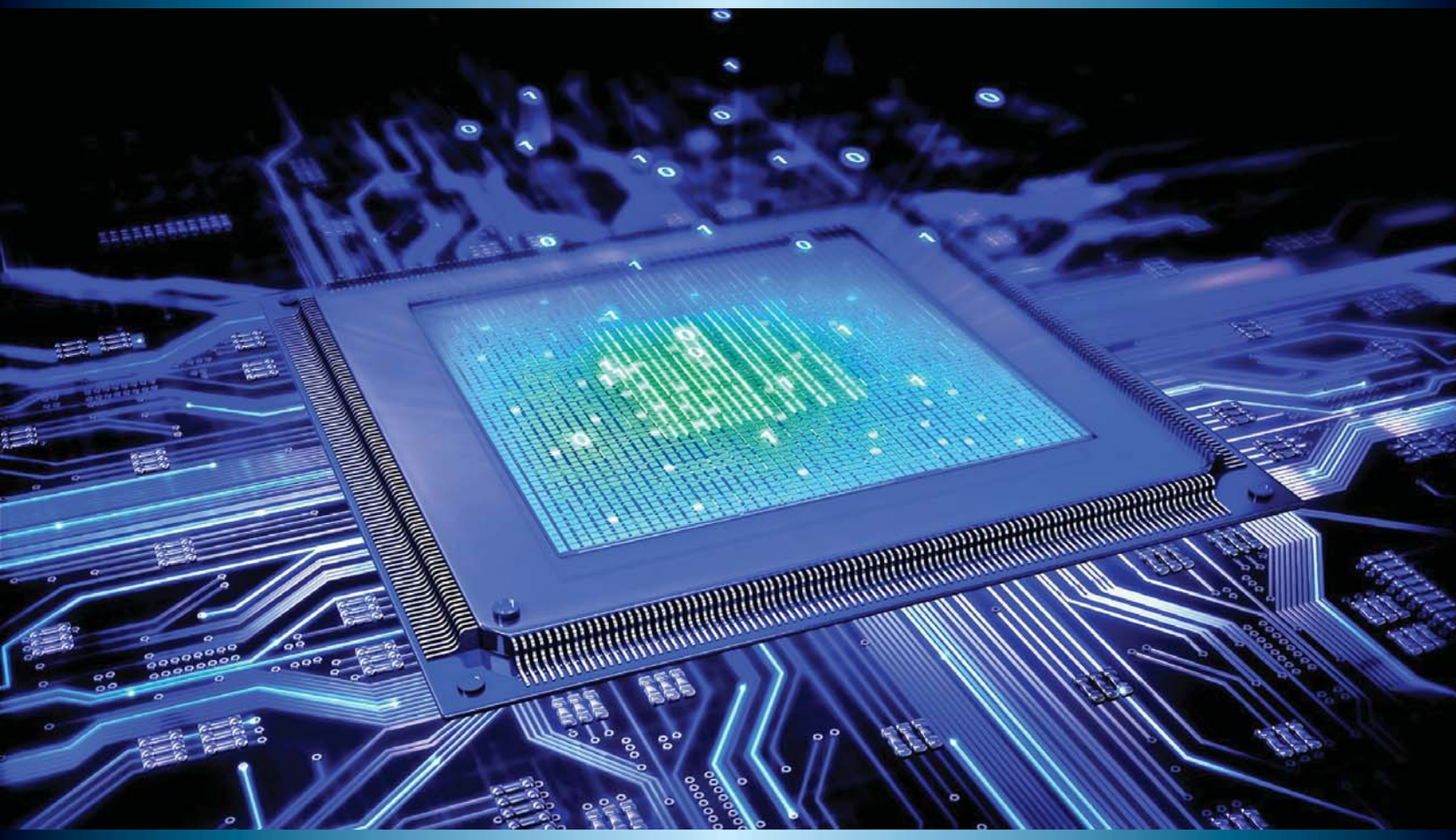
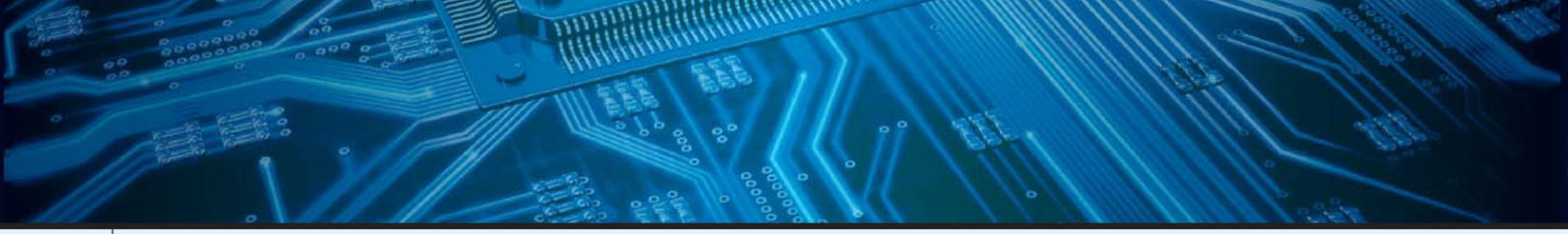
ОДБРАНА

Специјални прилог 103

# ИСКУШЕЊА И ИЗАЗОВИ МОДЕРНЕ ИНФОРМАЦИОНО-КОМУНИКАЦИОНЕ ТЕХНОЛОГИЈЕ



Пише Милорад Маркагић



# ИСКУШЕЊА И ИЗАЗОВИ МОДЕРНЕ ИНФОРМАЦИОНО-КОМУНИКАЦИОНЕ ТЕХНОЛОГИЈЕ

**Од почетка развоја људске мисли и издвајања човека од осталих примата у посебну категорију интелигентних и свесних бића, јавила се и потреба за разменом информација и употребом неког медија као носиоца података, јер непосредни контакт, који се најчешће и данас користи, није био довољан за потпуну комуникацију, размену, чување и заштиту података. У круговима уметника и стручњака из области телекомуникација и криптографије честе су дискусије о томе да ли прачовеково изражавање, кроз пећинско сликарство, представља само уметнички израз осећања, или и неки вид преноса и заштите информација.**

Развојем писма на светску сцену ступила је и размена информација ван блиског контакта, а самим тим и њихова заштита на неком материјалном носиоцу, као што је папирус, пергамент или папир, па све до данашњих електронских медија. Такође, сведоци смо и многобројних начина преноса информација на приручним или за то посебно употребљеним средствима – заставицама, удараљкама од шупљег балвана, бубњевима, димним сигналима, роговима....

За почетак развоја средстава модерних телекомуникација узима се средина 19. века, када је остварен први бежични пренос порука. Био је то Морзеов први пренос телеграфског сигнала између Балтимора и Вашингтона, чиме се пренос сигнала у електричном облику сврстава у ред основног носиоца информација.

Развојем научне мисли и технолошким достигнућима, средства телекомуникација и информационих технологија до данашњих дана достигла су такав стадијум да је комуникација између појединаца, група или држава постала незамислива без коришћења великог броја информационо-телекомуникационих средстава. Свакако, у најчешћој и најмасовнијој примени су телефони и рачунари.

## Средства и системи у свакодневној употреби

Не може се извршити стриктна подела структуре средстава која се данас користе у комуникацији, преносу, чувању и заштити информација, јер су, вртоглавим развојем информационих технологија, многа класична средства и средства за једну намену добила друге карактеристике и сврстала се у мултиконверзацијске уређаје и системе. Та строга подела свакако и не би имала смисла, осим у теоријским разматрањима, јер је огроман број функција данас смештен у само једном уређају.

Ипак, основна намена, без обзира на ниво развоја, диктира и поделу средстава на неколико категорија или група, од којих су у најмасовнијој употреби фиксни и мобилни телефони и персонални рачунари.

## Фиксна телефонија

Без обзира на брзи напредак средстава информационо-комуникационе технологије, фиксни (стабилни или кућни) телефони су и даље у масовној употреби. У односу на првобитне телефонске централе и телефонске апарате, садашња технологија омогућила је да се кућни телефон користи, осим за пренос гласа, и за пренос порука и мултимедијалних садржаја по истом воду или каналу.

Предности тог вида комуникације су, свакако, ниска цена и лака доступност опреме за комуникацију, како за индивидуалну, тако и за масовну употребу. Недостаци се односе на статичност употребе, развијање скупе инфраструктуре и веома лако праћење и прислушкивање саобраћаја од трећих лица, уз минималну могућност сазнања да се комуникација прати, прислушкује или снима.

Наравно да су и за ту врсту (овлашћеног или неовлашћеног) праћења комуникације потребни инфраструктура, кадрови, опрема и испуњење низа других предуслова, нарочито због тога што је за обављање тог посла неопходан и физички приступ преносном путу.

## Мобилна телефонија и рачунари

Једноставно коришћење, широк избор уређаја, релативно јефтина и мања потреба за инфраструктуром, омогућили су да мобилни телефони данас постану саставни део живота, како за пренос гласовних порука, тако и за пренос текста, слике, графике, а у последње време и праћења мултимедијалних садржаја.

Последња генерација паметних телефона има скоро све одлике мини-рачунара.

Тај вид комуникација подложнији је утицају треће стране, како за пресретање и праћење, тако и за ометање уз употребу широког спектра опреме за надзор, прислушкивање, ометање или обмањивање.

Савремени рачунари јављају се у неколико облика, од којих су у најширој употреби сервери, персонални десктоп или лаптоп рачунари, а у последње време и таблет рачунари.

Употреба тих средстава, осим за информатичку делатност, веома је раширена и за масовну комуникацију и пренос података.

## Облици комуникације

Различити су видови комуникације, али ћемо се задржати само на неколико најосновнијих и најчешће коришћених. Млађе генерације већ су усвојиле појмове попут: електронска пошта, месенџер, скајп, ВОИП, причаоница, чет, блог, друштвена мрежа и сл.

Глобална мрежа – интернет, лако доступна, једноставна за коришћење, јефтина и распрострањена у целом свету, брише границе класичних контаката и доприноси повезивању људи и компанија на светском нивоу уз минимална улагања, а нажалост и минимална знања и предзнања из области правилне употребе и заштите на мрежама.

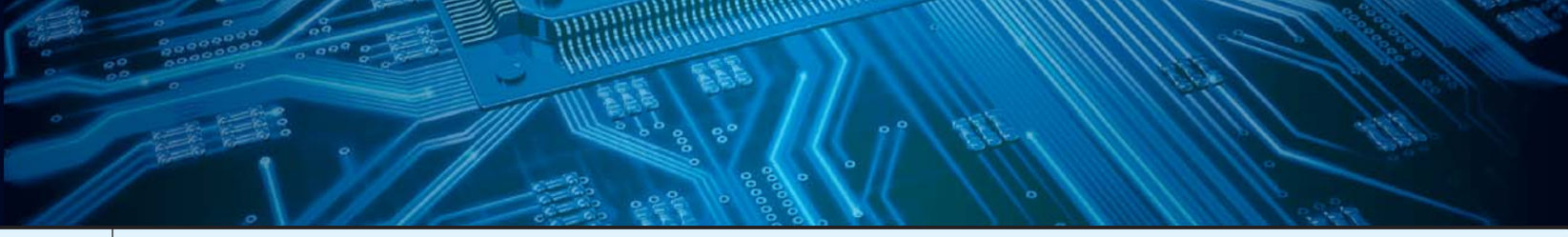
> Пратећи кашњење до три најближе базне станице одређује се тачан положај корисника на одређеној територији, чија се прецизност мери до неколико десетина метара. Телефон се може активирати и без знања власника, даљински, софтверским путем, што омогућава праћење целокупног телефонског саобраћаја који се обавља, па чак и праћење догађаја у непосредној околини корисника који се прислушкује. При томе, праћеном субјекту скенирају се фонетске карактеристике, тако да се, приликом следећег прислушкивања, чак и ако у међувремену дође до замене претплатничког броја, или телефонског апарата, у бази података веома лако може сазнати о којој особи је реч.

Неколико светских гиганата у области софтверске технологије, укрупњавањем организација и ширењем пословних мрежа по целом свету, користи савремене развојне резултате и кроз апликативне софтвере омогућава да се једним логовањем на било коју мрежу може приступити великом броју домена.

Такав начин доприноси да се једним приступом и коришћењем једне апликације сви налози могу пречицама међусобно повезати. Самим тим је и могућност долазака до личних података, уплива у мрежна логовања и крађе идентитета постала лак плен злонамерним корисницима интернета.

## Прислушкивање и праћење комуникације

Информације о могућностима, средствима и распрострањености праћења и прислушкивања фиксних и мобилних комуникација процуре, обично, поводом неких афера или се ради о релативно маскираним, али ипак јавно саопштеним обавештењима о начину до-



Познато је да се сва опрема за надзор и заштиту комуникација у скоро свим земљама света сматра пословном или неком другом тајном, а да, истовремено, све више држава доноси законе, којима својим операторима фиксне и мобилне комуникације налажу да пружају услуге владиним органима за спровођење прислушкивања телефонског и интернет саобраћаја, што истовремено значи и да владе више немају потребу за набавком уређаја за прислушкивање и дешифровање у реалном времену.

На светској сцени непрекидно је у порасту трка у осавремењавању прислушним уређајима, нарочито у безбедносним и полицијским службама, јер криминалци за међусобну комуникацију веома често користе нерегистроване бројеве, мењају телефонске апарате или користе телефоне за једнократну употребу. Да би се некако пратили сумњиви токови у илегалним операцијама, обавештајне и безбедносне структуре често су принуђене да прате целокупно фреквентно подручје. Опрема се најчешће смешта у возила, ради повећане мобилности оператера – прислушкивача. Без обзира на то који модел и коју картицу праћено лице користи, прислушкивачи очитају његов кориснички број чим прође поред возила за надзор.

Недостатак те методе јесте у томе да прислушни симулатор базне станце региструје све бројеве мобилних телефона, а не само праћеног субјекта, тако да често може доћи до неповољних реакција појединаца, или организација, због угрожавања приватности. Управо због тога је у великом броју земаља под строгу законску контролу стављена опрема за прислушкивање мобилних телефона, која је знатно напреднија у односу на класичну методу прислушкивања фиксних комуникација.

Када је о овим другима реч, прислушкивање је знатно једноставније и не изискује мобилност оператера, већ се врши у стационарним условима. По томе је познат пример обавештајне службе Босне и Херцеговине, која у међуразделнику у пошти у Сарајеву, по неким тврдњама, дневно прати и више од 500 телефонских прикључака. (Међуразделник или помоћни разделник јесте паралелна форма главном поштанском разделнику, на коју се, без опасности, може физички прикључити опрема за надзор и снимање.)

ласка до информација, најчешће када су у питању кривична дела или политичком пропагандом мотивисани догађаји, везани за одређени субјекат. Та се појава манифестује кроз два облика, у зависности од тога да ли податке пласира појединац, који има сазнања или сумња да је праћен и прислушкиван, или их, пак, даје надлежна државна, обавештајна, полицијска или судска служба. Сведоци смо свакодневних, некада лажних, али веома често недемантованих објава прислушкиваних разговора, најчешће коришћених у политичке или корупционашке сврхе и афере.

Међутим, било да се ради о процесима са судским епилогом, или се они заврше на нивоу медијског нагађања, скоро је незамисливо да се истовремено појави и извор, метода или начин долазака до тих информација. Због тога су и сазнања о начину прислушкивања и техничким средствима коришћеним за ту намену, ако их уопште и има, веома штура и непотпуна. Покушаћемо, зато, без залажења у етичке норме прислушкивања, да објаснимо неке појавне облике (зло)употребе података, који се добију прислушкивањем телефонских комуникација.

Развојем интернета и његовом лаком доступношћу широкој популацији, омогућена је и његова злоупотреба у различите сврхе, па и у сврху понуде разних електронских уређаја за надзор, прислушкивање или одбрану од њих, који су, често, само плод манипулација због могућности лаке зараде.

## Превентивно деловање

Како на подручју превентивне полицијске делатности, тако и на подручју истражних радњи и судских вештачења из области телекомуникација, постигнут је значајан напредак у законској регулативи тајног надзора телекомуникација. У Европи, као и у већини суседних земаља, донети су прописи у складу са Резолуцијом Савета Европе о законском тајном праћењу телекомуникација и одговарајућим регулативним нормама Европског института за телекомуникационе норме – ETSI.

Према одредбама тих прописа телекомуникациони и мрежни оператери су обавезни да, о свом трошку, граде уређаје за надзор у своје мреже и осигурају њихово одржавање и исправан рад за потребе Оперативно-техничког центра за надзор телекомуникација. Такође, операторима се налаже да, осим садржаја телефонских позива, дају на увид и све остале податке о позивима, односно време и датум успоставе, или покушаја успоставе везе, прекиде позива, промене статуса, услуге, локације корисника итд. Све такве податке морају чувати, а сва сазнања о средствима, поступцима и подацима примене мера надзора обавезни су да чувају као државну тајну. Поред свега, оператери морају да обезбеде да надзирана или било која друга неовлашћена особа не осети промену која би могла бити узрокована применом мера надзора и прислушкивања.

Тачан број телефонских претплатника који су под повременим или трајним надзором никада не изађе у јавност, али се поуздано зна да се у опрему за наведене намене, у зависности од величине земље и броја становника, улаже од неколико милиона до више десетина милиона долара.

Познато је да се сви подаци, које поседују оператери и пружаоци услуга, дају на увид полицији, службама безбедности и војсци, а користите се и током кривичних предистражних и истражних радњи. Телефонске компаније тврде да немају ништа против да дају свој допринос борби против криминала, али негодују због огромних трошкова. С друге стране, корисници телекомуникационих услуга су забринути и оправдано страхују да ће они и платити највећи цех, не само кроз додатно по-

скупљење импулса, већ и због угрожавања њихове личне безбедности.

Појавом новијих генерација, пре свега мобилних телефонских апарата, појам класичног прислушкивања губи своју првобитну намену. Сваки апарат има шеснаестоцифрени идентификациони број, тако да свака нова картица, која се укључи у апарат, само допуњује већ стечена сазнања о кориснику апарата.

Пратећи кашњење до три најближе базне станице одређује се тачан положај корисника на одређеној територији, чија се прецизност мери до неколико десетина метара. Телефон се може активирати и без знања власника, даљински, софтверским путем, што омогућава праћење целокупног телефонског саобраћаја који се обавља, па чак и праћење догађаја у непосредној околини корисника који се прислушкује. При томе, праћеном субјекту скенирају се фонетске карактеристике, тако да се, приликом следећег прислушкивања, чак и ако у међувремену дође до замене претплатничког броја, или телефонског апарата, у бази података веома лако пронађе о којој особи је реч.

## Заштита приватности

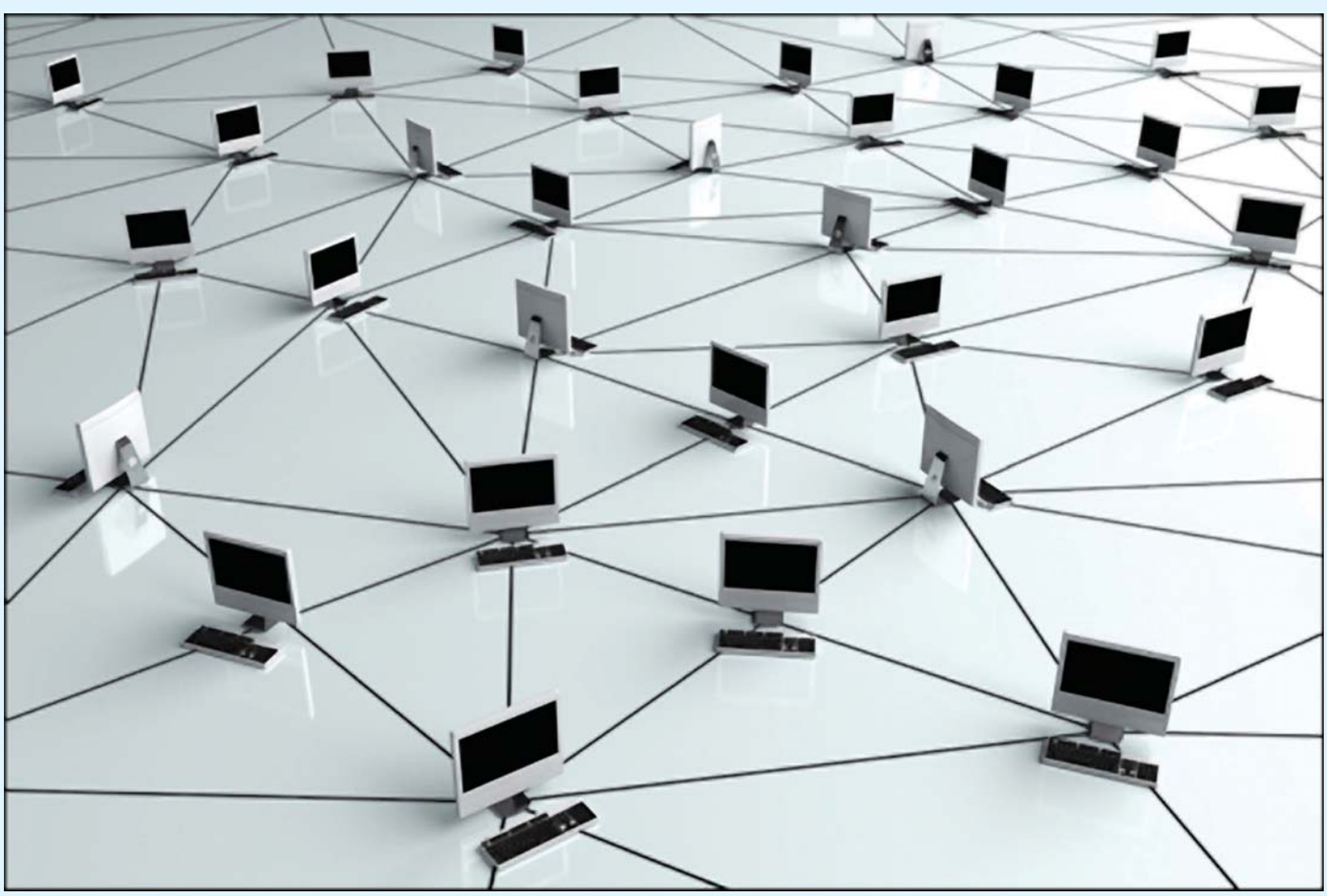
Проблему заштите приватности појединци, али и велики број компанија, посвећују се најчешће када дођу до сазнања да су и сами били жртве неког вида криминала, или ако примете већа одступања у коришћењу средстава ИКТ комуникације, што је најчешће већ знак да је касно да се реагује и могу се само санирати или отклањати последице. Неретко се дешава да су последице толико катастрофалне да је немогуће опорављање система или уређаја, а о губитку података излишно је и говорити.

Заштити комуникација путем јавних телефонских мрежа и мобилних мрежа могуће је приступити на више начина, али су најширем кругу корисника бројне методе и софтверска решења већином непознати и недоступни, па им се, као најефикасније, може саветовати и најдрастичније решење. У току приватних или службених разговора путем отворене комуникације треба што мање користити поверљиве податке и разговарати што је краће могуће. Ипак, ако уоче необичне појаве – промену тона у слушалици, појаву неуобичајених шумова, повремене „клик" или „бип" тонове, чудне звукове, брзо пражњење батерије и слично потребно је да одмах прекину разговор.

Организације и државни органи имају могућност набавке хардверских и софтверских решења за заштиту говорних података, али је та заштита често скупа или људство није довољно оспособљено за правилну примену поступака, па често долази до „цурења" информација без намере и знања корисника.

Чести су случајеви намерног праћења, прислушкивања и ометања телефонског саобраћаја, али су најмасовнији они које изводе појединци ради забаве или вршења злонамерних радњи према кориснику, методама случајног избора жртве.

Савремени мобилни телефони, такозвани паметни телефони, садрже ин-




Имајући у виду да су палтформе креиране тако да се „паметним телефонима" може телефонирати, слати поруке у текстуалним или мултимедијалном облику, приступити глобалној мрежи – интернету, да је до сада познато преко 250.000 апликација за додатно инсталирање на њима, може се закључити да је коришћење тих телефона за пренос поверљивих података неадекватно, те да се они могу користити само за отворени вид комуникације.

сталиране оперативне системе и преузимају улогу микрорачунара, тако да, осим сновне намене преноса говорних информација, имају улогу и преносног рачунара, са минималним ограничењима интерфејса и дела хардверских компоненти који их и издвајају од класичних рачунара.

## Заштита рачунара

Последња сазнања о праћењу комуникација на глобалном нивоу, повезана са досадашњим искуствима из области деловања хакера и осталих начина уплива у мреже и персоналне рачунаре, изискују потребу свеобухватног сагледавања тог проблема, враћању неким основним постулатима коришћења рачунара и мрежа и додатно оспособљавање појединца, као основне карике у коришћењу рачунара.

Рачунар је састављен од неколико компоненти, међу којима су кућиште за смештај делова, са хардвером за напајање, хард-диск, матична плоча са процесором, графичка картица, меморија, звучна картица, модем, оптички уређај (CD или DVD), мрежна картица, миш, тастатура и екран – класични монитор или дисплеј рачунара.

Свака компонента има своје место и улогу у коришћењу машине, али је за разматрање, у смислу заштите података, довољно да се фокусирамо на неколико основних, које служе за манипулацију, смештај и пренос података.

Хард-диск чини саставни део сваког рачунара и најкоришћенији је медиј за чување података. Чине га следећи елементи: магнетне плоче (носачи података), магнетне главе (читачи података), мотор и електроника.

За функционисање хард-диска, поред његових саставних компоненти, значајан је и програм – firmware који је задужен за синхронизацију рада магнетних плоча, глава и електронике. Неисправност сваке од компоненти хард-диска, као и firmware-а, може довести до губитка података.

Хардверски проблеми на хард-диску могу се јавити у следећим облицима: неисправна глава, електроника, мо-

тор, firmware и оштећење плоче (појава такозваних Bad sector-а).

Флеш USB дискови и меморијске картице настали су из потребе да се створе мали, издржљиви, отпорни на механичке утицаје и преносни уређаји за чување података.

У својој структури, веома једноставни и без покретних делова, мотора и глава, лаки за манипулацију, истиснули су из употребе хард-дискове за употребу у мобилним уређајима.

Мане тих меморија јесу осетљивост на електрична пражњења и ограничен број уписа у сваку меморијску локацију. Ти уређаји састоје се од контролера и меморије. У највећем броју случајева долази до отказа контролера.

Због врло мале употребе и ограничених ресурса и капацитета нећемо посебно разматрати флопи дискете и CDили DVD дискове, иако и они још увек имају своје место у чувању података.

На поменутим медијима за обраду, чување и пренос података, потребно је извршити низ радњи како би се извршила екстерна или интерна заштита података. На интерном нивоу могу се размотрити сви видови ограничења приступа, физичке заштите, криптовања фајлова и коришћење лозинки за важније податке. Екстерна заштита доста је компликованија и захтева, како познавање метода и поступака, тако и употребу одговарајућих софтверских алата.

Било да је реч о појединцу, компанији или државној установи, предмет уплива треће стране најчешће су материјална корист или откривање тајних података.

## Губитак и спасавање података

Важно је знати да ниједан медиј, без обзира на квалитет, структуру или произвођача, није имун на отказе и кварове. Зато је неопходно да се у свакој ситуацији врши backup података. Губитком података сматра се сваки вид недоступности података кориснику, било да је реч о механичком или софтверском проблему.

Губици података настају из више разлога и на више начина, а примарни и најчешћи су: губитак партиција, губитак због дејства вируса и осталих малициозних програма, губитак после реинсталације оперативног система или после намерног или ненамерног брисања фајлова, губитак услед оштећења база података и услед оштећења e-mail база.Такви кварови често се називају и логичким кваровима.

Најчешћи разлози немогућности спасавања обрисаних података су: дуго време које је протекло од брисања података до покушаја спасавања, нестручан покушај спасавања података, вишеструко форматирање ХДД и коришћење неадекватних алата. У зависности од медија са којег се врши спасавање података, користи се и метод, односно алат који је примерен том материјалном носиоцу информације.

Постоје и неки изузеци; SD картице (мини и микроверзија) не поседују контролере, а неки уређаји имају енкриптоване стране у оквиру меморија које је немогуће декриптовати у случају отказа контролера.

Методе и поступци спасавања података са електронских медија усмерени су на поступак којим се копира садржај медија којем није могуће приступити на уобичајен начин, на неки други медиј, попут HDD, SSD, флеш меморије, меморијске картице, RAID система, NAS – Network Attached Storage, CD/DVD, флопи диска, ЗИП и ЈАЗ драјв.

Без обзира на то који је медиј и која је врста квара у питању, спасавање података врши се тако што се пресликава целокупни садржај неисправног медија на други исправан медиј. То пресликавање назива се „клонирање" и обавља се употребом специјалних хардверских алата који омогућавају потпун приступ медију и свим његовим параметрима. Након клонирања, ископирани садржај на клону анализира се и на њему се примењују различити софтверски алати како би се подаци спасили.

## Намерно уништавање података

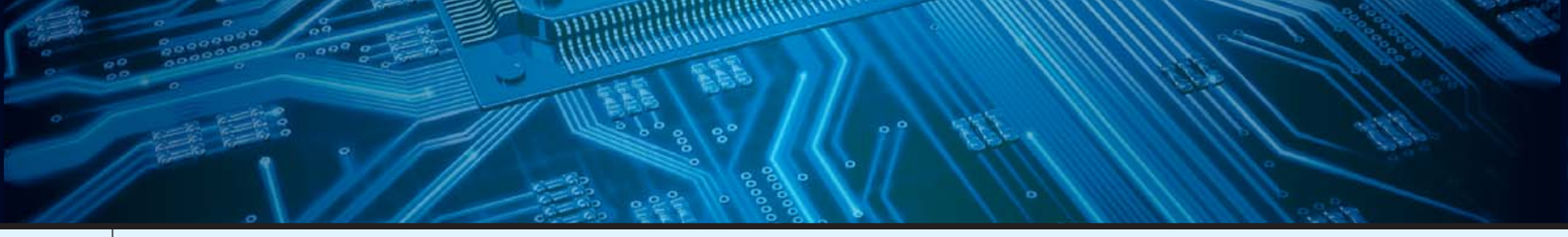
Под губитком података, осим логичких и ненамерних узрока, подразумева се и намерно уништавање непотребних, искоришћених или података који због стављања медија ван употребе морају бити уништени. Ако се узме у обзир да податак у најопштијем смислу представља скуп јединица и нула, који се смештају на одређеном носиоцу, логично се намеће и питање – како намерно и трајно избрисати и уништити податке?

Ако бисмо сматрали да се брисањем фајла или фолдера и његовим простим уклањањем са медија податак доиста брише, или уништава, дошли бисмо у заблуду, јер једноставна чињеница да брисање траје вишеструко краће од уписа указује на то да оно није уклонило податке са медија, већ га учинило само тренутно невидљивим.

Трајно брисање података могуће је извршити уписом нових садржаја преко старих и коришћењем софтверских алата, чишћењем диска, дефрагментацијом или употребом неког од лиценцираних програма ван оперативног система. То је могуће извести само на исправним медијима, али и тада треба имати у виду да су развијени алати који могу извршити повраћај података са медија и након вишеструког уписа и брисања, као и након реинсталације оперативног система или форматирања преносног медија.

Други вид уништавања података, најчешће коришћен када се медији стављају ван употребе или се врши њихова прерасподела унутар компаније, јесте демагнетизација. То је процес брисања података јаким магнетним пољем. Де-

Чести су примери цурења информација управо када се неки од магнетних медија преда на сервис, оправку, дијагностику или у гарантном року мења новим. Корисници веома ретко воде рачуна о садржајима који су били меморисани на медију, што представља идеалан начин да се до података дође, а да то не представља криминални чин.



магнетизација је могућа на готово свим савременим уређајима за чување дигиталних података.

Када подаци више нису потребни, неопходно је заштитити их од сваког покушаја читања. Просто брисање фајлова оставља њихов садржај на медију са отвореном могућношћу повраћаја и приступа.

## Заштита на мрежи

Кад неког корисника бројних савремених средстава информационо-комуникационе технологије упитате како користи мобилни телефон, таблет, или лаптоп добијате углавном исте, или веома сличне одговоре – читам вести, проверавам е-пошту, играм игрице, дописујем се са пријатељима… Мада су такви видови коришћења ИКТ опреме тачни, нису ни близу потпуној истини. Дугачак је списак активности од којих ћемо набројати најважније и по статистици најчешће. Ту су претрага и проналажење потребних информација, размена мејлова, информације о хобијима или интересовањима, тражење места и улица, временска прогноза, читање вести, потрага за одређеним производима и услугама, бесциљно лутање сајтовима из досаде, куповина и продаја производа, слушање музике, гледање филмова, гледање видео-клипова, праћење сајтова јавних и државних институција, комуникација преко друштвених мрежа, куповина карата за путовања, концерте, спортске и друге манифестације, преглед и трансакције по текућим и штедним рачунима, тражење посла, преглед отворених енциклопедија, клађење и информисање о спортским резултатима, претрага за несталим и недоступним рођацима или познаницима, дељење фотографија, читање и писање по разним форумима, бесплатно телефонирање коришћењем једног од многих сервиса, упознавање преко многих сајтова, контрола сопственог сајта. Једном речју – „живот" у виртуелном свету...

Наравно да је списак активности много дужи и да нису споменуте оне о којима је било речи у одељку о заштити уређаја и комуникација, али свакако низ активности појединаца који су усмерени на криминалне радње (илегална трговина оружјем, наркотицима и људима, дечја порнографија, упад у уређаје појединца или компаније, па чак и државних институција, крађа новца, крађа идентитета, ширење малициозних програма...), такође показује да се на интернету време проводи и у те сврхе.

> То што не видимо нападача не мора да значи да нисмо нападнути. Идеална одбрана не постоји, али менаџери компанија могу да утичу на едукацију запослених, које уче како да препознају потенцијалне нападе и како да реагују у таквом случају, уз обавезу да се сигурносни системи у компанијама ажурирају и да се унапређују у складу са новим достигнућима.

## Сајбер криминал

У скоро свакој држави постоји посебна организација или тим људи којима је основни задатак сајбер ратовање или тзв. „електронски рат". Тај виртуелни вид ратовања изводи се на интернету, ради праћења и прикупљања података, односно шпијунирања или онеспособљавања функционисања одређених система; дакле, ради се о саботажи или саботажама друге земље.

Видљиви су и јавно доступни само неки подаци, који указују на то да се за ту намену издвајају значајна материјална средства. У јавности се о тим активностима сазна тек када прође дуг период и отворе се архиве или када земља жртва огласи да је нападнута.

Свакодневни напади хакера на сајтове државних или јавних институција приметни су и јавно оглашени свакодневно у медијима јавног информисања,

Напади се изводе тако да се врши анализа изворног кода софтвера који жртва користи, након чега се развијају специјализовани вируси који адресирају и инфицирају тачно дефинисане рачунаре на којима су пронађени сигурносни пропусти. Наравно, све то ради се тако да се прикрију сопствени трагови. Поред примарних циљева често страдају и секундарни циљеви, па чак и циљеви треће или четврте категорије.

## Заштита од праћења на интернету

Коришћењем интернета у просечним границама сваки корисник поред себе „има" много особа које прате његове навике, било да се ради претраживање помоћу спајвера, веб скрипти или употреби камере. Скидањем таквих информација особа из било којег дела планете може сазнати ваше име, адресу, као и многе поступке и навике и открити приступне шифре логовања.

Два су полазна и основна начина да се неко може пратити преко интернета, било инсталирањем малвера на рачунар или праћењем информација које корисник размењује са удаљеним сервером. Најлакше је да се изврши провала или инсталира спајвер/вирус на рачунар. Због тога је неопходно користити лиценцирани ОС, редовно га одржавати и ажурирати критичне делове, чиме се може спречити аутоматски сигурносни продор претварањем спајвера у гомилу бескорисних података.

Такође, неопходно је да антивирус програм буде стално активан и редовно ажуриран. Ако је база података о вирусима одређеног антивирусног програма застарела, он неће бити у могућности да на време препозна неке савремене сигурносне претње. Подаци говоре да светским мрежама у изворној верзији кружи неколико стотина милиона вируса, а уз њихову мутацију и накнадну генерацију број је вишеструко већи.

Уколико се примети да антивирус програм није активан у позадини и ако сигурност система, с времена на време није проверавана, обавезно је реинсталирати антивирус програм, јер је безбедност највероватније компромитована. Поред тога, пожељно је користити само један антивирусни програм. Уколико, ипак, користите два или више антивирусних програма, они ће давати лажне узбуне, па можда и блокирати један другог и на тај начин спречавати коректну детекцију безбедносних претњи.

Треба водити рачуна о тома де се никада не преузимају садржаји са неофицијелних и сумњивих сајтова, чак и ако антивирус програм не показује дефетизам, јер просечан корисник углавном користи или бесплатну верзију антивируса, која има веома мали опсег заштите, или антивирус програм којем је лиценца истекла. Чак и ако је у питању лиценцирани софтвер, често се догађа да је неажуриран.

Препорука је да се код оперативног система Windows користи firewall, док код оперативног система Линукс постоји интегрисан netfilter firewall. Ако се користи Windows платформа и ради са админ профилом, било који програм може затражити админ режим рада за себе, па чак и малвер који је случајно инсталиран. Ако програм нема администраторска права он не може користити веома битне делове система који служе за слање података. Такође, малвер је много лакше уклонити у стандардном режиму.

Све што је речено, наравно, ни издалека није и све што се може предузети ради повећања сигурности у раду с информационим и телекомуникационим уређајима. Уз пуну одговорност у раду с мобилним телефонима, преносним рачунарима и таблетима треба предузимати још неке мере од којих су важније зналачко коришћење енкрипције података, осигурање и заштита wireless мреже, избегавање сајтова који нуде услуге сакривања ИП адресе, одбијање електронске поште од непознатих пошиљалаца, коришћење једног, а не више различитих спајвер детектора у исто време, редовно пражњење спам поште без отварања и избегавање фајлова који су пристигли као додатак са електронском поштом у виду реклама, понуда и слично.

Модернизацијом мобилних телефона и повећавањем могућности и облика комуникације помоћу њих јавља се и њихова све чешћа употреба на интернету. Тако се јавила и потреба за повећаном сигурношћу у мрежној комуникацији. Од самог почетка дигиталне мобилне телефоније присутне су такозване паметне картице, које су се у почетку користиле само за идентификацију телефона, јер је долазило до злоупотреба, прислушкивања и позива на туђи рачун. Безбедност данашњег GSM подразумева заштиту и тајност идентитета претплатника и заштиту претплатничких података. Паметне картице, које то обезбеђују, познате су и као SIM модули и налазе се у сваком GSM телефону. Прва фаза спецификације GSM захтевала је употребу 4 килобајта EEPROM, док је друга фаза захтевала дупло више, чак 8 килобајта EEPROM, искоришћених за меморисање кључева, података о кориснику и телефонским бројевима. У оптицају је већ и следећа фаза, која предвиђа употребу елиптичких кривих за оверу корисника и измену сесијског кључа.

Претплатник се у мрежи идентификује IMSI бројем. Тај број заједно са личним претплатничким бројем сачињава поверљиву информацију којом мрежа препознаје претплатника. Шеме за шифровање и безбедност GSM-а дизајниране су на такав начин да се тако осетљиве информације никада не преносе преко радио-канала.

Разговори се шифрују коришћењем привременог случајно генерисаног кључа за шифровање. Мобилна станица идентификује се TMSI бројем који издаје GSM мрежа и због додатне безбедности може се периодично мењати. Безбедносни механизми GSM-а састављени су од три различита елемента: претплатничког броја (SIM), GSM мобилне станице и мреже. SIM картица садржи ИМСИ број, лични претплатнички број, алгоритам за шифровање (A8), алгоритам за заштиту (A3) и PIN број. GSM уређај садржи алгоритам за шифровање A5. Центар за идентификацију (АУЦ) садржи базу података о претплатничким подацима. Они садрже IMSI, TMSI, LAI и лични претплатнички број за сваког корисника. Оваква расподела сигурносних елемената и алгоритама за шифровање омогућава висок ниво безбедности

У неким земљама није дозвољен увоз било какве криптографске опреме, па су, самим тим, и комуникације потпуно незаштићене. Потенцијални прислушкивач то може искористити уз још један технички пропуст у ГСМ мрежи, а то је да није предвиђена ауторизација базних станица. У том случају довољно је направити властиту базну станицу, која би телефону послала информацију да је на одређеној територији, чиме би он аутоматски искључио криптозаштиту и омогућио прислушкивање.

од могућег прислушкивања и неовлашћеног коришћења.

## Чишћење кеш-меморија и убрзавање рачунара

Ако се деси да рачунар ради коректно, а на мрежи приликом коришћења претраживача показује успорени рад, најчешћи узрок је препуњена кеш-меморија. Пуна кеш-меморија није само знак великог оптерећења рада, већ неретко и користан извор података нападачима. Зато је потребно свакодневно вршити њено пражњење, што изискује веома мало времена, а доноси вишеструку корист. Брисање кеш меморије врши се различито за поједине претраживаче. Углавном, за интернет експлорер потребно је одабрати опцију tools, па из наредног менија кликнути на internet options. Када се отвори нови прозор под Browsing history изабрати опцију delete, кликнути на delete all у наредном прозору и тиме је кеш-меморија избрисана. За њено брисање на претраживачу Mozilla потребно је отворити претраживач, кликнути на tools у мени бару и изабрати options, затим изабрати Advanced–Network–Cached Web Content. Десно од назива опције кликнути Clear Now и сачекати неколико секунди.

Претраживач Гугл хром има у десном горњем углу дугме са нацртаним кључем. Треба га изабрати, кликнути на њега и у падајућем менију изабрати Tools. По отварању тог менија изабрати Clear Browsing Data, затим откачити опцију Empty the cache и потом кликнути на clear browsing data. Рефрешовати страницу (Ctrl+F5). За Оперу у горњем левом углу кликнути на дугме Опера. У падајућем менију изабрати Settings – Delete Private Data. У наредном прозору изабрати Detailed Options, откачити опцију Delete entire cache и кликните на Delete.

Многи од наведених, али и других претраживача, у менију одржавање или подешавања имају и опцију поставки на матерњи језик корисника, те се наведени поступци могу пратити и без доброг познавања језика на којем је програм израђен у оригиналној верзији.

## Одржавање ИКТ опреме

Подаци говоре да је данас, на глобалном нивоу, у употреби, отприлике, око десет милијарди мобилних телефона. Поред праћења, прислушкивања и крађе података смештених на уређају, та област интересантна је и због великих могућности за физичко отуђење апарата и њихову продају на илегалан начин. Неки поступци заштите апарата и заштите апликација на њима односе се на физичку заштиту од крађе, док се други односе на софтверску заштиту. Када је реч о заштити апарата од крађе, потребно је на пригодан начин обележити телефонски апарат, закључавати тастатуру и то не уобичајено, већ помоћу шифре, сачувати IMEI (петнаесто-

цифрени идентификациони број) телефонског апарата и не остављати телефон у колима, на столовима кафића и ресторана...

Када се ради о софтверској заштити, односно о заштити програма инсталираних на апарату, неопходно је заштитити телефон антивирусним програмом, ограничити коришћење блутут сигнала, редовно одржавати оперативни систем телефона и опрезно користити бежично логовање телефоном на интернет. Поред тога, пожељно је инсталацију апликација вршити само са званичних извора и не плаћати на интернету преко мобилног телефона.

## Софтверско и хардверско одржавање рачунара

Имајући у виду да се на хард-диску подаци не уписују стиктно редоследом, већ по неком случајном избору, и да се налазе на више места на диску, неопходно је повремено извршити дефрагментацију података. Тај веома пожељан и користан процес може се извршити и коришћењем алата у самом оперативном систему, али се тада обавља само делимични опоравак диска, јер систем не дозвољава премештање такозваних „закључаних" фрагмената. Уколико, пак, постоји потреба за целокупном дефрагментацијом на располагању је неколико софтверских алата којима се врши тотална дефрагментација. Тим поступком врши сте истовремено чишћење и оптимизација диска.

Када рачунар не ради у константним темературним условима, поготово у зимском периоду, потребно је да се диску дозволи време за прилагођавање условима околине. Кад год је могуће, треба се трудити да се задовоље минимални услови експлоатације телекомуникационих уређаја. У раду с рачунаром увек треба водити рачуна о његовим експлоатационим карактеристикама и знати да је идеално да он ради на собној температури. Пожељно је, за сваки случај, повремено урадити копију важнијих података. Пре евентуалне оправке рачунара обавезно га треба искључити из напајања, не треба га укључивати ако је на ћебету, тепиху и сличним материјалима, као ни излагати директном извору топлоте... Преносни рачунар, по уношењу у просторију, пожељно је оставити извесно време да се прилагоди температури околине, па га тек онда укључити.

## Заштита података на УСБ меморији

У зависности од уређаја, USB или флеш меморије имају ограничен број уписа, између две и десет хиљада уписа, док ограничење приступу и читању не постоји. Та се ситуација не може избећи, али се правилним коришћењем и једнаким бројем уписа и читања умногоме продужава век трајања.

Заштита флеш меморије може се побољшати и коришћењем неких програма као што су wear leveling (изједначавање броја уписа) и error correcting code (код за исправљање грешака). Препорука је да се не врши рад директно на флеш меморији, као ни покретање апликација или њихово инсталирање директно са флеша, већ њихово копирање на хард- диск, па тек онда рад са њима.

## Складиштење података

Такозвани зависници од честе и вишесатне употребе средстава ИКТ знају колика је мука кад систем падне или се поквари срце уређаја – његов хард-диск. Тада се често дешава да садржај телефона или рачунара остане недоступан или трајно изгубљен. Препорука је, стога, да се сви важнији подаци складиште на још једној партицији хард-диска или да се изради резервна копија на екстерном хард-диску, CD, DVD или на флеш меморији. То је, уосталом, најпрепоручљивије.

Многи провајдери нуде бесплатно складиштење садржаја у оквиру њихових сајтова, преко сопствених налога корисника. У последње време у оптицају је и опција складиштења података у такозваном „облаку" где се нуди опција дела бесплатног складиштења података, а делом ако се ради о већим количинама уз наплату по веома повољним ценама. Та два начина можда доприносе растерећењу рачунара корисника, али је проблем безбедности и приватности података занемарен. Остаје кориснику да сам одлучи где ће, како, колико и које податке да складишти.

## Звоно за узбуну

Упад у рачунар хакери могу да остваре једном од многобројних метода уплива, али и сами корисници могу допринети рањивости рачунара тиме што повуку неки од малициозних програма приликом скидања и инсталирања неке апликације. То, свакако, не треба помешати са интернет преварама којима сами корисници доприносе, најчешће приликом финансијских трансакција.

Ако приметите да сте хаковани или нападнути вирусом прво што треба урадити јесте да се покуша пронаћи узрок напада на ваш рачунар – да ли је у питању игра и забава, крађа података или финансијска корист. Свакако, треба обратити пажњу који је део система или

која је апликација нападнута. Одмах ресетујте све шифре на сервису који је нападнут и на свим осталим сервисима које користите, без обзира на то да ли су и они нападнути или не. Иначе, се препоручује повремена промена лозинки и ако нисте жртва напада. Извршите ажурирање антивирусног програма, а по потреби и замените га или инсталирајте поново, а затим извршите скенирање компјутера антивирус програмом.

Ако је дошло до губитка налога, преко провајдера или администратора сајта извршите повраћај свог корисничког налога. Повраћај се врши веома једноставно и лако или употребом сигурносних питања или слањем и-мејла администратору сајта. Након тога следи провера да ли су остављена „задња" врата или тајни улази, како их хакери зову, а што се најлакше може извести преко подешавања филтера на налогу. Одмах након тога треба извршити промену питања и одговора за сигурносну проверу.

Уколико сте утврдили или сумњате да је мета напада био ваш рачун у банци, одмах преко кол-центра о томе известите банку и у договору са особљем извршите блокирање рачуна и хитну промену ПИН кода, или приступне лозинке електронског банкарства. Након тога већина банака захтева долазак у банку где се изврши детаљан преглед историје рада рачуна, након чега се сагледају све последице упада. Кад год је могуће избегавајте сајтове који нуде плаћање на клик или нуде посебне картице или рачуне за интернет пословање.

Провера осталих налога на свим сервисима се подразумева, јер они могу поново довести хакера до ваших података. То је нарочито опасно преко друштвених мрежа и и-мејл налога. Онемогућите међусобно повезивање сервиса чије апликације нуде да приступате свом налогу преко првог на који се логујете, као и блокирање дозвола приступа информацијама трећим лицима које тако великодушно нуде. Ако на тај начин дозволите међусобно повезивање, искусан хакер искористиће било који налог да поново приступи вашим подацима, тако да вам претходни кораци неће дати резултате.

Дакле, свака апликација подразумева посебан налог и обавезну промену шифре, као и повремену измену након тога, без обзира да ли је напад поново извршен или не.

Веома важан корак јесте и подела искустава са свима познаницима на друштвеним мрежама, преко електронске поште или личним контактом, па чак и јавно објављивање, чиме нападачу стављате до знања да је примећен. Тиме и упозоравате особе које су са вама у контакту да прегледају своје налоге или повезаност са вашим налозима.

И поред тога што општи закључак подразумева да на повећање сигурности у коришћењу средстава и уређаја ИКТ значајно утиче много чинилаца, може се нагласити неколико најважнијих. Њихово уважавање и коришћење правила у свакодневном раду значајно ће повећати безбедност у комуникацију мобилним телефоном, лаптопом или рачунаром. При томе треба имати у виду коришћење лиценцираних ОС и легалних надоградњи програма и апликација, коришћење и ажурирање антивирусних програма, контролу корисничких налога, периодичну промену приступних лозинки, редовну израду копије података и заштиту података – енкрипцију. ■