Прирачник за сајбер закани:

идентификација и борба против ризиците за корисниците во јавниот и приватниот сектор и граѓаните

Александар Братиќ

Октомври 2022 година

DCAF Geneva Centre for Security Sector Governance

За ДЦАФ

ДЦАФ – Женевскиот центар за управување со безбедносниот сектор е посветен на подобрувањето на безбедноста на државите и нивното население во рамките на демократско управување, владеење на право, почитување на човечки права и родова еднаквост. Од своето основање во 2000. година, ДЦАФ има придонесено кон креирање на поодржлив мир и развој, помагајќи им на државите партнери и меѓународните актери кои ги поддржуваат тие држави во подобрувањето на управувањето со безбедносниот сектор преку инклузивни и партиципативни реформи. Тој креира иновативни производи на знаење, промовира добри норми и пракси, дава правни совети и совети за политиките и го поддржува градењето на капацитетот на државните и недржавните актери во безбедносниот сектор.

ДЦАФ – Женевски центар за управување со безбедносниот сектор
Maison de la Paix
Chemin Eugène-Rigot 2E
CH-1202 Женева, Швајцарија
Tel: +41 22 730 94 00
info@dcaf.ch
www.dcaf.ch
Twitter @DCAF_Geneva
Design & layout: DTP studio

Оваа публикација е развиена во рамките на проектот „Добро управување во сајбер безбедноста на Западниот Балкан“ на ДЦАФ – Женевскиот центар за управување со безбедносниот сектор, кој е поддржан од канцеларијата за односи со странство, Комонвелт и развој на Обединетото Кралство.

DCAF Geneva Centre for Security Sector Governance

Содржина

Резиме

Светот зависи од поврзаноста на дигиталните системи и технологии во секој аспект на секојдневниот живот, како што се трговија, финансии, комуникации итн.

Ние живееме во дигитален свет каде што личните податоци се најважни. Важно е да се разбере дека личните податоци се поранливи од било кога. Често слушаме за упади во податоци и сајбер закани кои влијаат на милиони корисници. Повеќето компании и институции се борат да ги заштитат своите податоци од хакерите и сајбер криминалците, а вие исто така треба да играте улога во тоа. Сајбер безбедноста не се однесува само на организациите, туку и на личните компјутери, мобилни телефони и таблет уреди.

Сајбер закана или закана по сајбер безбедност е малициозна активност осмислена за крадење или оштетување на вашите податоци или нарушување на системот на еден поединец или цела организација.

Во овој прирачник ќе ви бидат претставени различни сајбер закани. Сајбер заканите вклучуваат широк спектар на различни напади, а најчестите се:

- Социјален инженеринг
- Фишинг напади (phishing – риболов)
- Преземање податоци во поминување (Drive by downloads)
- Напади Човек-во-средина (MITM напади)
- Напади со фрлени УСБ уреди
- Малвер - malware – малициозен софтвер

За да се заштитите себеси и своите системи, вие морате да научите за овие различни видови на сајбер закани и различните начини како да останете безбедни на интернет.

Вообичаени сајбер напади

Социјален инженеринг

Социјалниот инженеринг се користи за да се доведат во заблуда или манипулираат метите, со цел добивање на информации или пристап до нивните компјутери. Овие видови на напади се потпираат на човечката интеракција и вообичаено вклучуваат манипулација на корисникот за да ги прекрши безбедносните процедури и најдобрите пракси за така да добијат неовластен пристап до системи или за корисниците да им дадат чувствителни информации.

Сајбер криминалците го користат пристапот преку социјалните мрежи да ги скријат своите прави идентитети и мотиви и се претставуваат како лица од доверба.

Тоа се врши со мамење на корисникот да кликне малициозен линк или преку добивање на физички пристап до компјутерот со измама.

Измами на интернет

Измамите на интернет се различни методологии на делото измама кои сајбер криминалците ги вршат на интернет. Измамата може да се случи преку фишинг е-пошта, социјални медиуми, СМС пораки на вашиот мобилен телефон, лажни повици за техничка поддршка и повеќе. Главните цели на сите овие видови на измами се од крадење на кредитни картички, снимање на кориснички акредитиви за најава и лозинки, се до кражба на идентитет.[1]

Измамите на интернет главно функционираат бидејќи изгледаат реално и ве фаќаат неподготвени кога не ги очекувате. Сајбер криминалците – измамници (скемери) – стануваат сè попаметни и користат нови технологии, производи итн. Совети како да не ве убедат да им дадете ваши лични информации или детали:

- Измамите навистина постојат, бидете внимателни.
- Не отворајте сомнителни текстуални пораки, поп-ап прозорци и не кликајте на прилозите во е-поштата, туку избришете ги веднаш.
- Секогаш бидете свесни со кого имате работа.
- Не одговарајте на телефонски повици кои се однесуваат на ваши лични информации или информации за вашата кредитна картичка; спуштете ја слушалката.

Фишинг (phishing) напади

Повеќето сајбер напади почнуваат со фишинг (phishing – риболов) е-пошта. Фишинг е вид на социјален инженеринг во кој сајбер криминалците ќе ја измамат жртвата да им даде чувствителни информации или да инсталира малициозен софтвер.

И покрај тоа што техничките мерки за безбедност стануваат сè подобри, фишингот останува еден од најевтините и најлесните начини сајбер криминалците да добијат пристап до чувствителни и лични информации.

1 https://us.norton.com/internetsecurity-online-scams.html#

Ако корисниците кликнат на линк, нивната безбедност може да биде загрозена и да станат жртви на кражба на идентитет.

Со еден клик корисниците исто така можат да ги компромитираат своите лични информации, акредитиви за најави како што се кориснички имиња и лозинки и финансиски информации како што се броеви на кредитни картички.

Напаѓачите често го постигнуваат ова со малициозна е-пошта која делува како да е од извор од доверба, но понекогаш користат и други методи, кои се објаснети долу.

Како функционира фишинг?

Повеќето фишинг кампањи вклучуваат една од две основни методи:

- **Малициозен прилог (attachment)**

  Малициозен прилог во е-пошта, кој вообичаено има алармантен наслов како „ФАКТУРА“. Кога ќе бидат отворени, овие прилози инсталираат малвер на машината на корисникот.

- **Линкови до малициозни веб сајтови**

  Малициозните линкови водат до веб сајтови кои често се клонови на легитимни сајтови. Посетувањето на сајтот може да доведе до преземање на малициозен софтвер или страницата за најава на сајтот може да содржи скрипти кои крадат акредитиви[2].

Видови на фишинг напади

Целен фишинг (Spear Phishing)

Целен фишинг е малициозен напад со лажна е-пошта која е насочена против одредена организација или лице и претставува обид за добивање неовластен пристап до чувствителни информации[3]. Овој напад не се врши од случајни напаѓачи, туку е поверојатно дека се врши од сајбер криминалци кои сакаат на тој начин да постигнат финансиска добивка или да соберат вредни информации.

Целниот фишинг напад функционира така што се праќа е-пошта од извор од доверба, но таа води кон лажен веб сајт кој е преполн со малициозен софтвер. Оваа е-пошта најчесто користи креативни методи за привлекување на вниманието на корисникот.

Целниот фишинг напад е далеку поефективен од другите фишинг напади, бидејќи бара од криминалците потрошат време и ресурси во истражување пред нападот, заради тоа што ќе бидат многу поуспешни ако научат за нивната мета пред нападот.

Лов на китови (Whale Phishing/Whaling)

Лов на китови (whale phishing) е сличен со целниот фишинг, со неколку важни разлики. Додека целниот фишинг е вообичаено насочен против членови на одредена група, ловот на китови е насочен против конкретно лице – вообичаено „најголемата риба“ во целната организација или лице со значително богатство и моќ која сајбер криминалците сакаат да ја искористат.

2 What is phishing? Everything you need to know | IT Governance UK

3 What is Phishing? (gfidigital.com)

Вишинг (Vishing)

Вишинг или „гласовен фишинг“ вклучува манипулација на луѓе преку телефон и нивно заведување да им откријат чувствителни информации во обид да ги искористат тие податоци за своја лична корист, вообичаено финансиска.

Смишинг (Smishing)

Терминот смишинг се однесува на фишинг преку СМС пораки и вклучува текстуална порака наместо е-пошта. Метите вообичаено добиваат текстуална порака која содржи измама и која ги присилува да дадат лични или финансиски информации. Сајбер криминалците се преправаат дека се државен орган, банка или друга компанија за да делуваат легитимно во своите барања.

Смишинг напаѓачите често бараат лични или банковни податоци, како што се акредитиви на кориснички налози, броеви на кредитни картички и броеви за идентификација. Потоа, тие ги користат тие информации за спроведување на различни видови на напади, вклучувајќи и финансиски измами, измами со подароци и измами со поддршка за клиенти.

Преземање на податоци во „проаѓање“ (drive-by downloads)

Во напади со преземање на податоци во „проаѓање“ се преземаат малициозни скрипти на компјутерите или други уреди без знаење на корисникот, со што корисникот се изложува на различни сајбер напади. Тоа може да се случи на секој уред и на било кој оперативен систем. Вообичаено се случува кога корисникот ќе посети и пребарува компромитиран веб сајт.

Напад човек-во-средина (man in the middle (MITM))

MITM нападот се случува кога сајбер криминалецот тајно ќе се вклучи меѓу два уреда или меѓу уред и небезбедна ви-фи мрежа, со цел пресретнување на комуникациите кои потоа тој може да ги чита и/или менува. Во тој случај, корисникот може ненамерно на сајбер криминалецот да му прати акредитиви или други информации.

Напад со отфрлен УСБ уред

Во овој напад, УСБ уред кој содржи малициозен код се приклучува на компјутер.

Највообичаената сајбер заканата претставена со овој напад е инфекција со малициозен софтвер или вирус. Инфекциите преку УСБ дискот можат да бидат намерни и ненамерни, зависно од конкретниот малициозен софтвер.

Најпаметно е организациите да прекинат да и веруваат на застарена УСБ технологија и да почнат да ја користат моќта на безбедните дигитални мрежи и чување на податоци на интернет облак (cloud).

Малвер (malware – малициозен софтвер)

Малвер е генерален термин кој што се користи за дефинирање на секоја датотека или програма која има за цел да оштети или наруши компјутер:

- **Ботнет софтвер**

  Ботнет софтвер кој е осмислен да инфицира голем број на уреди кои се поврзани на интернет.

Некои ботнет (мрежи на роботи) се составени од голем број на уреди од кои секој користи релативно мала процесорска сила. Со тоа се отежнува откривањето на овој вид на малициозен софтвер, дури и кога ботнетот е во функција.

- **Рансомвер напади (напади со софтвер за уценување)**

  Рансомвер е вид на малициозен софтвер кој ги шифрира информациите на корисникот и бара плаќање за клуч за дешифрирање за да се вратат информациите. Меѓутоа, плаќањето на откупот не гарантира секогаш дека шифрираните податоци ќе бидат вратени.

- **Спајвер (шпионски софтвер)**

  Спајвер е вид на малициозен софтвер кој се користи за незаконско следење на активностите на корисникот на компјутерот и собирање на лични податоци.

- **Тројански вируси**

  Тројанските вируси се вид на малициозен софтвер кој делува како легитимен софтвер, но прават малициозни активности откако ќе бидат извршени.

- **Вируси и црви**

  Компјутерските вируси се малициозен код инсталиран без знаење на корисникот. Вирусите можат и да се множат и да се шират на други компјутери со тоа што се прикачуваат на други компјутерски датотеки.

  Црвите се слични на вирусите бидејќи исто така се множат сами, но тие не мораат да се прикачат на друга програма за да го направат тоа[4].

4 Types of Cyber Threat in 2019 | IT Governance USA

Како да останете безбедни на интернет

Бидете внимателни со своите лични информации и дигитален идентитет

Ние, како поединци, можеме да се идентификуваме на различни начини. Нашите имиња, адреси, возраст, професии и повеќе. Нашите идентитети се содржани во различни форми на нашите возачки дозволи, картички за осигурување, изводи од матична книга на родени, картички за работа или училиште, итн.

Ако размислиме за сите различни идентификации кои ги користиме во секојдневниот живот на и вон интернетот, дали можеме со сигурност да кажеме колку од нашите приватни податоци се користат без наша согласност и колку од тие податоци се чуваат на локации кои на нас ни се непознати и кои можеби имаат пристап до нив и ги користат.

Непотребно е да се споменува дека никогаш не треба да ги делите вашите лозинки, банковни информации или лични информации на интернет или со друго лице. Информациите за вашите лични односи или имињата на миленициte можат да бидат искористени како одговори на вашите безбедносни прашања или можат на криминалците да им дадат идеја како да ги нападнат вашите лозинки.

Хакерите постојано бараат нови начини за злоупотреба на лични податоци. Кражбата на идентитет од евиденции и упад во податоците се големи закани кои го компромитираат тоа што сме, бидејќи идентитетот е нашето основно средство за интеракција:

- Вратете си ја назад контролата врз вашите податоци
- Немојте да користите свои лични податоци кога креирате профили на интернет
- Немојте да ги давате вашите лични податоци за да добиете попуст во продавница
- Немојте непотребно да ги делите вашите приватни информации на социјалните медиуми
- Секогаш проверете како ќе бидат обработени вашите лични податоци кога користите некоја апликација
- Проверете дали страницата е безбедна пред да оставите лични информации

Ако услугата што ја користите е бесплатна, бидете екстра внимателни. Ако е бесплатно, вообичаено вие сте стоката (вашите податоци).

Креирајте и користете сложени лозинки

Секогаш требате да користите сложени лозинки. Ако вашата лозинка содржи очигледни или лесни за погодување комбинации на бројки (12345, 111111, 123321), популарни женски имиња (Николина, Џесика, Хана) или само низи на букви кои формираат хоризонтални или вертикални линии на QWERTY тастатура (asdfghjkl, qazwsx , 1qaz2wsx, итн.), требате да ја смените ВЕДНАШ! Изненадува тоа што најочигледната лозинка – „password“ – е сè уште многу популарна. И неа треба да ја смените веднаш (или ако вашата лозинка е слична било што од горе наведеното).

Ако ви треба помош да смислите безбедни лозинки, еве неколку совети:

- Треба да има најмалку 15 карактери – повеќе, ако е можно.
- Помешајте ги буквите (големи и мали), бројките и симболите.
- Не користете секвенца на бројки или букви, како „qwerty“.
- Избегнувајте замени како „хакерски говор“ (кога буквите се менуваат со бројки или симболи со сличен изглед).

Користете различни лозинки за различни кориснички налози. На тој начин, ако едниот налог е компромитиран, барем другите нема да бидат под ризик.

Ако не можете да се сетите на вашите лозинки, дефинитивно требате да пробате програма за управување со лозинки. Лозинките тешко се памтат сами по себе, особено ако ви е потребна посебна лозинка за секој сајт. Се советува користење на реномирани програми за управување со лозинки како што се LastPass или 1Password[5].

Двапати проверете ги линковите пред да кликнете

Кога ја проверувате вашата е-пошта или посетувате веб страници, проверете да ли ги знаете и дали им верувате на линковите пред да ги кликнете.

Еден начин да проверите дали линкот е безбеден е да прејдете со глувчето преку него. Тоа ќе ви покаже приказ на целиот линк во статусното поле на вашиот интернет пребарувач. Проверете дали прикажаниот линк одговара на веб страната од кој треба да доаѓа. Исто така, можете да го проверите и линкот до точниот сајт, ако го пребарате неговото име.

Ако добиете е-пошта која од вас бара да се пријавите некаде, побезбедно е да не го кликнете линкот за пријавување во пораката и да одите на официјалната страница и таму да се пријавите. Можете да прејдете на официјалната веб страна или со пребарување на неговото име или, ако го знаете напамет, со внесување на адресата во URL полето на вашиот пребарувач. Овој совет ги вклучува и линковите кои ви ги пратиле пријатели во апликациите за социјални мрежи.

Ако е-поштата или страницата бара од вас да се пријавите на вашата банковна, секогаш можете да се јавите и да го потврдите барањето.

Што се однесува до преземањето на податоци, требате да размислите двапати пред тоа да го направите. Одредени сајбер криминалци имаат за цел да го инфицираат вашиот уред со малициозен софтвер така што ќе ве измамат да преземате компромитирани апликации или друг софтвер. Пред да направите било што, проверете ја страницата од која ја преземате новата игра или апликација и едноставно не преземајте ништо што делува сомнително.

Користете безбедни ВИ-ФИ мрежи

Никогаш не треба да користите небезбедна, отклучена или ви-фи мрежа без лозинка, освен ако навистина не морате. Ако користите таква мрежа, немојте да се пријавувате на ниеден кориснички

5 How to Stay Safe Online: Internet Safety Tips and Resources (reviews.org)

налог на интернет или во апликации и немојте да внесувате лични или финансиски информации.

Сајбер криминалците често поставуваат лажни ви-фи мрежи за да ги намамат корисниците. Штом лицето ќе го поврзе својот телефон на ви-фи, сајбер криминалците во основа гледаат што прави тоа лице.

Ако барате ви-фи мрежа, најбезбедниот начин е да го прашате вработеното лице како се вика нивната ви-фи мрежа.

Исто така, осигурете се дека вашите уреди не се поставени автоматски да се поврзуваат на ви-фи мрежи, освен на работа или дома. Наместете го уредот да ве праша пред да се поврзе. На овој начин ќе бидете сигурни на што се поврзувате.

Користете VPN

VPN, или виртуелна приватна мрежа, безбедно ги поврзува вашите уреди на интернет, за никој да не може да ги следи вашите активности или да им пристапи на вашите информации преку интернет врската. VPN може да биде добар начин за безбедна врска по дома или дури и кога сте надвор и користите јавна ви-фи мрежа.

Единствениот недостаток на зголемената безбедност која ја дава VPN мрежата е тоа што може да ви ја забави интернет врската. Ова често е резултат на тоа што VPN мрежата ги пренасочува вашите податоци кон друг сервер, за да ги обезбеди вашето информации.

Се повеќе луѓе работат од дома во последно време, што значи дека многу од нас можат да станат мети за сајбер криминалци. Методата за одржување на заштита е користење на VPN мрежа и нејзино ажурирање по препорака.

За да добиете VPN, требате да одберете давател на VPN услуги, да ја преземете и инсталирате VPN и да се поврзете на сервер.

Користете сајтови кои почнуваат со https//

Ако требате да се пријавите на некоја страница, проверете дали адресата во горниот дел на пребарувачот почнува со **https://**, а не со **http://**. Можеби ќе видите и **симбол на катанец** покрај адресата на сајтот.

“S” значи “secure” – безбедно и значи дека сајтот ги шифрира вашите податоци.

Купувањето преку интернет значи дека вие давате лични информации, како што се банковни сметки и информации за кредитни картички. Секогаш двапати проверете дали веб страната на која се наоѓате е безбедна, а потоа пополните ги податоците.

Исклучете го вашиот Блутут (Bluetooth)

Блутут комуникациите можат да се компромитираат или дури и манипулираат. Тоа не значи дека никогаш не треба да користите Блутут, но ако не сте поврзани со друг уред и активно не го користите, подобро е да го исклучите.

Користете антивирус и антималвер софтвер

Не се препорачува пребарување на интернет без заштита. Ако не можете да си го дозволите, барем најдете бесплатен и евтин антивирус на интернет. Одберете внимателно и мудро.

Плаќањето на мали суми за софтвер за да ја избегнете главоболката од соочување со малвер или рансомвер вреди. Ако веќе имате антивирус и антималвер софтвер, постојано ажурирајте го.

Некои препорачани антивирус и антималвер софтвери ги вклучуваат следните:

- Microsoft Defender (доаѓа со Windows, но морате да го вклучите и ажурирате)
- Norton AntiVirus Plus
- Bitdefender
- AVG
- Malwarebytes
- Avast
- SpyBot Search and Destroy

Направете бекап (резервни копии) на вашите податоци

Нашите компјутери и други уреди се дом на сите наши податоци. Меѓутоа, ако уредот е компромитиран, изгубен или украден, вашите важни податоци можат да бидат изгубени. Без оглед на тоа дали се работи за хардверски дефект, кражба, природна катастрофа или инфекција на вашиот уред со малициозен софтвер, враќањето на податоците може да биде скапо или невозможно.

Бекапот е дигитална копија на вашите најважни информации.

Кога правите резервни копии на вашите податоци, копии на вашите датотеки (пр. фотографии, документи, видеа итн.) се снимаат на надворешен уред за чување на податоци или интернет сервис како облак (cloud).

Ако имате бекап тоа значи дека можете да ги вратите вашите податоци ако нешто тргне на лошо. Тоа е превентивна мерка за вашите податоци да бидат достапни ако нешто му се случи на вашиот компјутер. Ве советуваме редовно да вршите бекап на вашите датотеки[6].

Постојат многу начини за бекап на вашите податоци, од користење на екстерни дискови, до чување на податоци на оддалечен сервер преку интернет. Ова се предностите и недостатоците на секоја од методите:

- **Бекап на надворешен диск**: за да извршите бекап на податоци на надворешен хард диск, можете да ги искористите вградените бекап опции во компјутерот. Од време на време, поврзете го дискот на вашиот компјутер и употребете ја алатка за бекап, или оставете го дискот вклучен и бекапот ќе се прави автоматски.
  Позитивни страни: бекапот е брз и евтин.
  Негативни страни: екстерниот диск може да биде изгубен или украден.

6 Back Up and Restore - Microsoft Windows | Cyber.gov.au

- **Бекап на вашите податоци на вашиот компјутер**: ова се некои упатства за различните начини за бекап на вашите податоци на Mac, iOS уреди или PC:
  * iCloud (iOS уреди)
  * Time Machine (Mac)
  * Windows 8.1 (PC)
  * Windows 10 (PC)

  Позитивни страни: бекапот е брз и евтин.
  Негативни страни: бекапот може да биде изгубен или украден.

- **Користете услуга за чување на податоците на интернет (cloud)**: наместо да ги чувате вашите податоци на хард дискот на вашиот компјутер, можете да ги чувате и на сервис како Dropbox, Google Drive, Microsoft OneDrive, или слична услуга за чување на податоци на интернет - облак. Тие автоматски ќе се синхронизираат со вашите кориснички налози на интернет и вашите други уреди. Ако се расипе вашиот хард диск или ако ви го украдат компјутерот, сè уште ќе ги имате копиите на тие датотеки кои се чуваат на интернет и на вашите други уреди.
  Позитивни страни: оваа метода е брза и лесна и во многу случаи бесплатна, а бидејќи е на интернет ве штити од сите видови на губење на податоци.
  Негативни страни: повеќето сервиси за чување податоци на облак нудат само неколку бесплатни гигабајти на податоци, така што ова функционира само ако имате мал број на датотеки кои сакате да ги ставите на бекап или ако сте волни да плаќате за дополнителен простор[7].

На крајот, треба да се размисли и за тоа каде се наоѓаат вашите важни податоци и да проверите/тестирате дали имате неколку копии во секој момент. Идеално, тие копии треба да се наоѓаат на неколку физички локации. Се додека мислите за тоа што ако нешто лошо му се случи на уредот, би требале да бидете пред повеќето луѓе.

7 Best ways to backup your computer. • Nerds in a Flash

Заклучок

Сè поголеми закани се откриваат во новите технологии како што се социјалните медиуми, компјутерската работа на интернет, технологијата за паметни телефони или критична инфраструктура, а тие закани често ги злоупотребуваат нивните уникатни карактеристики.

Наместо обид за решавање на проблемите на интернет или во компјутерските системи, подобар пристап е на вашиот уред да примените некои од советите од овој Прирачник и да внимавате на препорачаното однесување за да останете безбедни на интернет.

Референтни материјали

Online Scams, Avoiding Internet Scams, Norton

What is phishing? Everything you need to know, IT Governance UK

What is Phishing?, gfidigital.com

Types of Cyber Threat in 2019, IT Governance USA

What Is Cyberbullying, StopBullying.gov

Catherine McNally, How to Stay Safe Online: Internet Safety Tips and Resources, reviews.org

Back Up and Restore - Microsoft Windows, Cyber.gov.au

Best ways to back up your computer, Nerds in a Flash

Анекс: Листа на добри пракси

ВООБИЧАЕНИ САЈБЕР НАПАДИ	
СОЦИЈАЛЕН ИНЖЕНЕРИНГ	- Социјалниот инженеринг се користи за да се доведат во заблуда или манипулираат метите, со цел добивање на информации или пристап до нивните компјутери. Овие видови на напади се потпираат на човечката интеракција и вообичаено вклучуваат манипулација на корисникот за да ги прекрши безбедносните процедури и најдобрите пракси за така да добијат неовластен пристап до системи или за корисниците да им дадат чувствителни информации.
ФИШИНГ (PHISHING) НАПАДИ	- Фишинг е вид на напад во кој сајбер криминалците ќе ја измамат жртвата да им даде чувствителни информации или да инсталира малициозен софтвер: • Целен фишинг (Spear Phishing) – малициозна е-пошта која е насочена против одредена организација или лице со цел добивање неовластен пристап до чувствителни информации. • Лов на китови (Whale Phishing/Whaling) – насочен против конкретно лице – вообичаено „најголемата риба“ во целната организација или лице со значително богатство и моќ која сајбер криминалците сакаат да ја искористат. • Вишинг (Vishing) – е обид за добивање на податоци од жртвата и нивно користење за финансиска корист, а жртвите се мамат преку телефон. • Смишинг (Smishing) – е текстуална СМС порака која содржи измама да ги привлече лицата да дадат лични или финансиски информации (акредитиви на кориснички налози, броеви на кредитни картички, итн...), а сајбер криминалците се преправаат дека се државен орган, банка или друга компанија за да делуваат легитимно во своите барања.
ПРЕЗЕМАЊЕ НА ПОДАТОЦИ ВО „ПРОАЃАЊЕ“	- Напад со преземање на податоци во „проаѓање“ е сајбер напад каде се преземаат малициозни скрипти на компјутерите или други уреди без знаење на корисникот, со што корисникот се изложува на различни сајбер напади. Вообичаено се случува кога корисникот ќе посети и пребарува компромитиран веб сајт.
MITM (човек во средина) НАПАДИ	- MITM нападот се случува кога сајбер криминалецот тајно ќе се вклучи меѓу два уреда или меѓу уред и небезбедна ви-фи мрежа, со цел пресретнување на комуникациите кои потоа тој може да ги чита и/или менува. Во тој случај, корисникот може ненамерно на сајбер криминалецот да му прати акредитиви или други информации.
НАПАД СО ОТФРЛЕН УСБ УРЕД	- Нападот со отфрлен УСБ уред се случува кога УСБ уред кој содржи малициозен код се приклучува на компјутер.
МАЛИЦИОЗЕН СОФТВЕР (МАЛВЕР –MALWARE)	- **Ботнет софтвер** – тој инфицира голем број уреди кои се поврзани на интернет. - **Рансомвер напади (напади со софтвер за уценување)** – тој ги шифрира информациите на корисникот и бара плаќање за клуч за дешифрирање за да се вратат информациите. - **Спајвер (шпионски софтвер)** - е вид на малициозен софтвер кој се користи за незаконско следење на активностите на корисникот на компјутерот и собирање на лични податоци. - **Тројански вируси** – се вид на малициозен софтвер кој делува како легитимен софтвер, но прават малициозни активности откако ќе бидат извршени. - **Вируси и црви** – • Вируси се малициозен код инсталиран без знаење на корисникот. Вирусите можат и да се множат и да се шират на други компјутери со тоа што се прикачуваат на други компјутерски датотеки. - Црвите се слични на вирусите бидејќи исто така се множат сами, но тие не мораат да се прикачат на друга програма за да го направат тоа.

КАКО ДА ОСТАНЕТЕ БЕЗБЕДНИ НА ИНТЕРНЕТ	
НЕМОЈТЕ ДА ГИ ДЕЛИТЕ СВОИТЕ ЛИЧНИ ИНФОРМАЦИИ	- **Никогаш со никого или на интернет не треба да делите информации за:** • вашите лозинки • банковни детали • лични информации - **Вратете си ја назад контролата врз вашите податоци** - **Немојте да користите свои лични податоци кога креирате профили на интернет** - **Немојте да ги давате вашите лични податоци за да добиете попуст во продавница** - **Немојте непотребно да ги делите вашите приватни информации на социјалните медиуми** - **Секогаш проверете како ќе бидат обработени вашите лични податоци кога користите некоја апликација:** • Проверете дали страницата е безбедна пред да оставите лични информации
КРЕИРАЈТЕ И КОРИСТЕТЕ СЛОЖЕНИ ЛОЗИНКИ	- **Uvek Секогаш требате да користите сложени лозинки:** • Треба да има најмалку 15 карактери – повеќе, ако е можно. • Помешајте ги буквите (големи и мали), бројките и симболите. • Не користете секвенца на бројки или букви, како „qwerty“. • Избегнувајте замени како „хакерски говор“ (кога буквите се менуваат со бројки или симболи со сличен изглед). - **Користете различни лозинки за различни кориснички налози** - **Пробајте софтвер за управување со лозинки**
ДВАПАТИ ПРОВЕРЕТЕ ГИ ЛИНКОВИТЕ ПРЕД ДА КЛИКНЕТЕ	- **Кога ја проверувате вашата е-пошта или посетувате веб страници, проверете да ли ги знаете и дали им верувате на линковите пред да ги кликнете**: • Прејдете со глувчето преку линкот и проверете дали сте добиле приказ на целиот линк во статусното поле на вашиот интернет пребарувач. • Ако добиете е-пошта која од вас бара да се пријавите некаде, побезбедно е да не го кликнете линкот за пријавување во пораката и да одите на официјалната страница и таму да се пријавите. • Ако е-поштата или страницата бара од вас да се пријавите на вашата банковна, секогаш можете да се јавите и да го потврдите барањето. • Пред да преземете податоци, проверете ја страницата од која ја преземате новата игра или апликација и едноставно не преземајте ништо што делува сомнително.
КОРИСТЕТЕ БЕЗБЕДНИ ВИ-ФИ МРЕЖИ	- Никогаш не треба да користите небезбедна, отклучена или ви-фи мрежа без лозинка, освен ако навистина не морате. - Додека сте на ви-фи мрежа, немојте да се пријавувате на ниеден кориснички налог на интернет или во апликации и немојте да внесувате лични или финансиски информации. - Осигурете се дека вашите уреди не се поставени автоматски да се поврзуваат на ви-фи мрежи.
КОРИСТЕТЕ VPN	- VPN, или виртуелна приватна мрежа, безбедно ги поврзува вашите уреди на интернет, за никој да не може да ги следи вашите активности или да им пристапи на вашите информации преку интернет врската. - За да добиете VPN, требате да одберете давател на VPN услуги, да ја преземете и инсталирате VPN и да се поврзете на сервер.
АКО ПОЧНУВА СО HTTPS, БЕЗБЕДНО Е	- Ако сакате да се пријавите на некоја страница, проверете дали адресата во горниот дел на пребарувачот почнува со https://, а не со http://. - Можеби ќе видите и симбол на катанец покрај адресата на сајтот.
ИСКЛУЧЕТЕ ГО ВАШИОТ БЛУТУТ (BLUETOOTH)	- Ако само понекогаш користите Блутут, исклучете го кога не го користите активно, за да избегнете негово компромитирање или манипулација.
КОРИСТЕТЕ АНТИВИРУС И АНТИМАЛВЕР СОФТВЕР	- Ако не можете да си го дозволите, барем најдете бесплатен и евтин антивирус на интернет за да избегнете соочување со малвер или рансомвер.
НАПРАВЕТЕ БЕКАП (РЕЗЕРВНИ КОПИИ) НА ВАШИТЕ ПОДАТОЦИ	- Кога правите резервни копии на вашите податоци, копии на вашите датотеки (пр. фотографии, документи, видеа итн.) се снимаат на надворешен уред за чување на податоци или интернет сервис како облак (cloud). - Постојат многу начини за бекап на вашите податоци • Бекап на надворешен диск • Бекап на податоци на вашиот компјутер - Користете услуга за чување на податоците на интернет (cloud)

DCAF Geneva Centre for Security Sector Governance

DCAF Geneva Headquarters

P.O.Box 1360
CH-1211 Geneva 1
Switzerland

info@dcaf.ch
+41 (0) 22 730 9400

www.dcaf.ch

@DCAF_Geneva