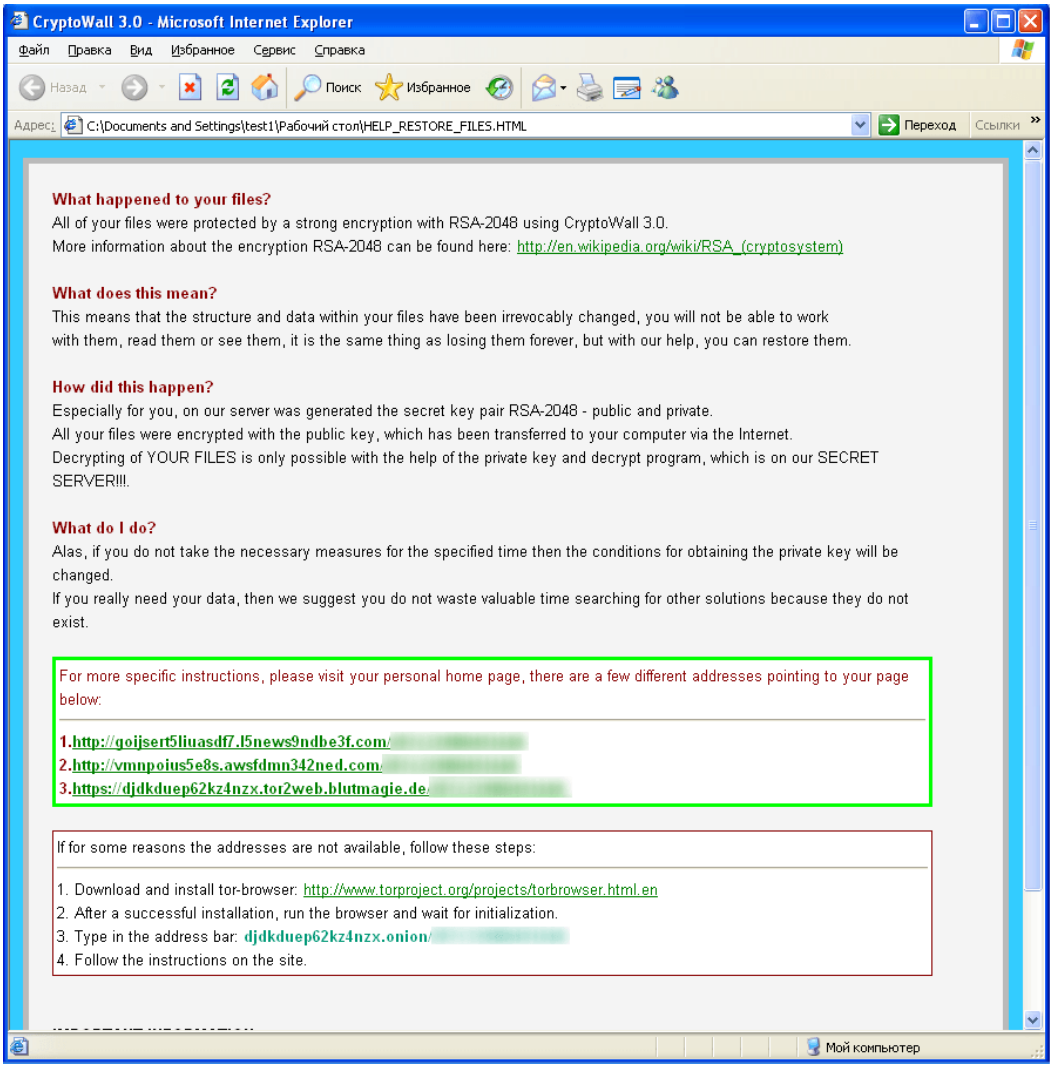

# Dakle, čak i iPhone je u opasnosti?

Do sada ne postoje ransomware programi namenjeni za iPhone i iPad. Uzgred, ovo važi za iPhone čiji operativni sistem nije otključan. Malware se može infiltrirati u uređaje koji nisu zaštićeni bezbednosnim ograničenjima iOS i Apple zaključanog App Store-a.

Ipak, iPhone ransomware može biti odmah iza ugla, i bez otključanog sistema. Možemo videti i pojavu IoT ransomware-a, takođe. Sajber kriminalci bi mogli zahtevati visoke otkupnine nakon preuzimanja pametnog televizora ili frižidera.

# Kako ću znati da li je moj kompjuter inficiran ransomware-om?

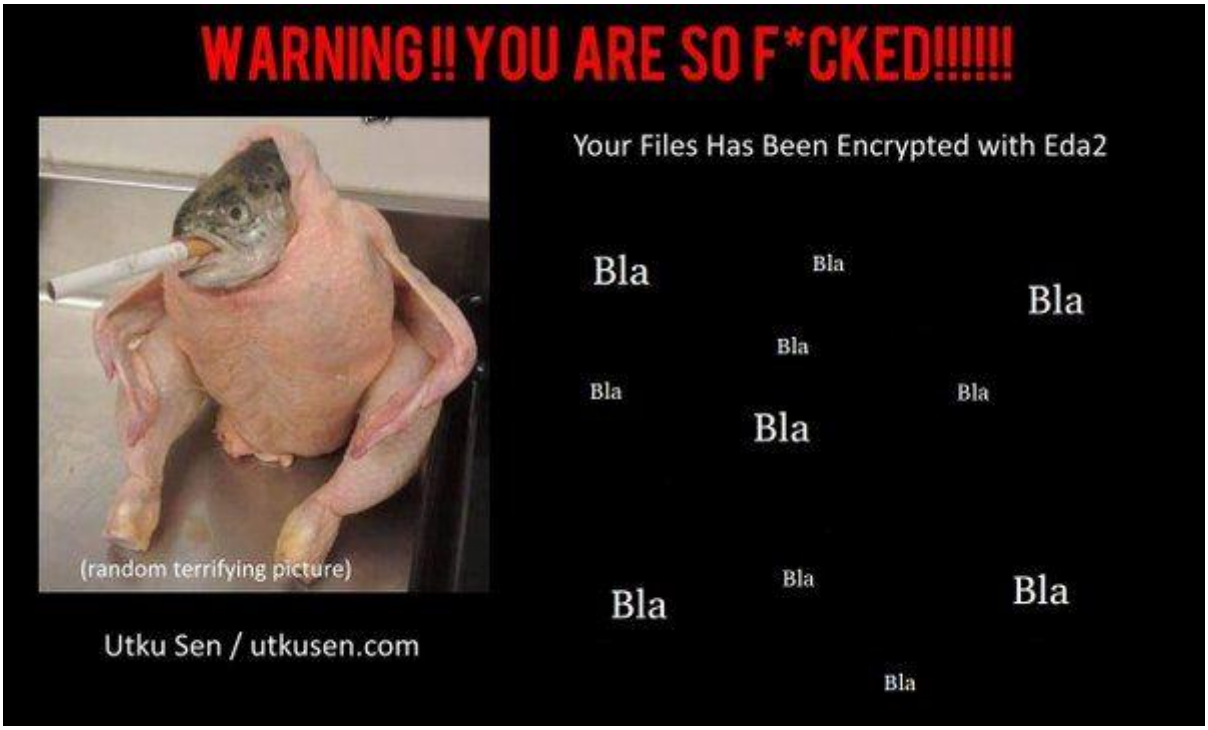
Ransomware nije suptilan. Sam će se najaviti, na primer ovako:


CryptoWall 3.0 - Microsoft Internet Explorer
Файл Правка Вид Избранное Сервис Справка
Назад Поиск Избранное
Адрес: C:\Documents and Settings\test1\Рабочий стол\HELP_RESTORE_FILES.HTML
Переход Ссылки
What happened to your files?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 3.0.
More information about the encryption RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)
What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.
How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of YOUR FILES is only possible with the help of the private key and decrypt program, which is on our SECRET SERVER!!!.
What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really need your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.
For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:
1.http://goijsert5liuasdf7.l5news9ndbe3f.com/
2.http://vmnpoius5e8s.awsfdmn342ned.com/
3.https://djdkduep62kz4nzx.tor2web.blutmagie.de/
If for some reasons the addresses are not available, follow these steps:
1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: djdkduep62kz4nzx.onion/
4. Follow the instructions on the site.
Мой компьютер

Ili ovako:


Ваши файлы были зашифрованы
Your files have been encrypted
Для расшифровки вы должны заплатить
2
To decrypt you have to pay
BITCOIN
СВЯЗЬ СО МНОЙ
CONTACT ME
dedcrypt@sigaint.org
ВНИМАНИЕ!!! WARNING!!!
Ключ для расшифровки хранится 24 часа!
The decryption key is valid 24 hours!
DED cryptor

Ili ovako:




Blokeri više izgledaju ovako:


# Koje vrste ransomware-a su najčešće?

Novi tipovi ransomware-a se pojavljuju svakog dana, tako da je teško reći koji su najpopularniji. Možemo nabrojati nekoliko istaknutih primera, poput Petya, koji enkriptuje kompletan hard disk. Takođe, tu je i CryptXXX, koji je još uvek moćan i koji smo već dva puta srušili. I naravno, TeslaCrypt je bio najrasprostranjeniji primer ransomware-a u prva četiri meseca 2016. godine; njegovi autori su, neočekivano, odlučili da objave glavni ključ (master key).

Садржај:

# 1. Основни појмови

Програм за обраду текста (текст процесор) ***Word*** је кориснички (апликативни) програм за писање, модификовање, обликовање, чување и штампање докумената. Word је саставни део програмског пакета Microsoft Office. Овим приручником ћемо обрадити верзију програма 2007 која је инсталирана на већини рачунара у Основном суду у Пожеги.

**Основни појмови Word процесора су:**

**Страна (Page)** креира се у радном делу екрана уносом карактера (слова, бројева, знакова) са тастатуре (улазне јединице). Формат стране може бити стандардне величине као што је B5, A4, A3... или нестандардне величине коју дефинише сам корисник (Custom Size). Страна може бити орјентисана усправно (Portrait) или хоризонтално (Landscape). Уобичајени стандард за величину папира у нашој земљи је A4 формат.

**Маргине** – су белине на страници, између руба текста и одговарајуће ивице папира, које ограничавају правоугани простор на папиру унутар којег се пише текст. Постоје четири маргине: горња (top), лева (left), доња (bottom) идесна (right). Стандардне маргине су 2,5 cm.

**Параграф (пасус)** је основни део текста откуцан **између два притиска Ентер** на тастатури.

**Заглавље (header) и подножје (footer)** папира је простор на страници у који се уписује текст који ће се приказивати на врху, односно на дну **сваке** странице.

**Типографија односно фонт – врста слова** је скуп знакова са истим визуелним карактеристикама. То могу бити слова, бројеви знаци интерпункције и специјални знаци. Постоји више различитих типова фонта: обична (Regular), *искошена (Italic) Ctrl+I,* **подебљана (Bold) Ctrl+B**, подвучена (Underline) Ctrl+U, као и њихове комбинације. Величина фонта се изражава у тачкама. Једна тачка износи 1/72 дела инча (1инч=2,54 cm).Подразумевани фонт у Word-у је Times New Roman, а величина 12pt, док за наслове користимо већа најчешће 14pt.

**Означавање (селектовање, маркирање**) текста у документу користимо када желимо било какву промену у документу (нпр. промену величине слова, прореда и сл.). **ПРВО МОРАМО ОЗНАЧИТИ ДЕО ТЕКСТА У ДОКУМЕНТУ КОЈИ ЖЕЛИМО МЕЊАТИ.** Означавање вршимо мишем или тастатуром.

По извршењу наредбе текст се демаркира кликом у белину радне површине.

**Ознавање текста помоћу миша**

Цео документ Притиснемо и држимо тастер Ctrl и кликнемо било где на леву маргину.
Пасус (параграф) Двоструки клик испред пасуса или троструки клик на пасус.
Ред Кликнемо на почетак реда
Реченица Притиснемо и држимо тастер Ctrl и кликнемо било где у реченицу.
Реч Двоструки клик било где у реч

Без ограничења Поставимо показивач (курсор) на почетак текста притиснемо и држимо леви тастер миша и вучемо преко текста који желимо селектовати

**Означавање текста помоћу тастатуре**

Цео документ Притиснемо и држимо тастер Ctrl и кликнемо тастер A

Без ограничења Позиционирамо се на почетак текста, притиснемо и држимо тастер Shift и користећи тастере за кретање (стрелице) селектујемо жељењно слово, реч, реченицу или пасус.

**Корисне пречице помоћу тастатуре (Први тастер држите, други се притисне једном)**

**Alt+Shift –** Промена тастатуре
**Alt+F4 –** Затварање активне ставке или излазак из програма или искључивање рачунара
**Ctrl+S** – Чување тренутне датотеке или документа
**Ctrl+C** – Копирање изабране ставке
**Ctrl+X** – Исецање изабране ставке
**Ctrl+V** – Лепљење изабране ставке
**Ctrl+Z** – Опозив радње
**Ctrl+B** – Подебљана слова (Bold)
**Ctrl+U** – Подвучена слова (Underline)
**Ctrl+I** – Накренута слова (Italic)
**Ctrl+L** – Лево поравнање
**Ctrl+R** – Десно поравнање
**Ctrl+E** – Обострано поравнање
**Ctrl+P** – Штампање
**Ctrl+N** – Отварање новог празног документа
**Ctrl+F, Ctrl+G, Ctrl+H** – Налажење задате речи и мењање жељеном (Find and Replace)
**Ctrl+O** – Отварање документа који већ постоје (мења команду File-Open)
**Ctrl+P** – Штампање
**Ctrl+A** – Селектовање целог документа
**Esc** – Отказивање тренутног задатка

## 2. Покретање програма

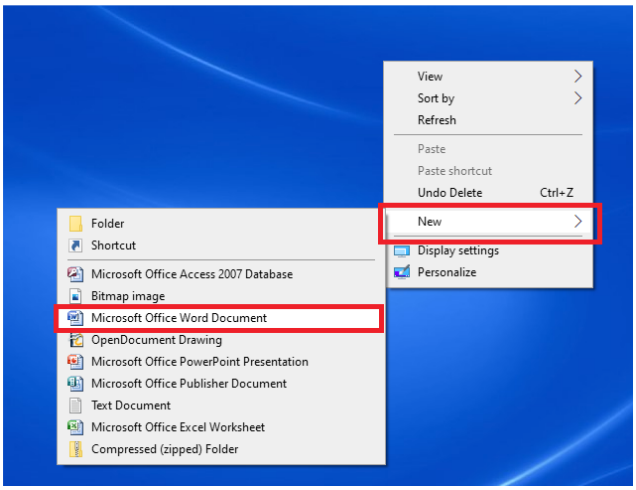
Постоји више начина да покренете Word:

1. Кликнете на Start  (Win 10) -> Microsoft Office -> Microsoft Word или

 (Win7) Start ->All Programs-> Microsoft Office-> Microsoft Word.

2. Уколико је на Desktopu извучена икона програма двокликом на њу покрећете програм. Пречица за Word 

3. Кликнути десни тастер миша на радну површину или неком фолдеру где желите да сачувате нови Word документ, из плутајућег менија станите показивачем миша на команду New, отвориће се додатни мени из листе понуђеног бирате New Word document.



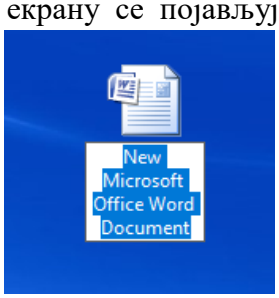

(Напомена: **све пречице имају стрелицу у доњем левом углу**. Пречица не представља сам програм или документ већ указује рачунару на путању како да стигне до одредишта које она представља. Често се дешава приликом нпр. копирања података са флеша да кликнемо десни тастер миша и бирамо комаду Send to Desktop чиме кажемо рачунару да направи пречицу селектованог фајла на десктопу. Онда када уклонимо флеш, рачунар није у могућности да отвори фајл, јер путања указује одредиште коме он више нема приступ, јер је уклоњена са рачунара).

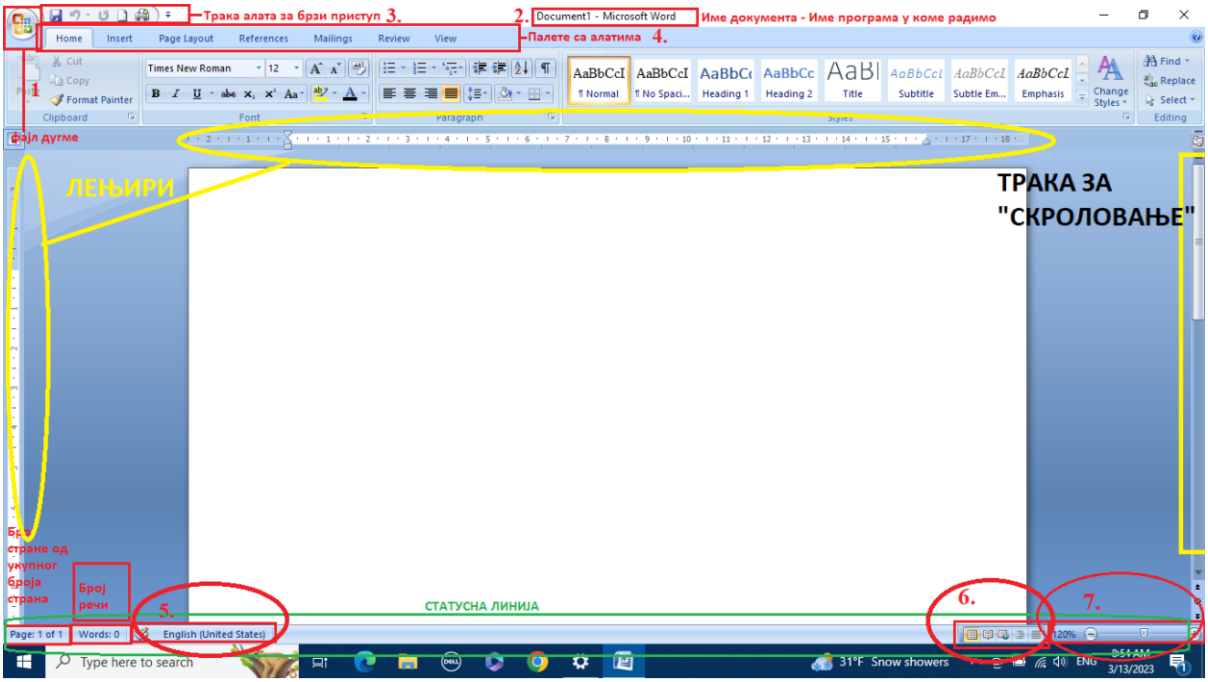
3. Уколико је већ отворен Word са палете брзи приступ бира се следећа иконица 

После покретања програма Microsft Word, на екрану се појављује прозор који се састоји из радног дела (радне површине) и дела за команде (линије менија и линије са алатима).

## 3. Елементи радног окружења програма Word

После покретања програма Microsoft Word, на екрану се појављује прозор који се састоји из радног дела (радне површине) и дела за команде (линије менија и линије са алатима).






1. Office(File)дугме

2. Име документа – Име програма у коме радимо

3. Трака са алатима за брзи приступ

4. Палета са алатима

5. Лењири

6. Трака за померање

У оквиру статусне линије приказано је следеће:

5. Број странице у документу од укупног броја страна

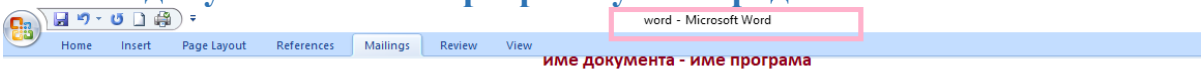
6. Број речи у документу Кликом на број речи добијамо информацију колико у документу има страна, речи, карактера тј. слова са и без размака, пасуса и линија односно редова текста.

7. Језик документа

8. Начин приказа документа

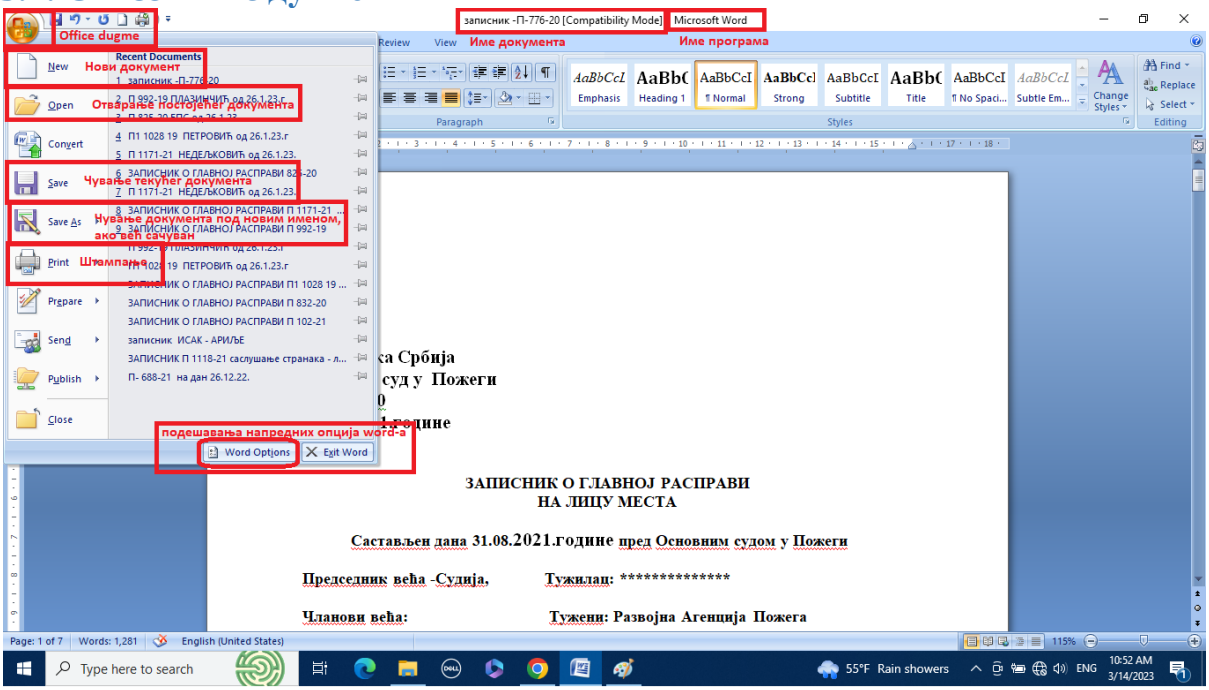
9. Увећавање или умањење документа

## 3.1. Име документа – Име програма у коме радимо




На насловној линији уколико је документ сачуван писаће име документа у коме радимо, као и назив програма, у нашем случају word.

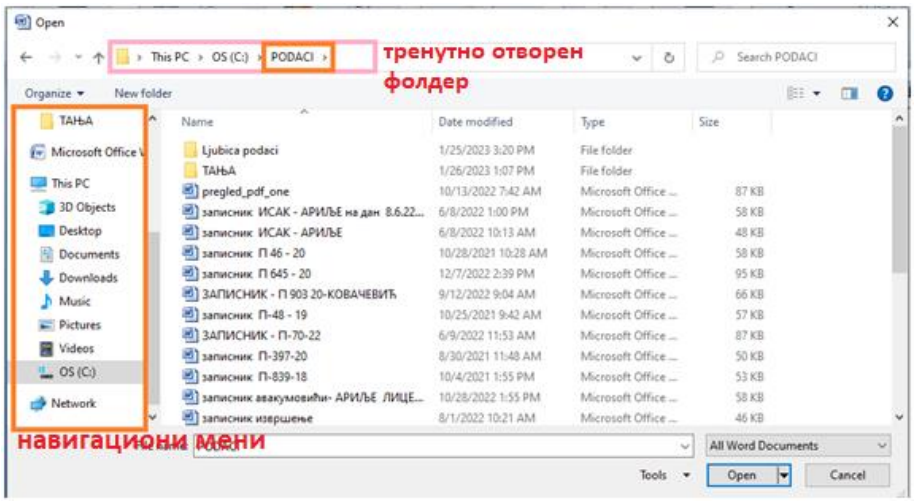
## 3.2. Office – File дугме




Кликом на дугме фајл отвара се следећа падајућа листа команди:

### 3.2.1. New – Отварамо нови неименовани документ ***(Ctrl+N)***

### 3.2.2.Open – Отвара се плутајући прозор из кога бирамо који документ желимо да отворимо, такође кликом на фајл дугме у десној колони понуђено 17 документа који су последњи отварани у програму Word. ***(Ctrl+O)***



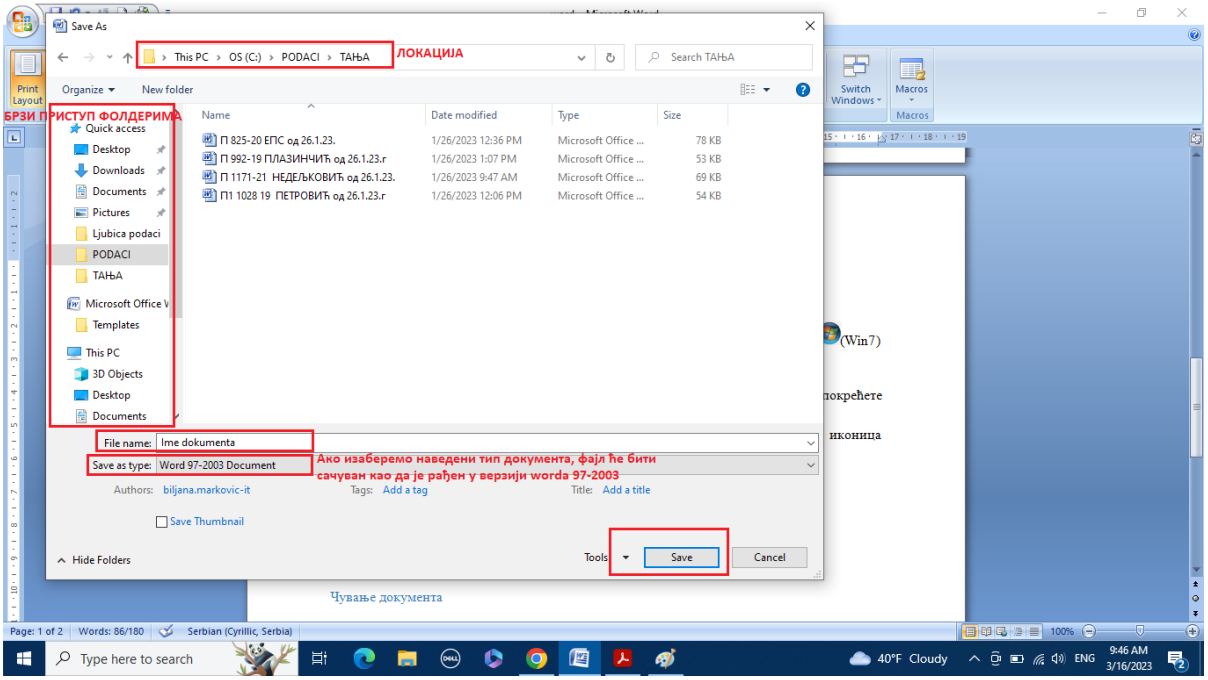

### 3.2.3. Save – Чување документа ***(Ctrl+S)***

Документ можемо да сачувамо командом Save, којом чувамо тренутну позицију у документу. Када применимо команду Save на документ коме још нисмо дали име, прво одређујемо име и место где ћемо да сачувамо.

Документ чувамо на следећи начин:

1. Office Button – Save

2. Кроз навигациони мени отворимо фолдер у коме желимо да сачувамо документ




3. У пољу поред опције File name упишемо жељено име

4. У пољу Save as type бирамо формат у коме желимо да сачувамо (моја препорука је чувати као Word 97-2003 Document, јер ће свака новија верзија програма отворити старију што обратно није случај).

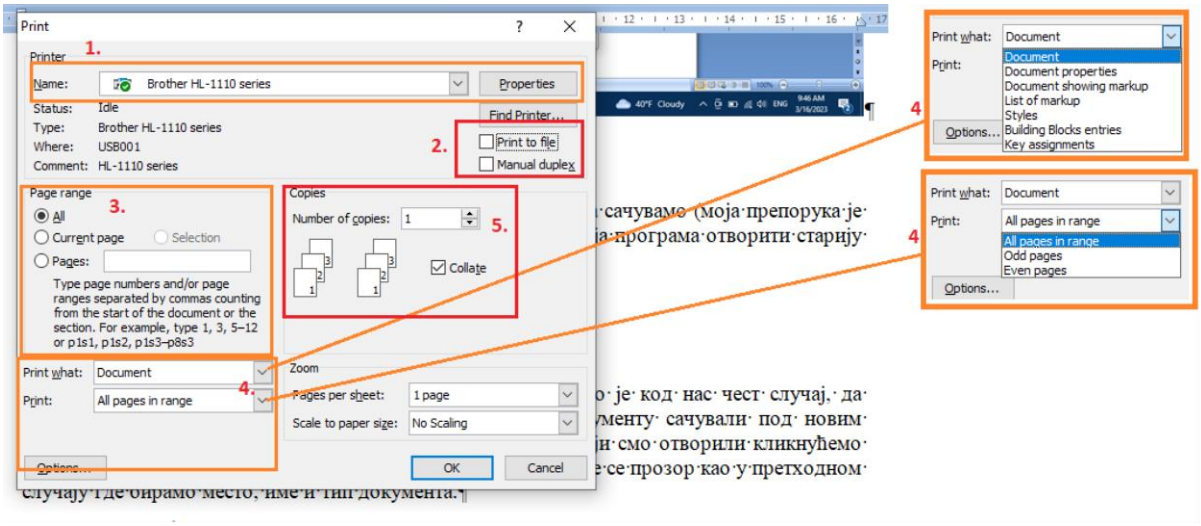
5. Кликнемо на дугме Save или притиснемо тастер Enter

### 3.2.4. Save As – Чување под новим именом

Ако куцамо нови текст преко већ отвореног документа, што је код нас чест случај, да бисмо све промене које смо направили у постојећем документу сачували под новим именом и притом сачували изглед првобитног документа који смо отворили кликнућемо на дугме Fajl и бирати команду Save As (Сачувај као) отвориће се прозор као у претходном случају где бирамо место, име и тип документа.

### 3.2.5. Print – Штампање ***(Ctrl+P)***

Кликом на команду **File – Print** отвара се нови прозор где бирамо шта, на ком штампачу и на који начин штампамо.




Под бројем ***1.*** бирамо штампач на коме желимо да одштампамо документ, у продужетку је дугме својства (Properties) изабраног штампача.

Често се дешава да случано чекирамо кућицу означеном бројем 2. Print to file, уколико је она чекирана када кликнемо Ок за штампу, документ се неће одштампати него ће се отворити дијалог прозор за чување документа, јер смо му то и дали команду да штампа у фајл, а не на штампачу. Друга кућица Manual duplex, уколико имамо једнострани штампач ако чекирамо ту кућицу, штампач ће одштампати само непарне странице и захтевати да одштампан папир вратимо у штампач и задамо команду за наставак штампе и нема потребе да сами наводимо све непарне, па онда парне странице за штампу.

Под бројем ***3.*** бирамо које стране желимо да штампамо – All – Све стране, Current page – Тренутну страну која се приказује, Pages – У овом пољу наводимо које стране желимо да одштампамо. Њих наводимо број стране – зарез – размак – следећа стр. за штампу или опсег страна које желимо одштампати раздвојене средњом цртом нпр. 3-5.

Под бројем ***4. Print what*** наводимо шта све желимо да се одштампа, па тако поред документа можемо одштампати и особине документа (Document properties) односно где је сачуван документ на рачунару колико има речи, страна... Такође под бројем ***4. Print*** можемо да наведемо да ли штампамо све (All) стране у документу, непарне (Odd pages) или парне (Even pages) странице.

Када смо изабрали на који начин и на ком штампачу желимо да штампамо кликнућемо ОК.

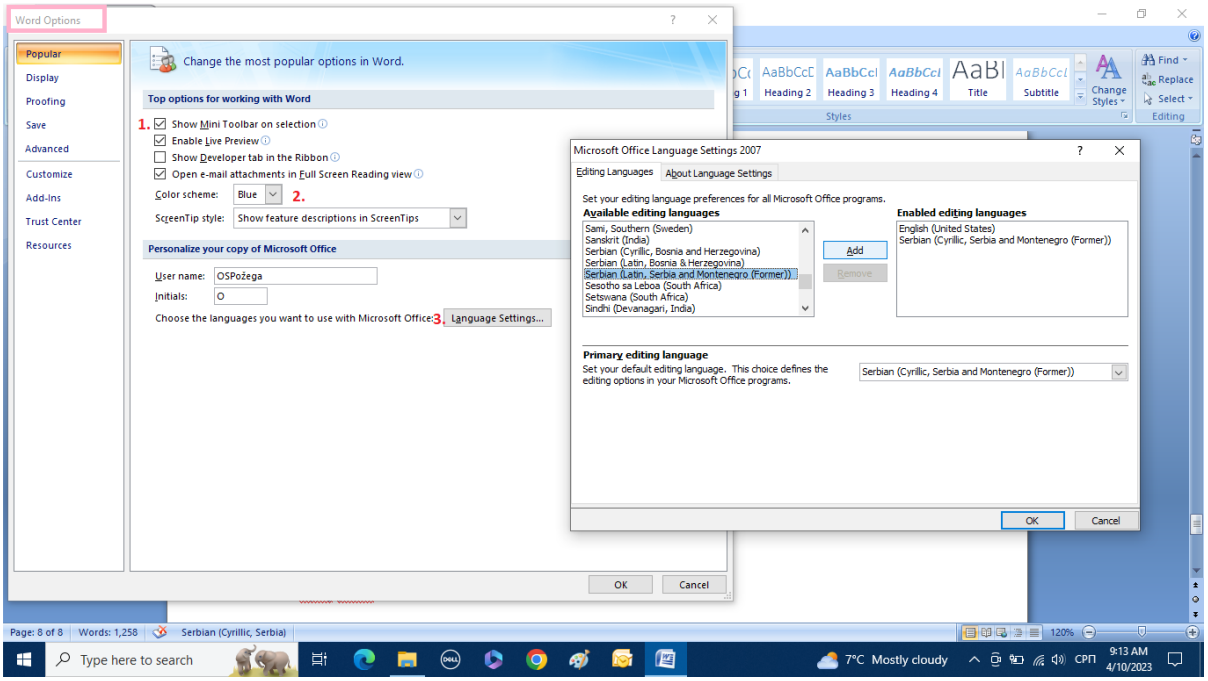
### 3.2.6. Close – Затварање програма (Alt+F4)

Поред ове команде за затврање програма File-Close, документ можемо затворити на добро познат X у горњем десном углу Word прозора или са тастатуре комбинацијом контролних и функционалних тастера – **Alt+F4**. Уколико постоје неке несачуване промене документа, приликом затварања програм ће нас питати да ли желимо да сачувамо настале промене, уколико кликнемо на *Yes* сачуваћемо промене у том документу. Уколико желимо да документ сачувамо под другим именом кликнућемо *Cancel* и онда поступити по већ описаном поступку чувања документа под другим именом.

## 3.2.7. Word Options – Напредне опције програма Word

Кликом на File дугме и бирањем команде Word Optons отвара се нови плутајући прозор као на слици. Нећу описивати команде које се ретко или никад не користе.

### Popular

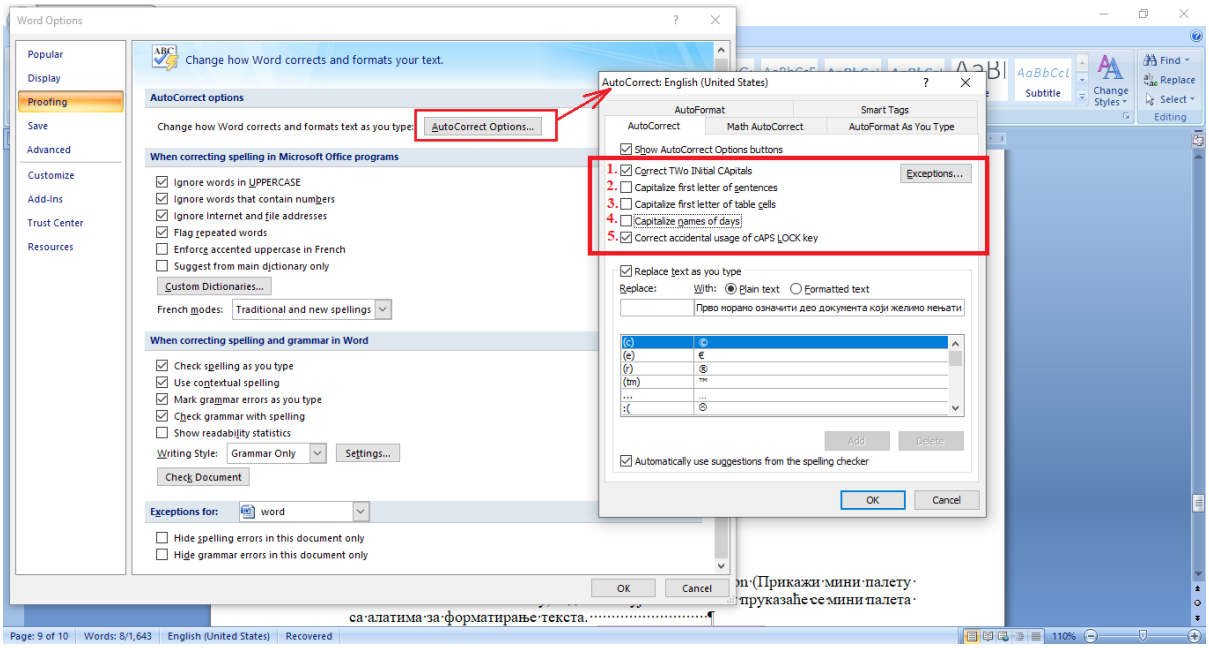



1. Уколико је чекирана опција Show Mini Toolbar on selection (Прикажи мини палету алата на селектованом тексту, када селектујете неки текст пруказаће се мини палета са алатима за форматирање текста.


2. Color scheme – Бирамо боју Worda,

3. Language settings… - Уколико су иза неке команде три тачке то значи да се кликом на њу отвара нови плутајући прозор, као што је у овом случају. Овде бирамо језик који желимо да користимо у word-у. Уколико нека реч није на бираном језику, програм ће је подвући црвеном или зеленом бојом.

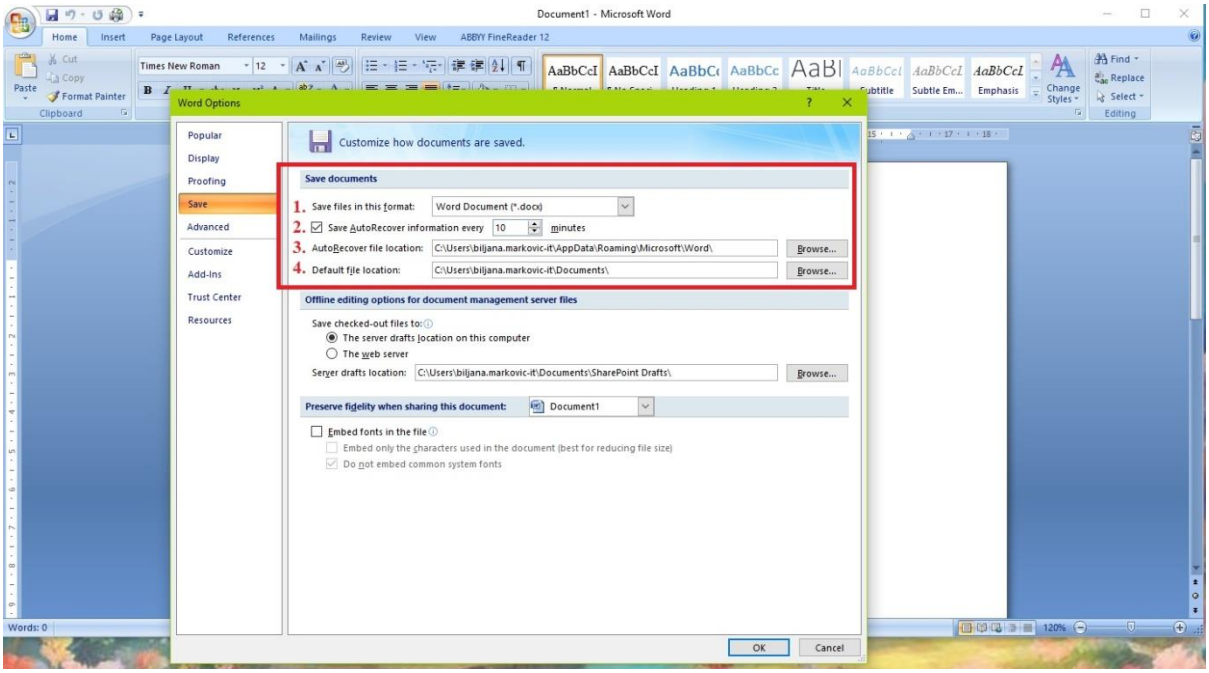
## Proofing



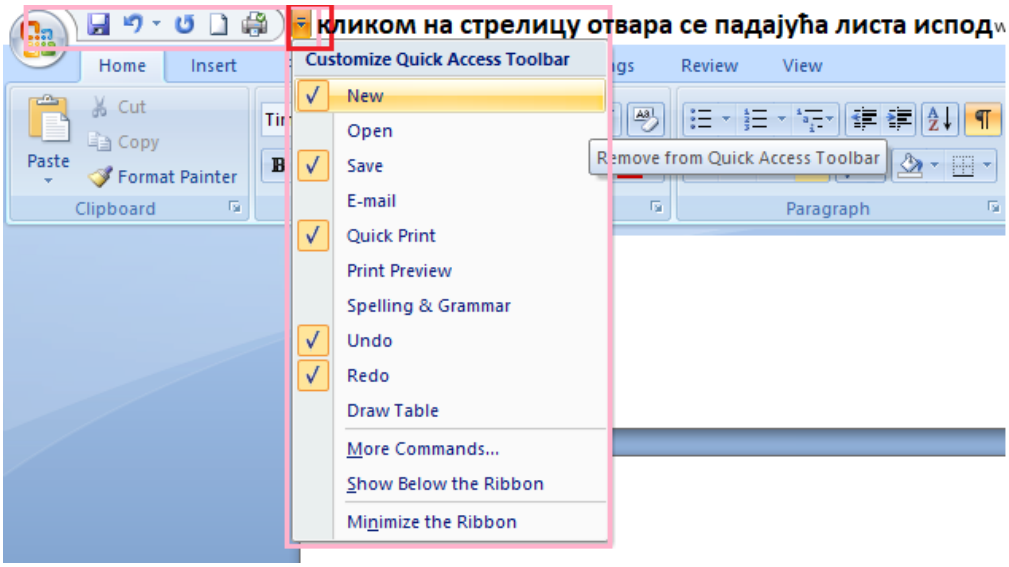

На овој картици у опцији AutoCorrect Options... се може подесити да Word аутоматски ради следеће:

1. Исправља грешко откуцана два велика слова у речи
2. После тачке велико почетно слово наредне речи
3. У ћелији табеле прво велико слово речи
4. Велико почетно слово имена дана
5. Исправља случајно укључена велика слова.

## Save



## 3.3. Трака са алатима за брзи приступ

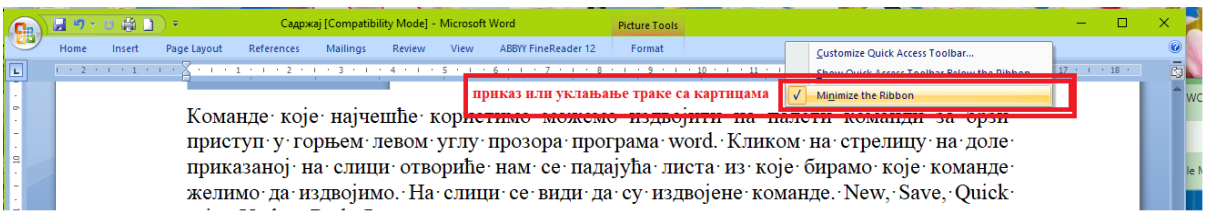



Команде које најчешће користимо можемо издвојити на палети команди за брзи приступ у горњем левом углу прозора програма word. Кликом на стрелицу на доле приказаној на слици отвориће нам се падајућа листа из које бирамо које команде желимо да издвојимо. На слици се види да су издвојене команде. New, Save, Quick print, Undo и Redo.

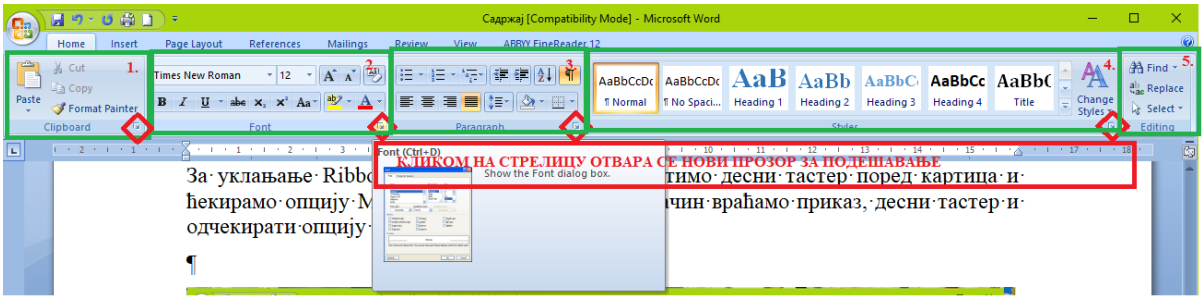
## 3.4. Трака са картицама (Ribbon)

Ribbon (трака) садржи више табова (картица) на којима се налазе групе команди, потребне за обављање уобичајених задатака. Неке групе команди садрже стрелице помоћу којих отварамо још доступних команди. Риббон се може уклањати и постављати, а постоји могућност да корисник дефинише и дода свој таб (картицу) на траку.

За уклањање Ribbona са радне површине користимо десни тастер поред картица и ћекирамо опцију Minimize the Ribbon, на исти начин враћамо приказ, десни тастер и одчекирати опцију Minimize the Ribbon.



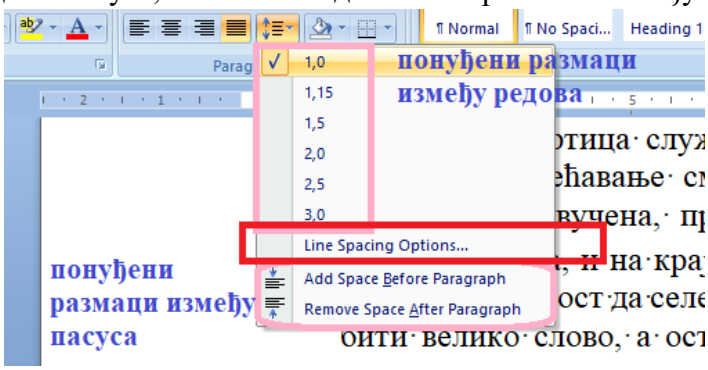
### 3.4.1. Home




У **Word** 2007 као и у осталим апликацијама у **Office** 2007 команде су организоване у траку /**Ribbon**/. Сваки **Tab** је подељен на групе.

**Home Tab** садржи групе : Clipboard, Fonts, Paragraph, Styles и Editing.

1. **Clipboard** – привремена меморија. Уколико се нешто налази у привременој меморији на команду Paste ћемо налепити у документу, на месту где се налази курсор.
2. **Font** – Ова картица служи за форматирање карактера у тексту. Врсте Fonta, величине, повећавање смањивање слова, брисање форматирања, подебљана, закошена, подвучена, прецртана, затим слова у индексу или степену, боја позадине слова, и на крају боја слова. Иконица Aa служи за мењање слова, па постоји могућност да селектовани текст променимо у реченицу, где че иза тачке бити велико слово, а остала мала слова, затим сва слова претворити у мала, затим сва слова претворити у велика, затим следећа команда у свакој речи прво ће бити велико и последња команда почетно слово сваке речи ће бити мало.
3. **Paragraph** – форматирање пасуса тј. праграфа прве три иконице су за набрајање, следеће две за увлачење првог реда пасуса или извлачење у односу на остале редове пасуса. Затим за сортирање по азбучном реду, приказ скривених знакова (размак, ентер, прелом стране итд..). Следећа група од четири иконе су за поравнање текста у пасусу. Иконица служи за подешавање размака између редова пасуса, као и за подешавање размака између пасуса. Опција Line Spacing

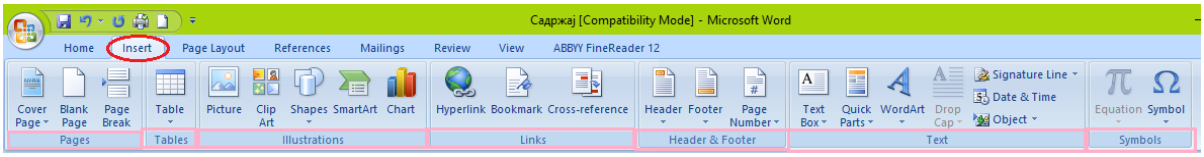



Options... отвара нови прозор за додатна подешавање пасуса.

4. **Styles** – Стилови су значајан део Microsoft Word апликације који нам омогућавају брзо, једноставно и конзистентно уређивање текста (а касније и аутоматско креирање садржаја). Стил је скуп особина које примењујемо над неким текстом (одломком). Те особине укључују боју текста, ефекте попут задебљања и подвлачења, боју позадине одломка, величину прореда, размак након сваког одломка, понашање одломака једних наспрам других и још много тога.

5. **Editing** – У овој групи се налазе комаде за проналажење (Find) одређеног објекта или речи у документу, као и команда за замену пронађене речи (Replace). Команда (Select) служи за селектовање целог документа, одређених објеката или текста са сличним форматирањем.

### 3.4.2. Insert




**Insert Tab** садржи групе: Pages, Tables, Illustrations, Links, Header & Footer, Text и Symbols

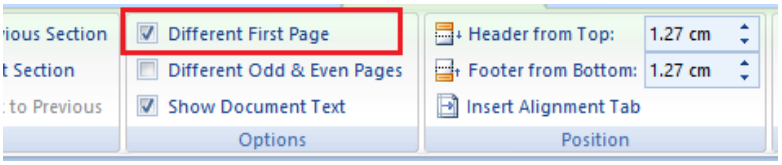
1. **Pages** група наредби се састоји од три дугмета: Cover Page: Служи за уметање насловне стране (Word 2007 има унапред урађене различите насловне стране). Blank Page: Служи за уметање празне странице, Page Break: Помоћу ове наредбе курсор прелази на следећу страницу.

2. **Tables** група садржи падајући мени из којег можемо уметнути табелу на више: Користећи се графичким алатом који нам омогућава да унесемо табелу до 10 x 8 поља. Уношењем свих потребних параметара табеле у подмениј Insert Table. Нацртати табелу помоћу опције Draw Table. Импортовањем радног папира из Excela помоћу опције Excel Spreadsheet. Користећи се готовим табелама из базе MS Office-а помоћу опције Quick Tables.

3. **Illustrations** – У овој групи се налазе команде за додавање слика, облика или графикона. Притиском на дугме Picture отвара нам се прозор помоћу којег додајемо слику користећи се Windows Explorer "стаблом". Дугме Clip Art отвара базу сличица који су део инсталационог пакета MS Office. Све сличице су разврстане по категоријама, тако да је претрага базе веома једноставна. Smart Art опција је први пут представљена у везији 2007 MS Office-а. Помоћу ње можемо лако и ефективно да прикажемо шематски приказ неких података. Поред великог броја облика, можемо подешавати боје, величину, сенке, 3D приказ, итд. Опција Chart има велику базу дизајна графикона, са могућношћу измене скоро свих елемената графикона: од облика, боја, па све до густине скале, подешавања x и y осе графикона, позадине графикона итд. Ова опција је везана за неку табелу, чије податке приказујемо на графикону.

4. **Links** у овој групи имамо три команде: **Hyperlink** – Служи за постављање линка који отвара друго место у документу, нови документ web страницу. **Bookmark** – Служи за постављање „маркера" у документу (меморишемо место у документу ради лакшег поновног проналаска тог места). **Cross-reference** – Представља унакрсно повезивање или упућивање на неки део текста.

5. **Header & Footer** У овој групи се налазе команде за креирање и уређивање горњег и доњег заглавља, као и нумерисање странице. У бази података се налазе разни built-in узорци за заглавља, а што се тиче опција у Page Number менију, можемо подесити положај бројева, фонт, број почетне странице, итд. Када не желимо број стране на првој страни чекирамо опцију Different First Page.



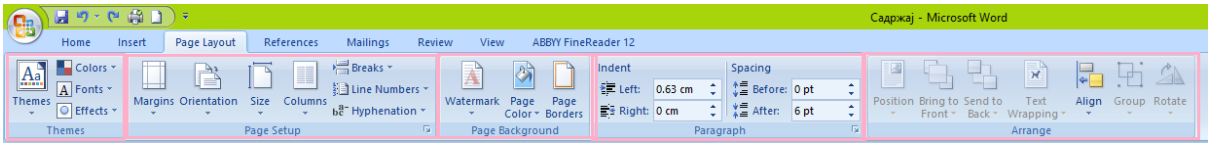

6. **Text** – Ова група служи за додавање разних елемената текстуалног дела документа. Садржи команде за додавање следећих елемената: Text Box: претходно ограничен простор за унос текста (могуће је подешавати разне опције у подменију Format...) Quick Parts: унапред одређене речи (назив компаније, број телефона, име аутора, итд.) Word Art: унос текста посебног дизајна који је уграђен у Word. Drop Cap: наглашено (увећано) означено слово. Signature Line: унос дигиталног потписа. Date&Time: убацивање тренутног времан и датума. Object: унос објеката из другог програма.

7. **Symbols** – Ова група наредби састоји се из две опције: Symbol i Equation. Symbol се користи за унос симбола који нам нису доступни са тастатуре. Equation се користи за унос формула и једначина, ради што прегледнијег приказа сложених израза.

### 3.4.3. Page Layout

Картица Page Layout вам омогућава да контролишете изглед вашег документа у програму Microsoft Word 2007. Можете да примените глобални дизајн на документ користећи једну од доступних тема и шема боја. Такође можете променити оријентацију документа, величину странице, маргине, увлачење, проред и поставке пасуса.

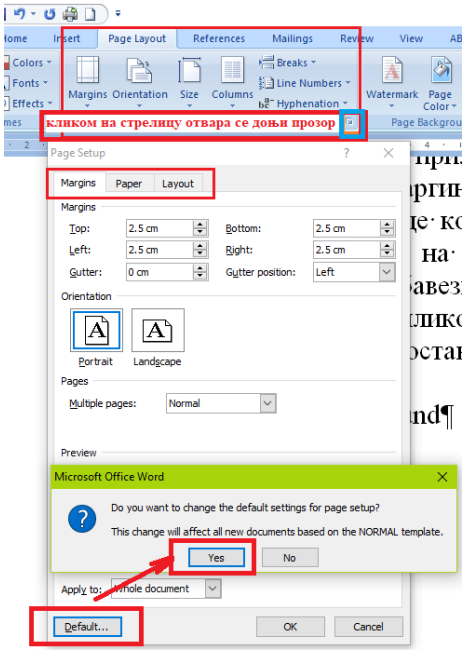
Када кликнете на картицу Page Layout приказује се следећи мени,



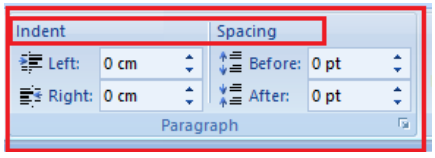

који садржи пет група команди и то Themes, Page Setup, Page Background, Paragraph i Arange.

1. Themes – Теме су унапред дефинисане и омогућавају да се промени цео дизајн стране користећи комбинацију боја, стилова, фонта и ефеката форматирања. Теме се неће применити на текст ако немамо дефинисан стил. Прво се мора са картице Home изабрати скуп стилова за цео документ. Пошто су теме подешене да раде са стиловима који се користе у документу потребно је изабрати стил за све наслове, поднаслове итд.

2. Page Setup – Подешавање странице су пареаметри које дефинише корисник, који помажу да се одреди како ће се одштампана страница појавити. Ти параметри могу укључивати све, од величине, маргина, оријентације странице и квалитета штампе. Још једноставније, то је алатка која омогућава корисницима да промене и прилагоде величину и изглед једне странице или целог документа. Прописане маргине за судске одлуке су 2,5cm, размак између редова је 1, осим за изреку пресуде код које је проред 1,5. Тип фонта Times New Roman величине 12pt. Такође на овој картици бирамо оријентацију папира (Портретно или пејзажно), обавезно променити величину папира на A4 да не би дошло до проблема приликом штампе. Када једном подесите жељене параметре странице можете их поставити као подразумеване за сваки нови документ на следећи начин:

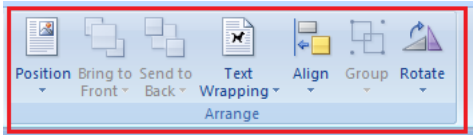



3. Page Background – На овој картици подешавамо позадину стране, можемо поставити водени жиг, променити боју листа папира и оквир стране.
4. Paragraph – као што се може форматирати размак између редова у документу, тако можемо одабрати опције размака између сваког пасуса, наслова и поднаслова. Додатни размак између пасуса додаје нагласак и чини документ лаким за читање.

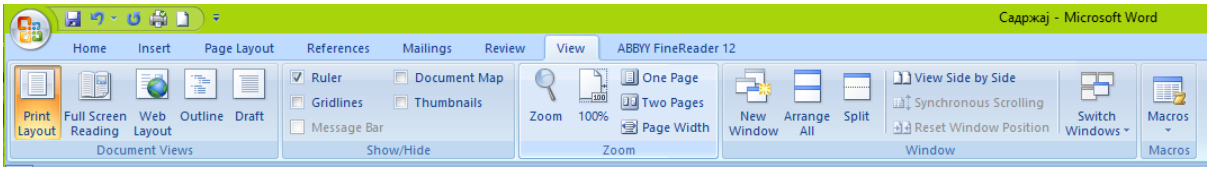



Испод Identa одређујемо колико ће пасус бити увучен са леве и десне стране у односу на маргине документа. Испод Spacing одрешујемо који размак ће бити пре и који после пасуса (Before i After) изражен у pt.

5. Arange – Ова картица служи за подешавање поравнања слике у односу на текст и страницу.



### 3.4.4. View




Картица садржи следеће групе команди Document Views, Show/Hide, Zoom, Window и Macros од којих се две најчешће користе. А то су Document Views и Zoom.

Картица Document views пружа могућност различитом приказа документа најчешће се користи Print Layout

На овој картици у групи команди Show/Hide можемо укључити приказ лењира, мапе документа, мреже итд.

## 4. Форма

Текстови се могу обликовати на два начина и то:

- у блок – форми (америчкој),

- зупчастој форми (француској).

Блок форма је једноставнија за обликовање, јер има одмах рачунарску понуду. Њене карактеристике су да се наслов и текст куцају у блоку тј. од почетка већ унапред одређене леве маргине. Пасуси се одвајају један од другог са два откуцаја - Ентер. На овај начин се углавном раде вежбе, те је блок форма донекле савладана.

Зупчаста форма има карактеристику: наслов се куца на средини, а пасуси се одвајају увлачењем новог реда за одређени број откуцаја од унапред одређене леве маргине. За увлачење пасуса се користи табулатор.

Пример писма у блок – форми:

Неговање радне културе

Основни задатак сваке области васпитања, а пре свега умног васпитања, јесте да дајући ученицима основу оних знања, навика и умења која ће им бити неопходна у животу, истовремено оспособљава сваког ученика за даље самостално стицање нових знања. Неопходно је неговати и развијати радну културу сваког ученика, сваког човека. Култура умног рада је саставни део сваке радне културе и укључена је у њу.

Пример писма у зупчастој форми:

Формирање навика и умења

Навике су аутоматизоване делатности које човеку омогућавају да са мање утрошка снаге и енергије и уз мање ангажовање свести брже и тачније обави једну радњу. Навике увек почивају на одређеним знањима. Иако до одређене мере ослобађају човекову свест, основа су за стицање нових знања.

Умења (вештине), као и навике, почивају на знањима. Она су такође резултат вежбања. Међутим, за разлику од навика умења су сложеније радње које још нису аутоматизоване. Ангажовање свести у њима је знатно. По томе умења обично претходе навикама и чине једну етапу у њиховом формирању.