

# Социјален инженеринг

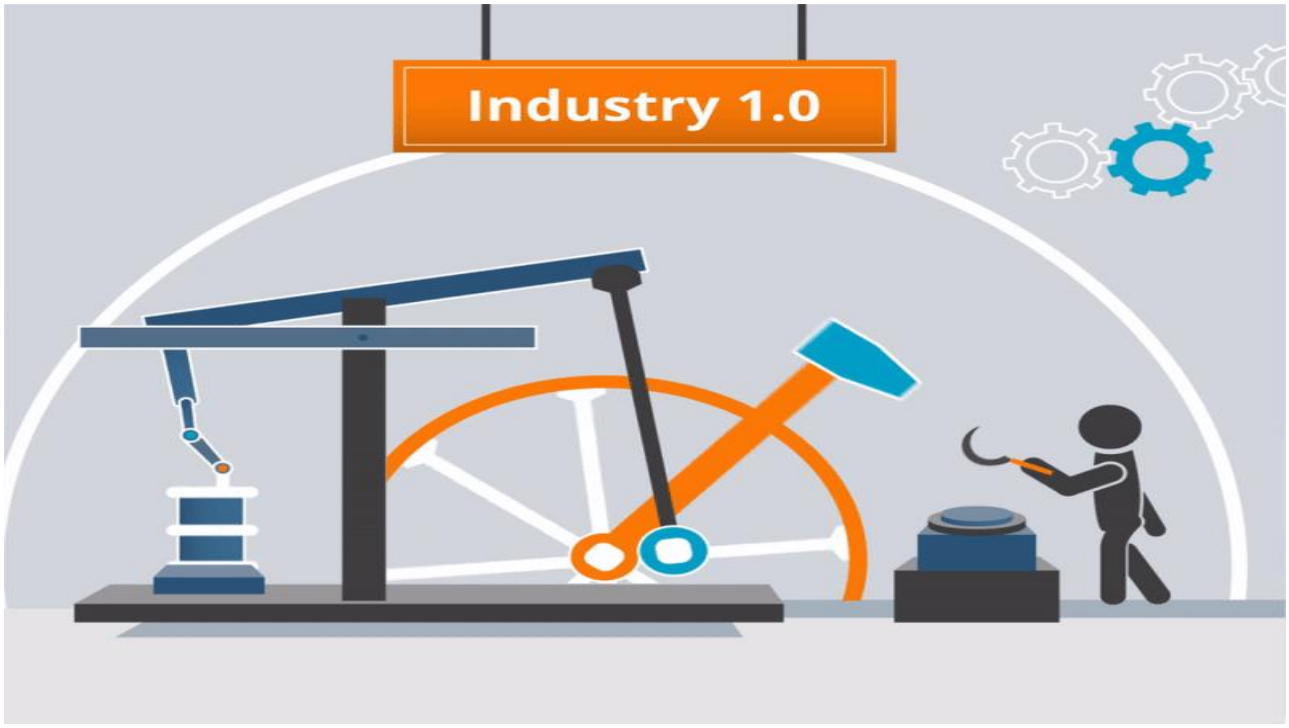
проф. д-р Митко Богданоски

@mitkobogdanoski

1




2

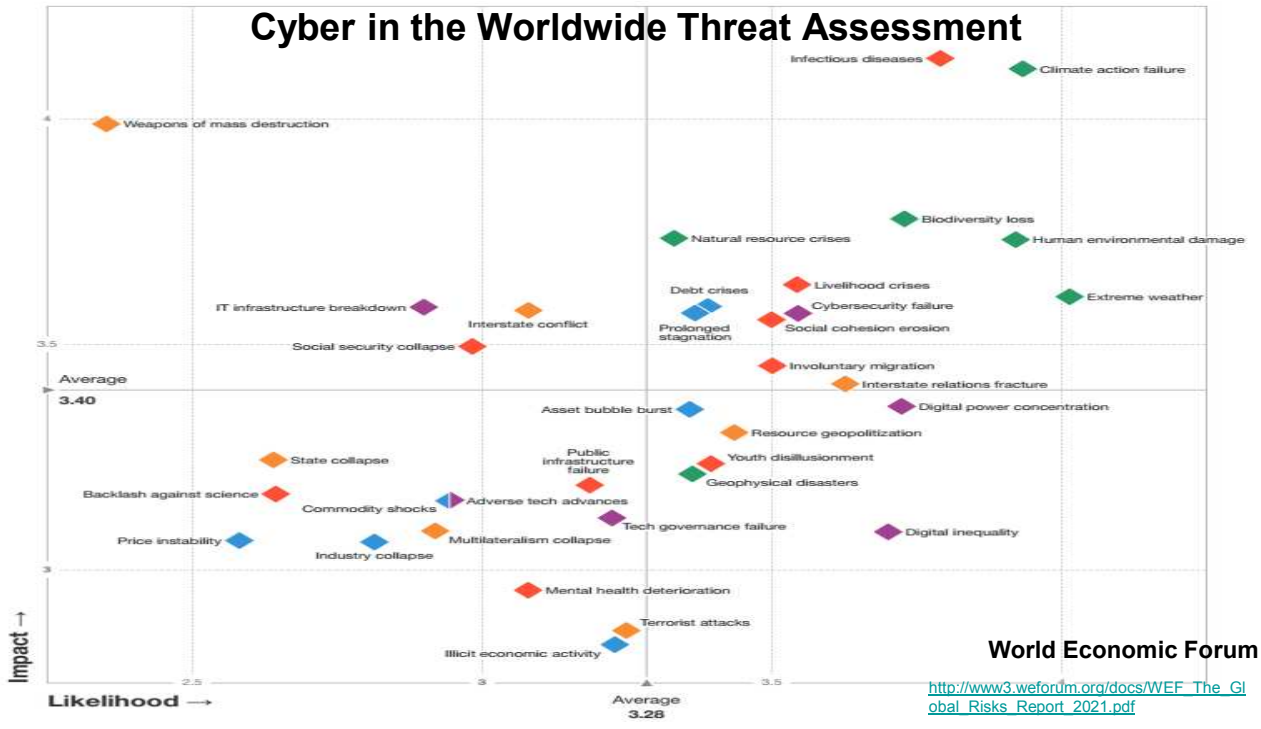

Industry 1.0

3


INDUSTRY
SECURITY
RETAIL
SOCIETY
HEALTHCARE
HOME
ENERGY
MOBILITY

4

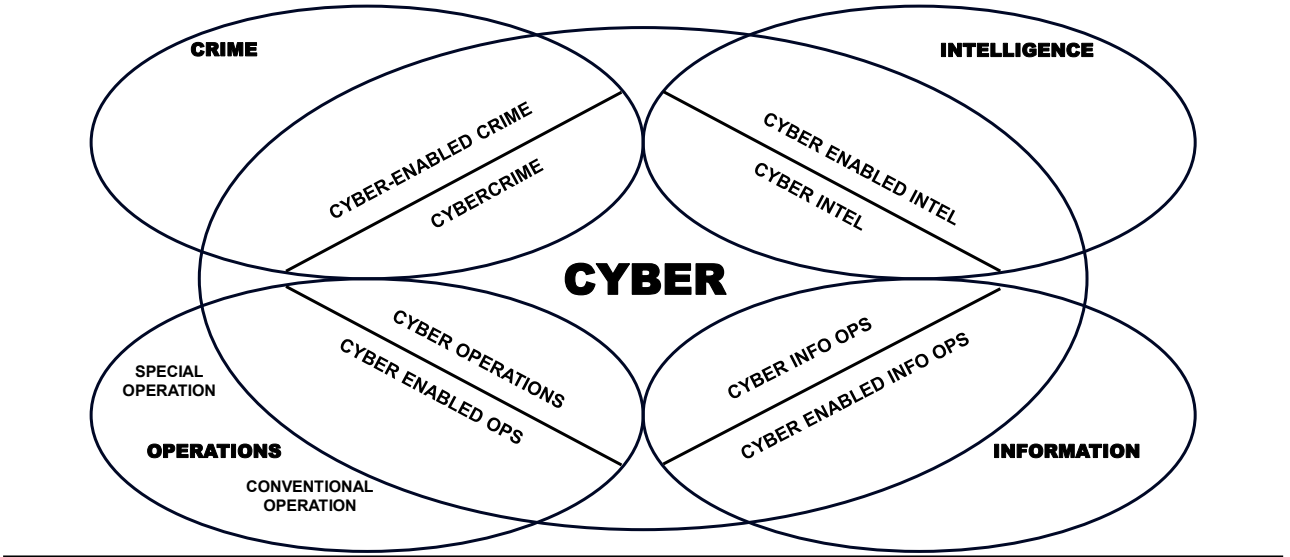
# Cyber in the Worldwide Threat Assessment




**World Economic Forum**

http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

5




@mitkobogdanoski

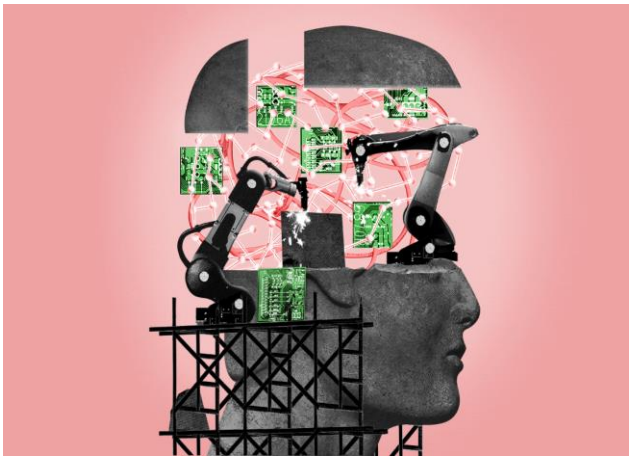
6

# Reasons for Successful Cyber Attack

## Technical

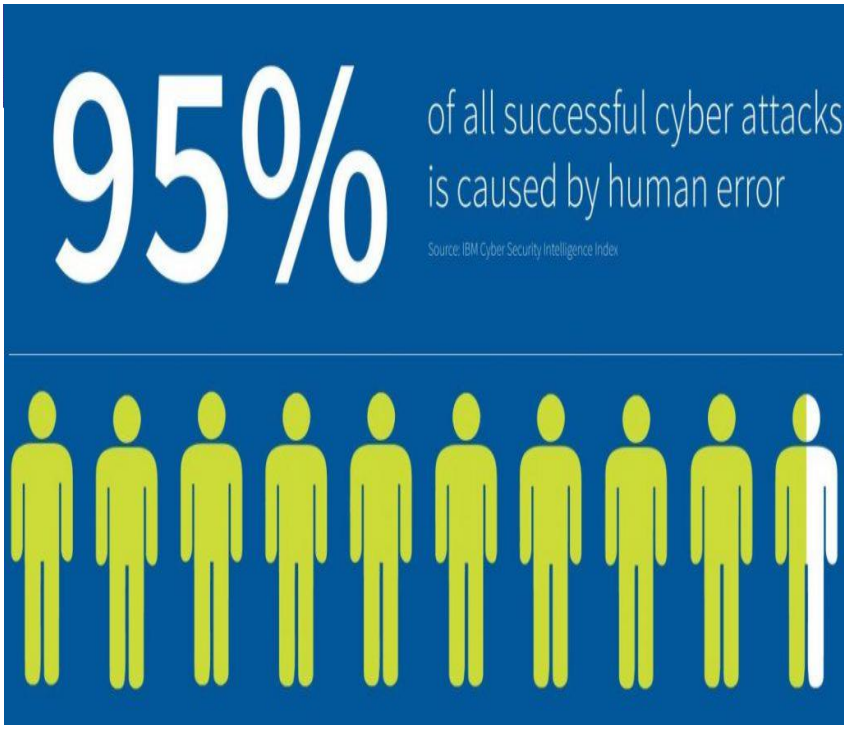


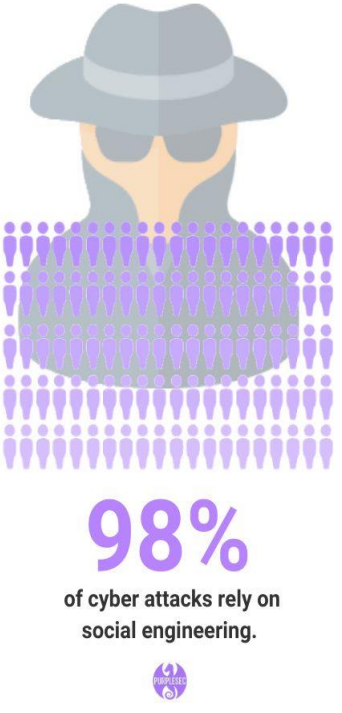
## People



@mitkobogdanoski

7




8

# Што е социјален инженеринг?

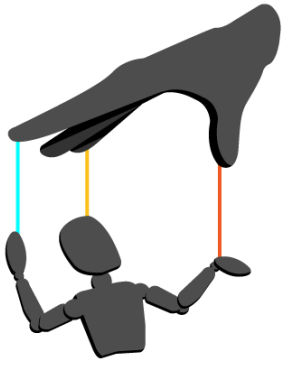
- „Социјалниот инженеринг е форма на техники искористени од сајбер криминалците дизајнирани да ги намамат наивните корисниците да им испраќаат доверливи податоци, да ги инфицираат нивните компјутери со злонамерен софтвер или да ги намамат преку линкови кон заразени страници“. - **Kaspersky**
- „Каков било вид напад што не е од техничка природа и вклучува некаков вид човечка интеракција со цел да се обиде да измами или принуди жртва да открие информации или да ги наруши нормалните безбедносни практики“ – **EC Council**
- „Искористување на наивноста на луѓето преку влијание, убедување и манипулација за да се добијат витални информации“ – **Kevin Mitnick**



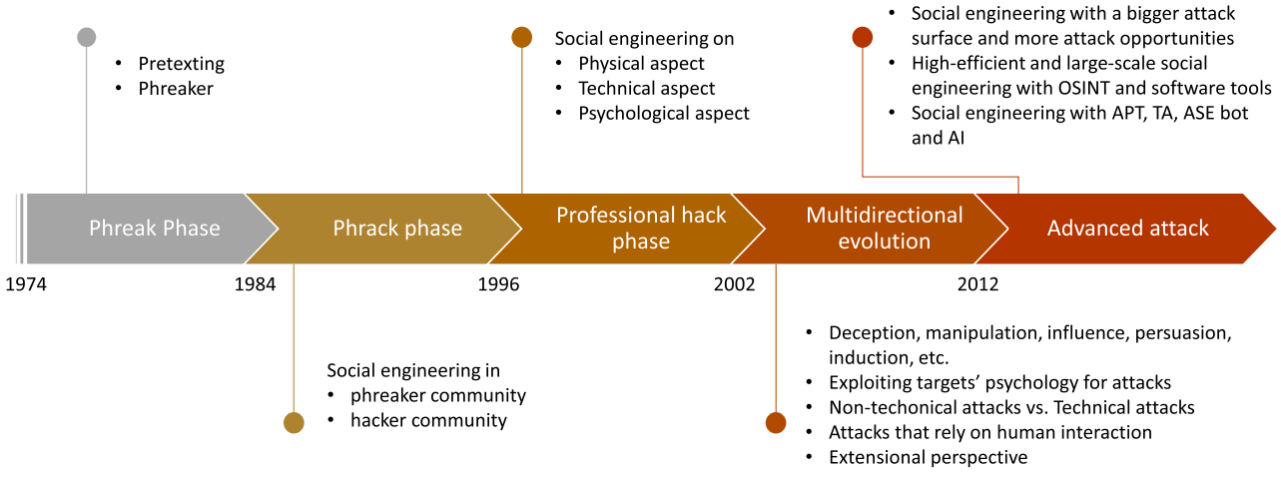
# Што е социјален инженеринг?

Уметност на манипулирање со луѓето, така што тие се откажуваат од доверливи информации или ги кршат стандардните безбедносни практики.





# Еволуција на социјалниот инженеринг



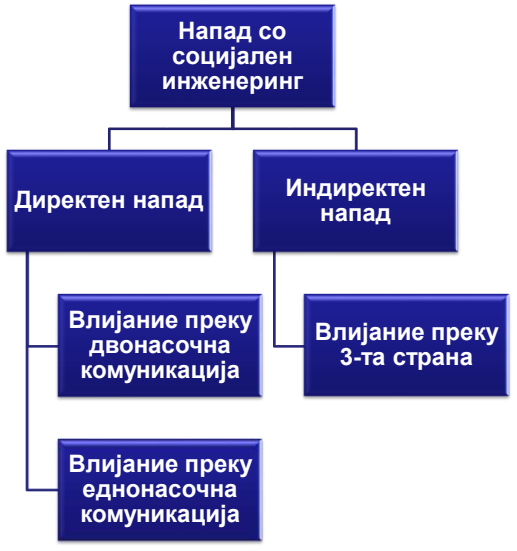

https://ieeexplore.ieee.org/document/9087851



# Факти за социјалниот инженеринг

- Секој е потенцијална жртва.
- Многу често на сајбер криминалците им е полесно да манипулираат со човекот отколку со компјутерската мрежа или систем.
- Нападите можат да бидат релативно ниско-технолошки, евтини и лесни за извршување.
- Технолошкиот развој е многу брз, заедно со софистицираноста на нападите.

# Поделба на нападите со социјален инженеринг




@mitkobogdanoski

13

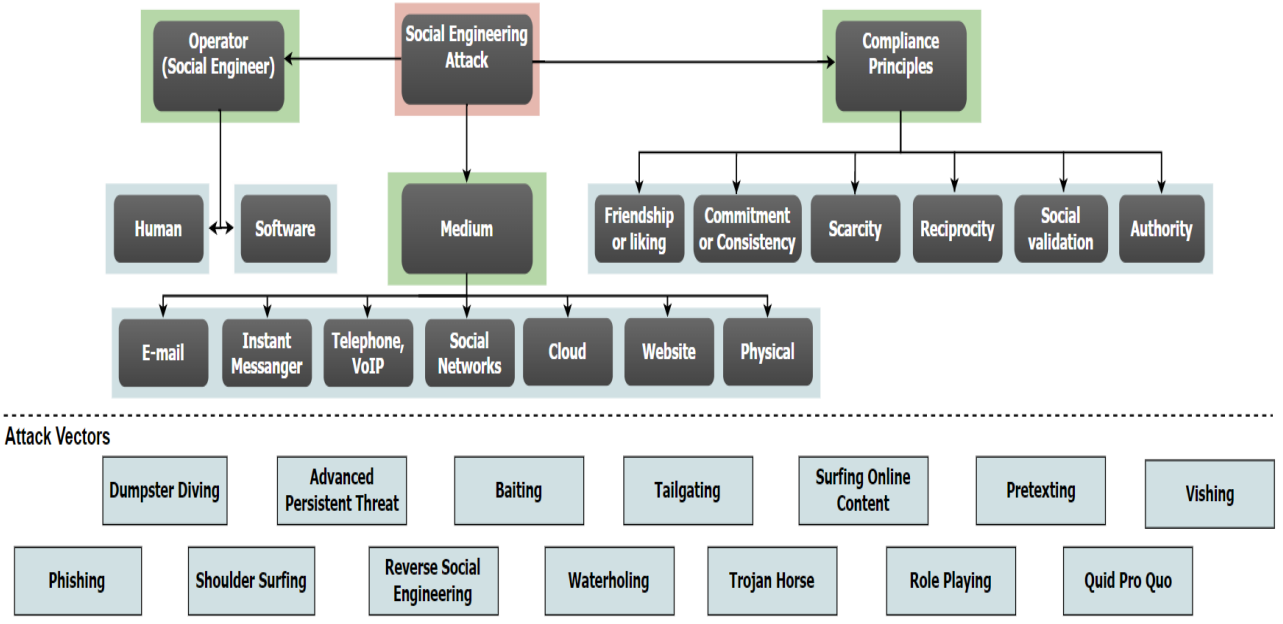
# Циклус на нападот со социјален инженеринг




@mitkobogdanoski

14

# Таксономија на нападите со социјален инженеринг




15

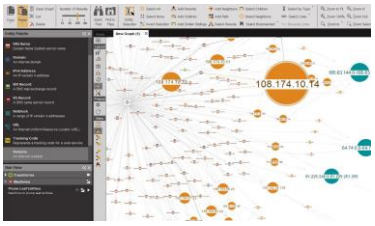
# Медиум




@mitkobogdanoski

16

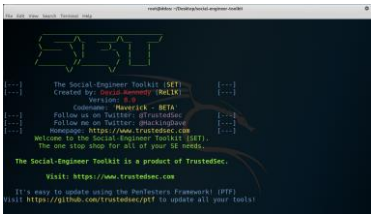
# Човек и софтвер (алатки)

















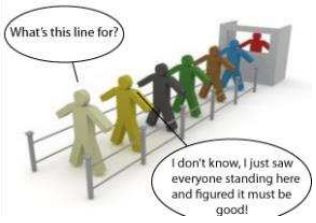


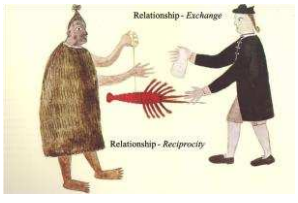
@mitkobogdanoski

17

# Принципи на усогласеност





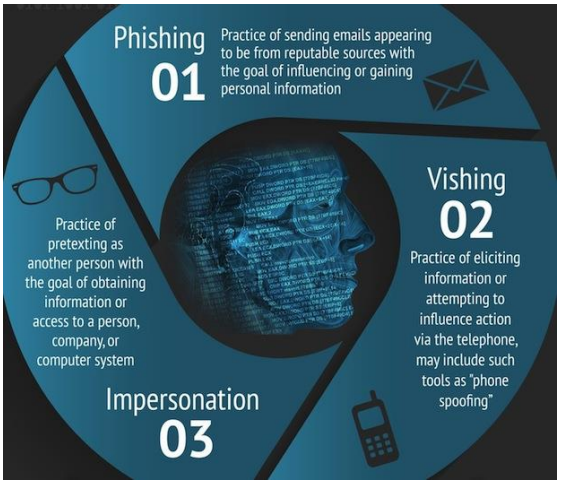





@mitkobogdanoski

18

# Најчест напади со социјален инженеринг




https://www.social-engineer.org/social-engineering/social-engineering-infographic/



# Најчест напади со социјален инженеринг

- Dumpster Diving
- Phishing/Spear Phishing
- Shoulder Surfing
- Advanced Persistent Threat
- Reverse Social Engineering
- Baiting
- Watering Hole
- Tailgating
- Trojan Hors
- Surfing Online Content
- Role Playing
- Pretexting
- Quid Pro Quo
- Vishing

https://www.smartfile.com/blog/social-engineering-attacks/

# Dumpster Diving




@mitkobogdanoski

21

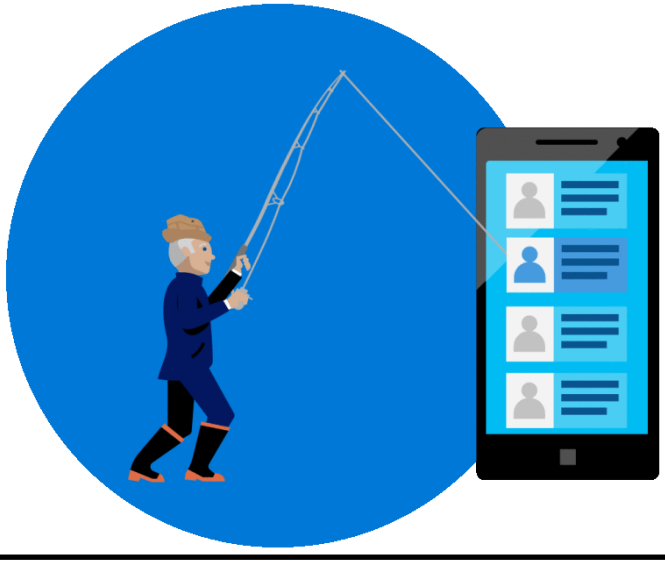
# Shoulder Surfing



@mitkobogdanoski

22

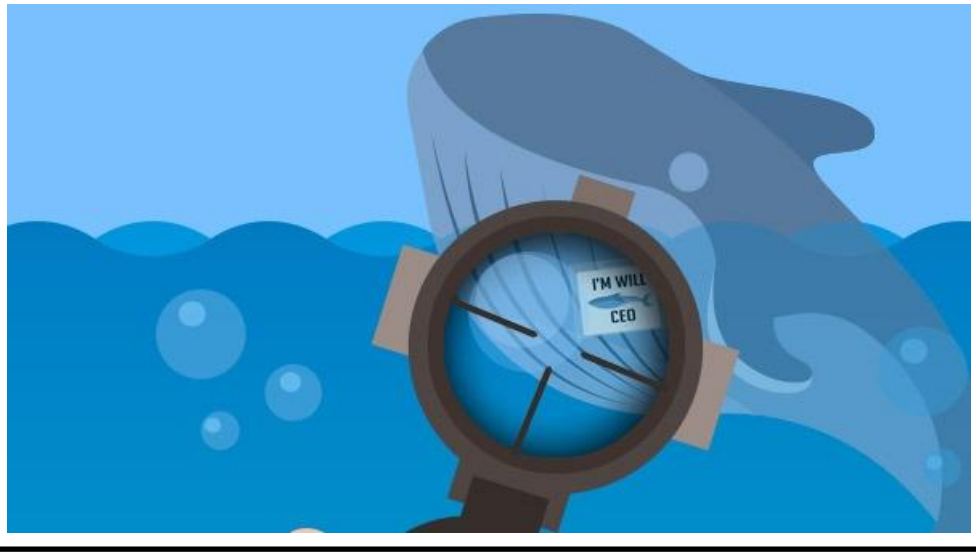
# Phishing



@mitkobogdanoski

23

# Whaling




@mitkobogdanoski

24

# Најчести знаци на фишинг

## Премногу добро за да биде вистинито

- Понуди дизајнирани на начин веднаш да го привлечат вниманието на луѓето. На пример, тврдење дека сте освоиле iPhone, лотарија или некоја друга награда.

## Чувство на итност

- Дејствувајте брзо затоа што супер зделките се само за ограничено време.
- Вашата сметка ќе биде суспендирана доколку не ги ажурирате вашите лични податоци веднаш.

## Хиперлинкови

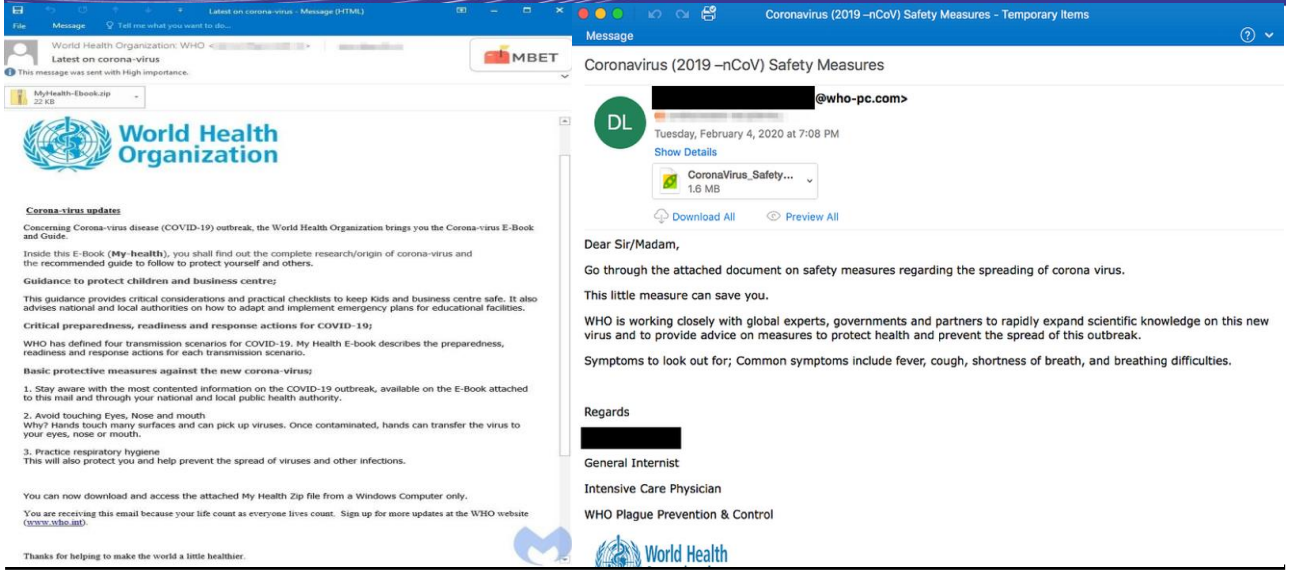
- Кликнете тука за да ја добиете вашата награда.
- Кликнете тука за да ги промените авторизациите за најава.

## Прилози

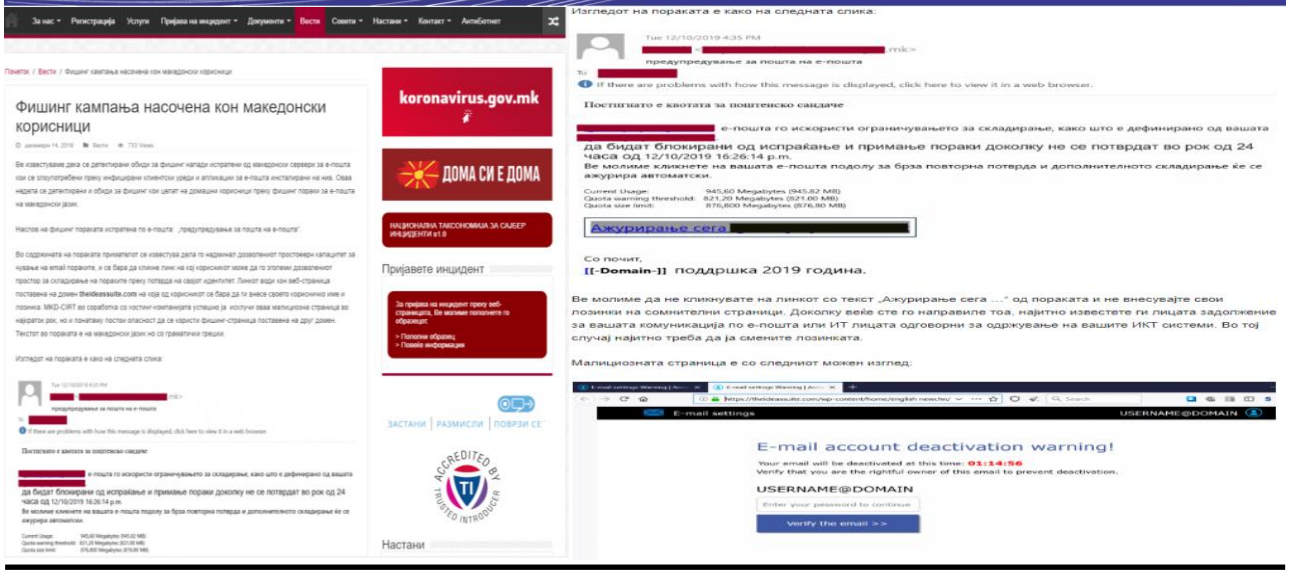
- Често содржат Ransomware, злонамерен софтвер или други вируси.



# Пример - фишинг



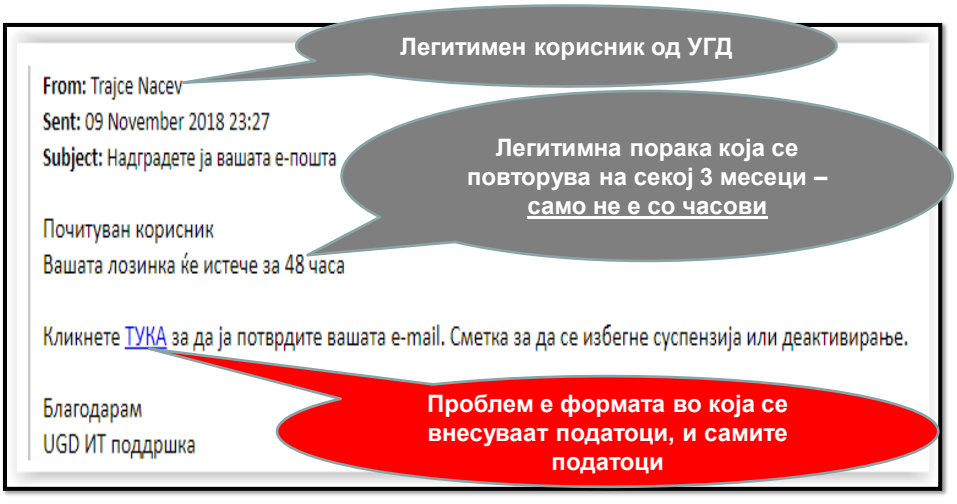
# Пример - фишинг




@mitkobogdanoski

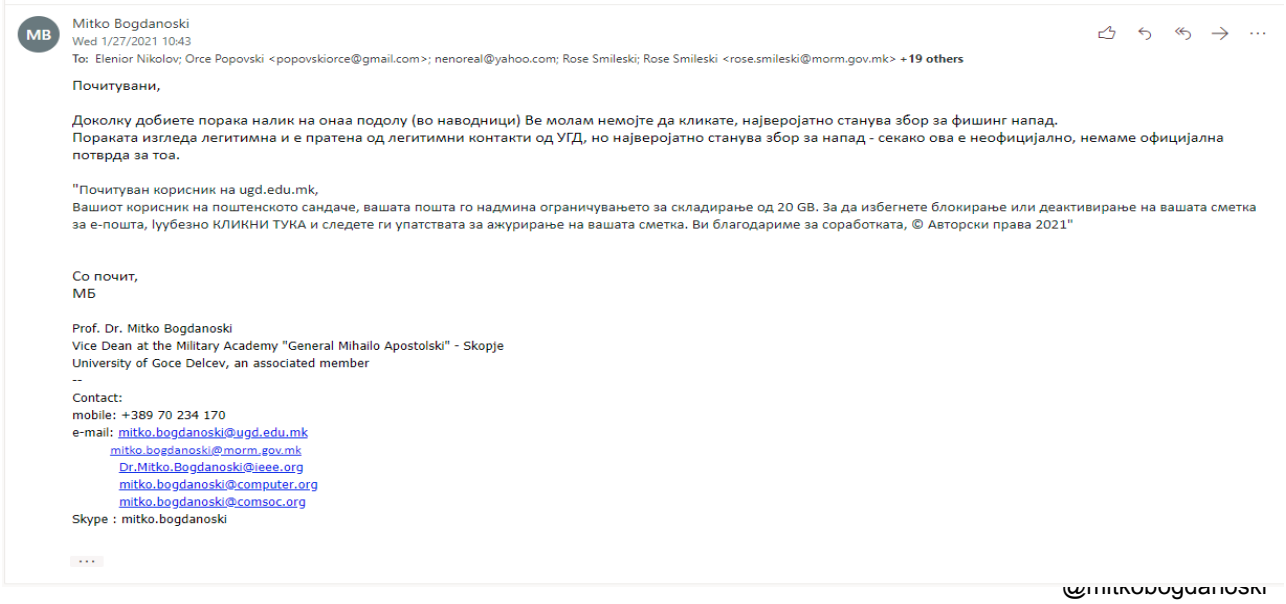


# Пример од реален phishing напад кај УГД – Штип, специфики, и како да го препознаете!




@mitkobogdanoski

# Пример - фишинг



Mitko Bogdanoski
Wed 1/27/2021 10:43
To: Elenior Nikolov; Orce Popovski <popovskiorce@gmail.com>; nenoreal@yahoo.com; Rose Smileski; Rose Smileski <rose.smileski@morm.gov.mk> +19 others

Почитувани,

Доколку добиете порака налик на онаа подолу (во наводници) Ве молам немојте да кликате, најверојатно станува збор за фишинг напад.
Пораката изгледа легитимна и е пратена од легитимни контакти од УГД, но најверојатно станува збор за напад - секако ова е неофицијално, немаме официјална потврда за тоа.

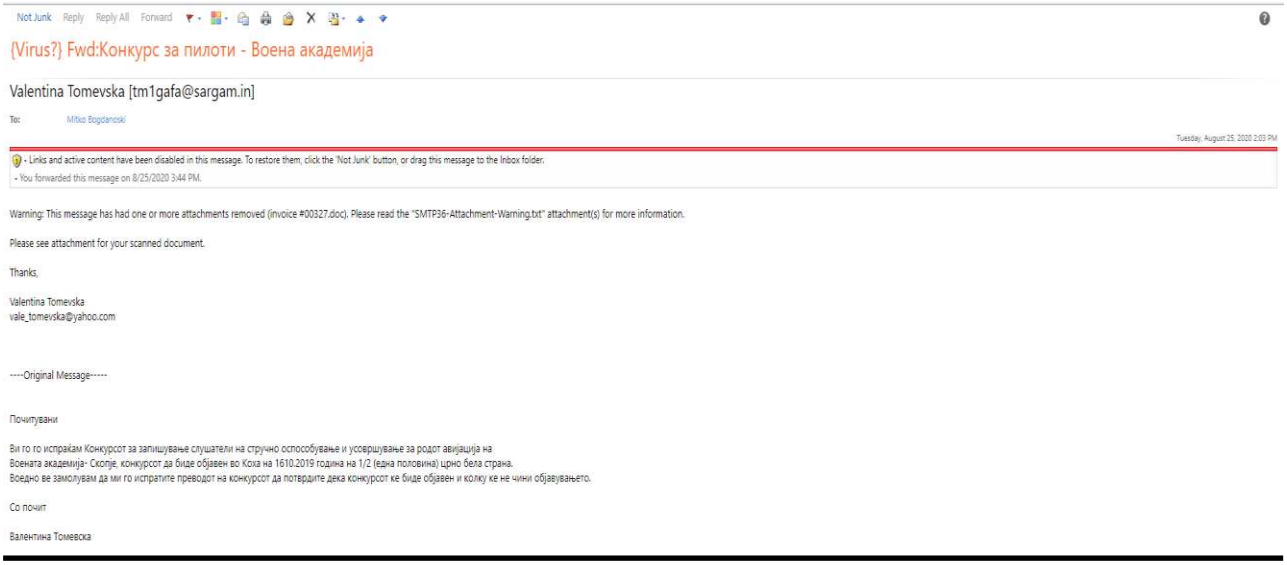
"Почитуван корисник на ugd.edu.mk,
Вашиот корисник на поштенското сандаче, вашата пошта го надмина ограничувањето за складирање од 20 GB. За да избегнете блокирање или деактивирање на вашата сметка за е-пошта, Iуубезно КЛИКНИ ТУКА и следете ги упатствата за ажурирање на вашата сметка. Ви благодариме за соработката, © Авторски права 2021"

Со почит,
МБ

Prof. Dr. Mitko Bogdanoski
Vice Dean at the Military Academy "General Mihailo Apostolski" - Skopje
University of Goce Delcev, an associated member
--
Contact:
mobile: +389 70 234 170
e-mail: mitko.bogdanoski@ugd.edu.mk
mitko.bogdanoski@morm.gov.mk
Dr.Mitko.Bogdanoski@ieee.org
mitko.bogdanoski@computer.org
mitko.bogdanoski@comsoc.org
Skype : mitko.bogdanoski



# Пример - фишинг



Not Junk Reply Reply All Forward

{Virus?} Fwd:Конкурс за пилоти - Воена академија

Valentina Tomevska [tm1gafa@sargam.in]

To: Mitko Bogdanoski

Tuesday, August 25, 2020 2:03 PM

- Links and active content have been disabled in this message. To restore them, click the 'Not Junk' button, or drag this message to the Inbox folder.
- You forwarded this message on 8/25/2020 3:44 PM.

Warning: This message has had one or more attachments removed (invoice #00327.doc). Please read the "SMTP36-Attachment-Warning.txt" attachment(s) for more information.

Please see attachment for your scanned document.

Thanks,

Valentina Tomevska
vale_tomevska@yahoo.com

----Original Message-----

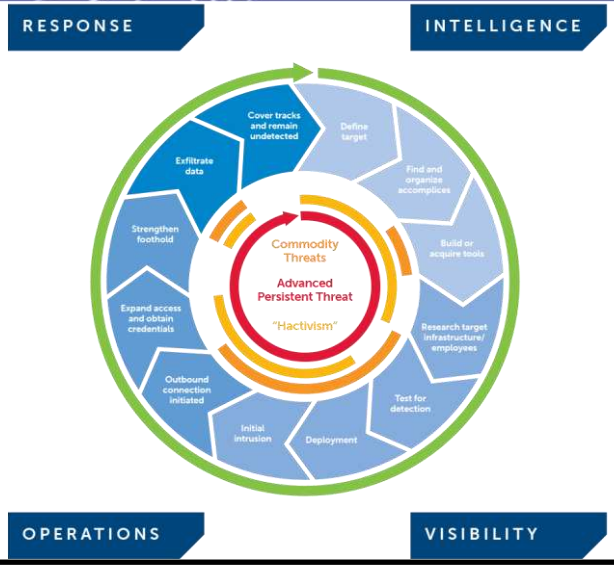
Почитувани

Ви го го испраќам Конкурсот за запишување слушатели на стручно оспособување и усовршување за родот авијација на
Воената академија- Скопје, конкурсот да биде објавен во Коха на 1610.2019 година на 1/2 (една половина) црно бела страна.
Воедно ве замолувам да ми го испратите преводот на конкурсот да потврдите дека конкурсот ке биде објавен и колку ке не чини објавувањето.

Со почит

Валентина Томевска

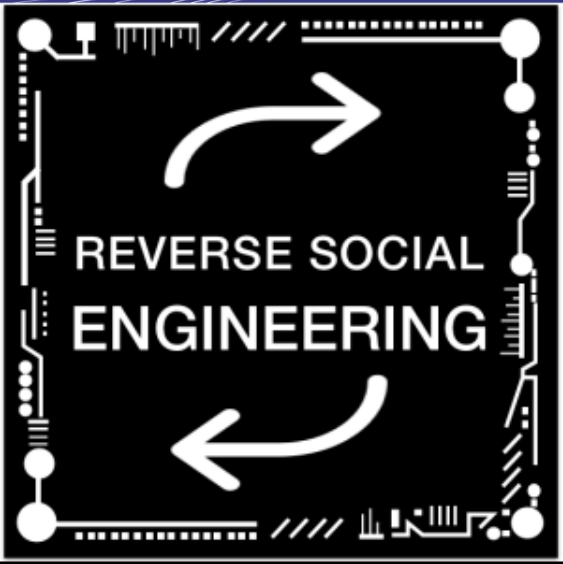
# APT (Advanced Persistent Threats)




@mitkobogdanoski

31

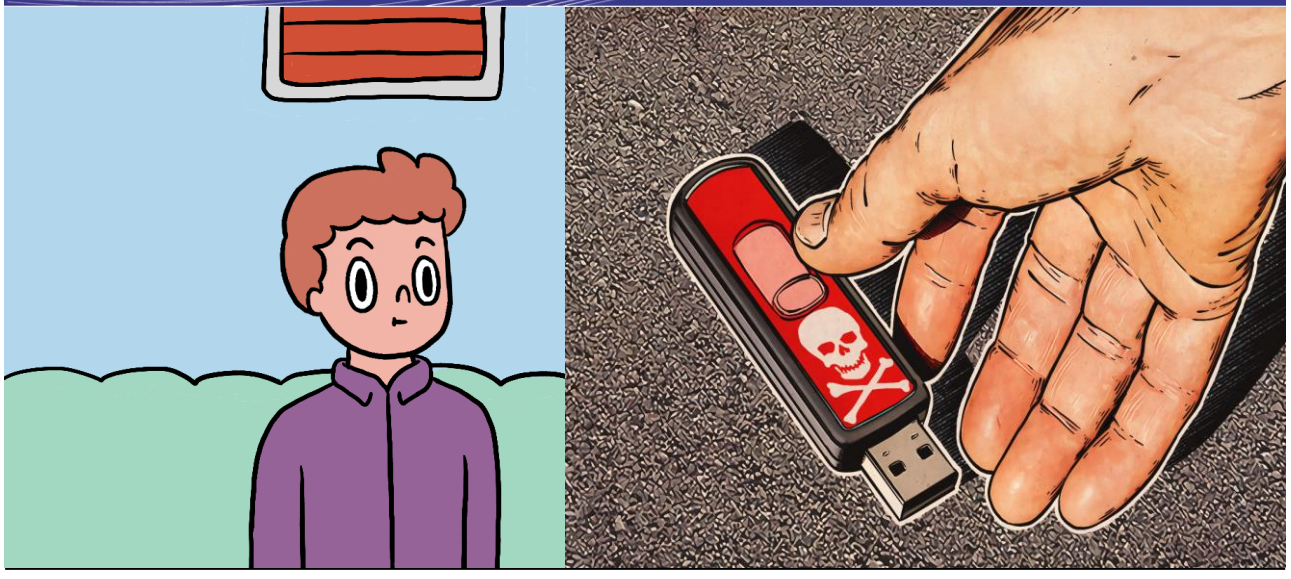
# Reverse Social Engineering




@mitkobogdanoski

33

# Baiting



@mitkobogdanoski

34

# Baiting техники

## Бесплатно преземање медиуми

Напаѓачите објавуваат линкови за преземање на web, претежно содржат злонамерен софтвер, нудејќи бесплатна музика, филм или видео игри ако целта ги предаде своите податоци за најавување на одредена страница.

## Производ со невообичаено со ниска цена

Напаѓачите рекламираат производи со исклучително ниска цена во онлајн продавница што ја создадоле, со надеж дека поединци ќе се обидат да го купат производот и да се откажат од деталите за своите кредитни или дебитни картички.

## Компромитиран USB Drive

Инфициран USB-уред што се користи за инјектирање на злонамерен софтвер, ве пренасочува кон веб-страници за фишинг или му дава пристап на напаѓачот до вашиот компјутер.

@mitkobogdanoski

35

# Quid Pro Quo




@mitkobogdanoski

36

# Waterholing (Watering Hole)




@mitkobogdanoski

37

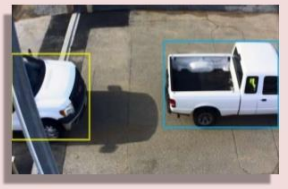
# Tailgating and Piggy Backing

**Piggy Backing occurs when an authorized individual permits others to follow behind**





**Tailgating**

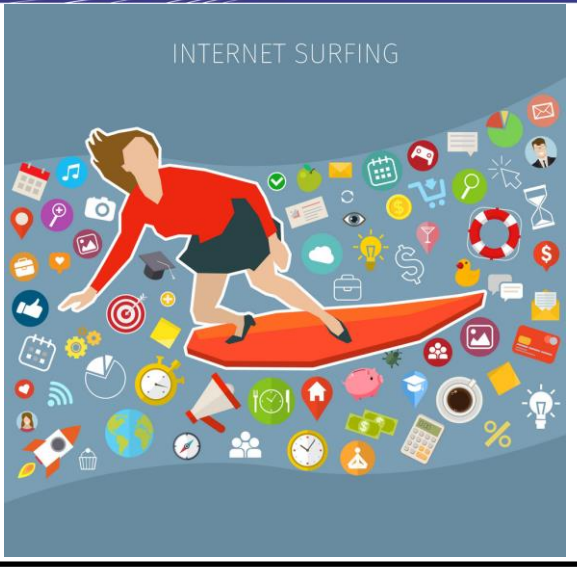




@mitkobogdanoski

38

# Surfing online content




@mitkobogdanoski

39

# Pretexting




https://www.youtube.com/watch?v=PWVN3Rq4gzw&t=114s

@mitkobogdanoski

40

# Pretexting техники и цели

## Како функционира Pretexting?

- Напаѓачите имитираат колеги, полицајци, банкари, даночни власти или добротворни организации.
- Напаѓачот гради веродостојна приказна (изговор) што не остава ни малку простор за сомнеж за нивната цел.
- Со жртвата се развива лажното чувство на доверба.
- Претекстер може да постави низа прашања дизајнирани да соберат лични информации.

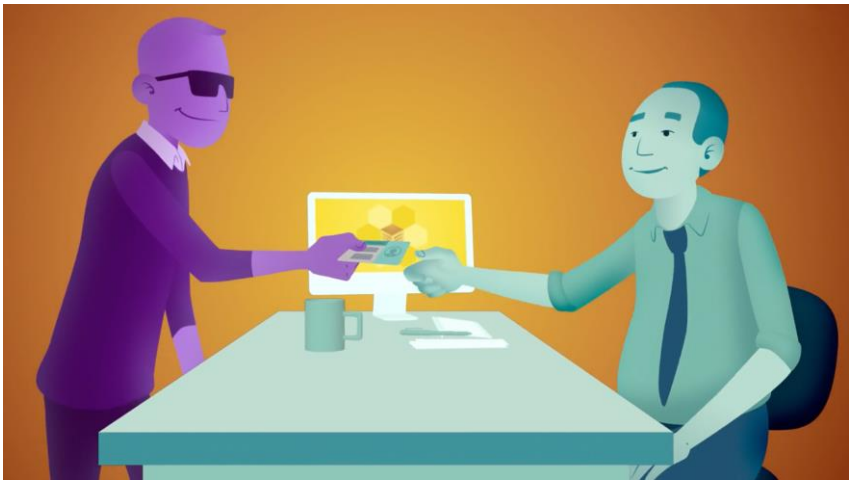
## Која е целта?

- Добијте чувствителни информации – матичен број, број на социјално осигурување, моминско презиме на мајка, место или датум на раѓање или броеви на сметка.

@mitkobogdanoski

41

# Role Playing



@mitkobogdanoski

42

# Smishing и Vishing



@mitkobogdanoski

43

# Smishing и Vishing




@mitkobogdanoski

44

# Smishing и Vishing




https://www.youtube.com/watch?v=PWVN3Rq4gzw
https://www.youtube.com/watch?v=lc7scxvKQOo&feature=emb_title

@mitkobogdanoski

45

# Smishing и Vishing

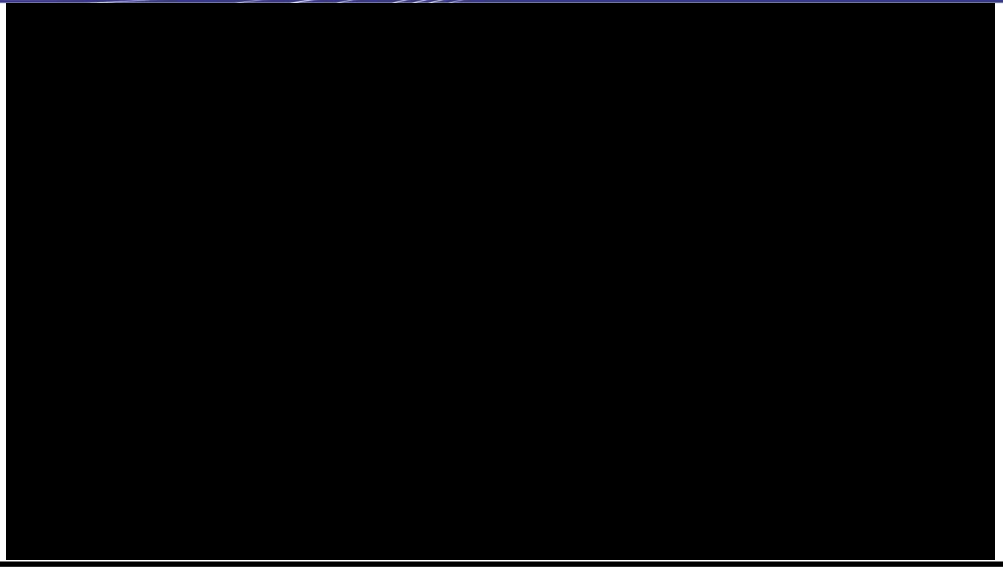



https://www.youtube.com/watch?v=PWVN3Rq4gzw
https://www.youtube.com/watch?v=lc7scxvKQOo&feature=emb_title

@mitkobogdanoski

46

# AI? и социјален инженеринг



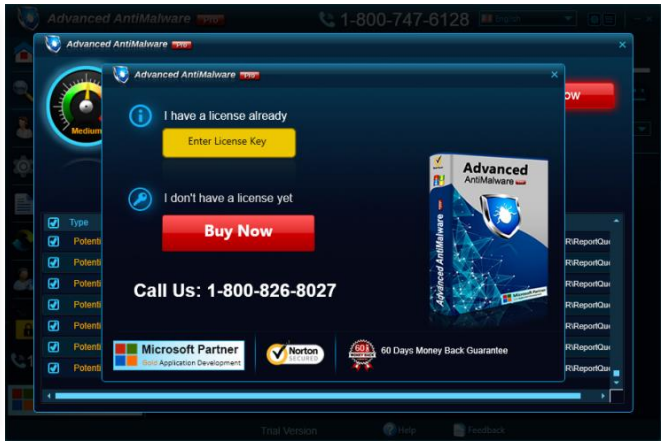
- https://www.youtube.com/watch?v=t5yw5cR79VA&feature=emb_title
- https://www.youtube.com/watch?v=B78TE_zxx8w

@mitkobogdanoski

47

# Scareware




@mitkobogdanoski

48

# Како функционира Scareware?

Најчесто генерира скокачки прозорци кои ги имитираат системските пораки на Windows, честопати препрaвајќи се дека се антивирусен софтвер. Во пораката обично се вели дека во компјутерот на корисниците се пронајдени заразените датотеки.

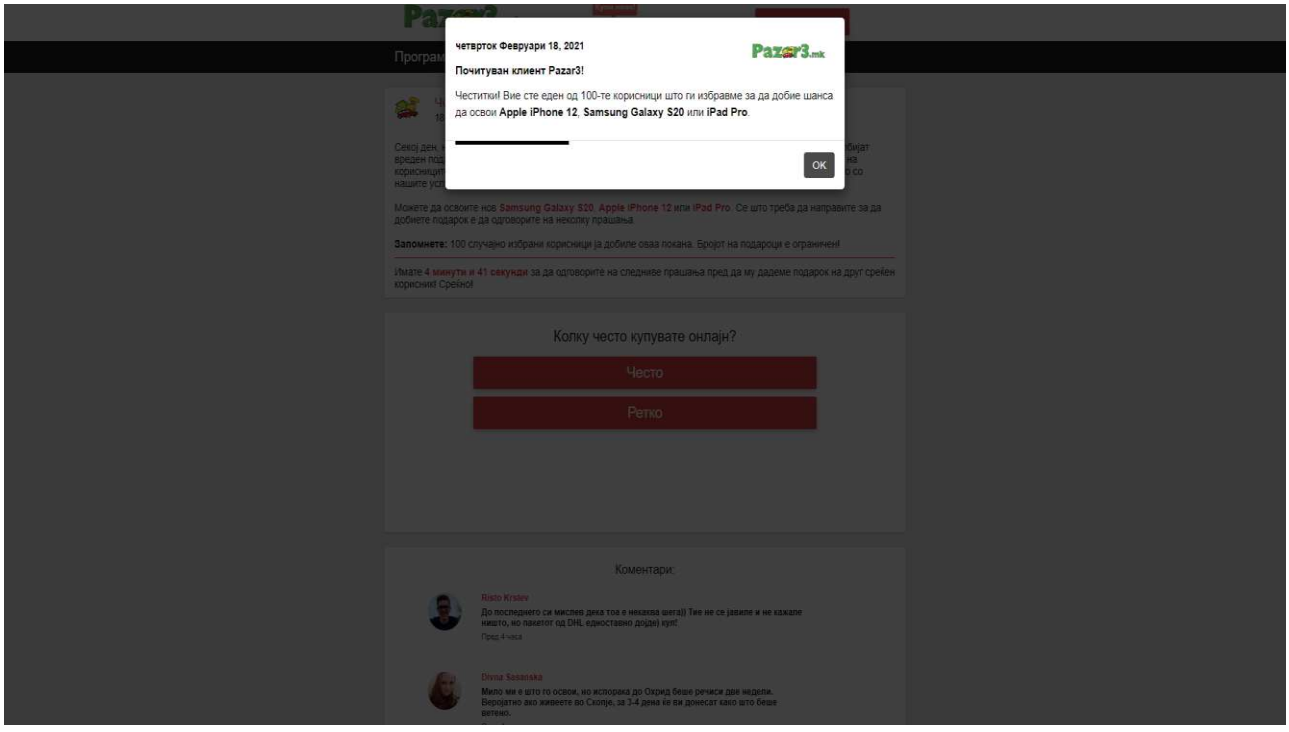
Дадена е понуда за преземање на софтвер за да се надмине проблемот или на корисникот му се препорачува да повика телефонски број прикажан во пораката за техничка поддршка.

Корисникот добива / презема софтвер кој е ефикасно бескорисен или му овозможува на напаѓачот што го повикал корисникот да се поврзе со нивниот компјутер од далечина за да инсталира злонамерен софтвер.

Парите на корисниците се губат ако се изврши плаќање, а нивниот компјутер најверојатно ќе стане нестабилен поради новоинсталираниот злонамерен софтвер.

@mitkobogdanoski

49




50

# Trojan Horse



@mitkobogdanoski

51

# Ransomware - WannaCry






# Некои препораки за одбрана од нападите со социјален инженеринг!

## Како да се избегне напад со Социјален инженеринг

- Едуцирајте се.
- Бидете свесни за информациите што ги објавувате.
- Одредете кои од вашите средства/информации се најценети за криминалците.
- Напишете добри политики, имплементирајте ги и дополнете ги ја со добри обуки за подигање на свеста.
- Чувајте го вашиот софтвер ажуриран.
- Дајте им на вработените чувство за сопственост кога станува збор за безбедноста.
- Кога ќе ве прашаат за информации, размислете дали лицето со кое разговарате навистина треба да ги има информациите за кои прашуваат.
- Внимавајте за прашања што не одговараат на лицето со кое разговарате.
- Ако некој побара информации што не знаете дали треба да ги објавите, прашајте го вашиот претпоставен.

# Одбрана од Фишинг

## Како да избегнете Phishing измами

- Не реагирајте на комуникацијата за која не сте запознаени.
- Не повикувајте телефонски броеви наведени во е-пошта, текстуална порака или инстант порака.
- Не кликнувајте на сите линкови во е-порака и не отворајте прилози содржани во сомнителна е-пошта.
- Не внесувајте лични информации во ниту еден скокачки прозорец (pop up). Легитимните организации не бараат лични информации користејќи скокачки прозорци. Контактирајте ја претпоставената организација и проверете.
- Доколку се сомневате, избришете ја е-поштата или пораката.



# Одбрана од Baiting!

## Како да се избегне Baiting измама

- Размислете двапати пред да кликнете на непознати линкови додека сурфате на мрежата.
- Користете реномирани продавачи/продавници кога купувате производи или услуги.
- Не кликнувајте на хиперлинкови кои нудат бесплатно преземање музика, филм или видео игри.
- Избегнувајте какви било линкови кои се враќаат на вашиот пребарувач и се класифицирани како реклами.
- Не вметнувајте USB уреди во вашиот компјутер што ги наоѓате наоколу. Дадете го на тимот за безбедност во вашата организација.

# Одбрана од Pretexting!

## Како да се избегне Pretexting измама

- Никогаш не давајте приватни информации за себе или за кој било друг преку телефон или Интернет, освен ако не сте го иницирале контактот.
- Легитимните организации никогаш нема да ве контактираат преку телефон и да побараат лични информации.
- Ако ви пристапи некој што не го познавате и бара лични информации за вас или некој што го познавате, веднаш завршете го разговорот. Кажете му дека сакате да ја контактирате неговата организација и прво да го проверите неговиот идентитет и мотив.



# Одбрана од Scareware!

## Како да избегнете Scareware

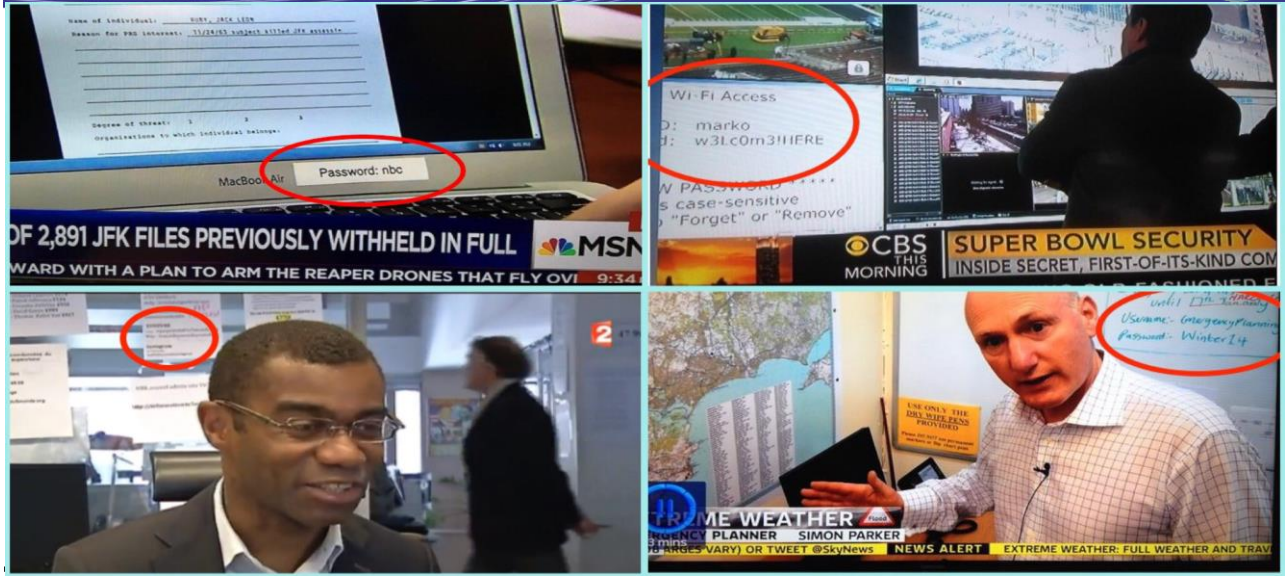
- Секогаш користете ажурирани веб-пребарувачи за да се осигурате дека се применуваат најновите безбедносни ажурирања.
- Вклучете pop-up блокатори.
- Ако добиете скокачки прозорец, целосно затворете го прелистувачот. Користете Ctrl-Alt-Delete за да го затворите прелистувачот ако не можете да го затворите нормално.
- Не кликнувајте на какви било линкови доколку ви се појави скокачки прозорец.
- Ажурирајте ја секогаш вашата антивирусна програма.
- Не давајте лични информации доколку ви се бараат во појавен скокачки прозорец.



58

59

## Please stop exposing your passwords



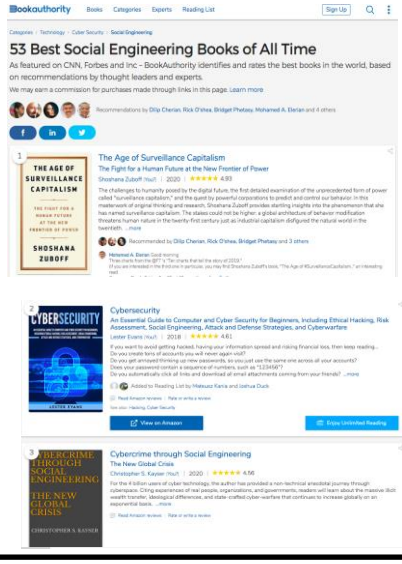

@mitkobogdanoski

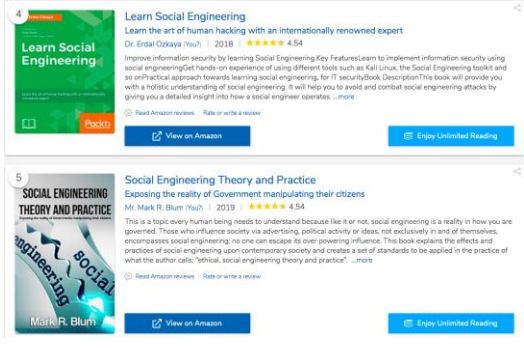
59




60

# Референци




@mitkobogdanoski

61




62