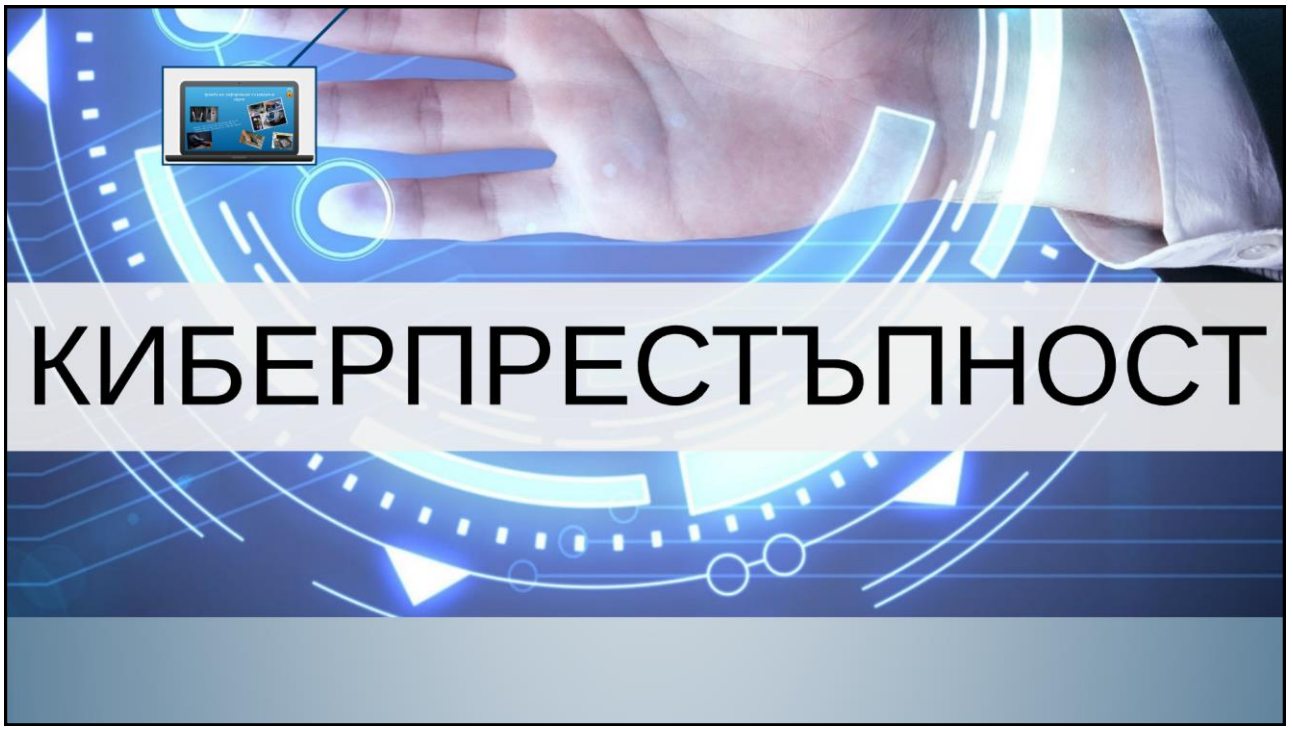

КИБЕРПРЕСТЪПНОСТТА
КАТО ЗАПЛАХА ЗА НАЦИОНАЛНАТА СИГУРНОСТ
Ръководител: проф. д-р Павел Николов
Дипломант: ЗНС - МССТ 6390 Георги Сачков

1

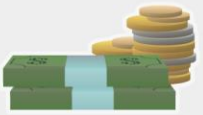

КИБЕРПРЕСТЪПНОСТ

2

СЪЩНОСТ

"Правонарушения, които са извършени срещу индивиди или групи от индивиди с криминален мотив с цел умишлена вреда върху репутацията на жертвата или причиняване на физическа или морална щета на жертвата директно или индиректно, използвайки модерни телекомуникационни мрежи като Интернет (чат, имейли, форуми и групи) и мобилни телефони (SMS/ MMS)".

Компютърно престъпление или съкратено киберпрестъпление се отнася до всеки тип престъпление, който включва компютър и компютърна мрежа.



3

Компютърни престъпления

Компютърни престъпления, на които се обръща особено високо внимание са:
- грууминг
- детска порнография
- кражби на информация по кредитни карти
- вируси
- спам
- онлайн тормоз
- онлайн активности, свързани с трафик на наркотици и др.

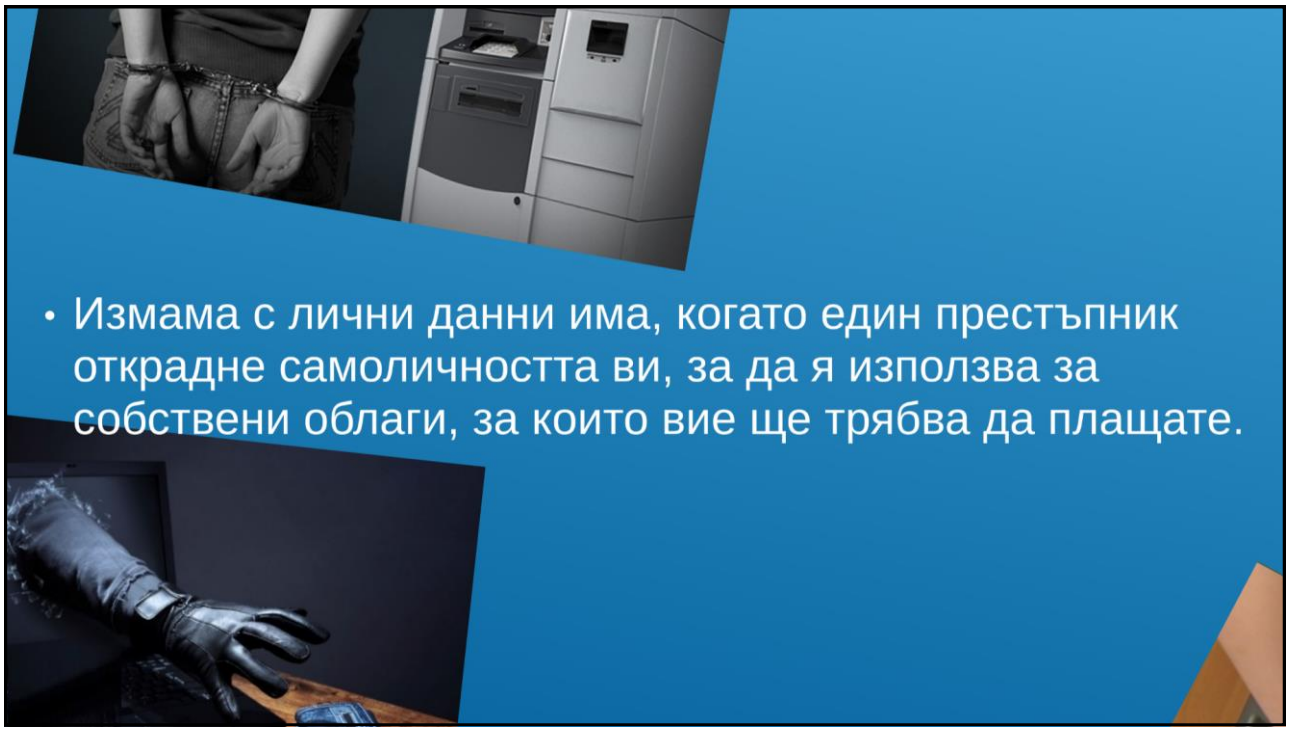
4


STOP
Груумингът е използван за въвличане на деца в сексуална експлоатация (проституция или детска порнография).

5


Грууминг
Груумингът- действия, предприети преднамерено с цел "сприятеляване" и установяване на емоционална връзка с дете, с което да се понижат задръжките му, което е в действителност подготовка за сексуална злоупотреба.
STOP
Груумингът е използван за въвличане на деца в сексуална експлоатация (проституция или детска порнография).

6


• Измама с лични данни има, когато един престъпник открадне самоличността ви, за да я използва за собствени облаги, за които вие ще трябва да плащате.

7

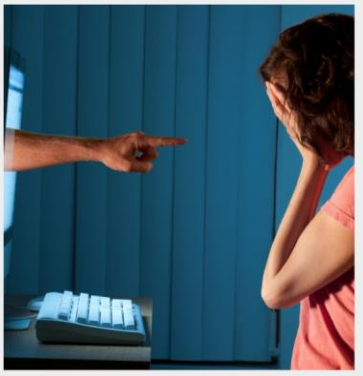

СПАМ
Inbox
Outbox
Spam (3015)
Trash
NO!
no!
NO SPAM
TODAY
TOMORROW
EVER
SPAM
Спамът, разпространяван чрез услугите за моментни съобщения е по-известен като spim.
Спам (spam) е използване на среда за електронни комуникации за масово изпращане на нежелани съобщения. Най-известната форма на спам е под формата на съобщения с рекламно съдържание по електронната поща. Спамът е използван и с други цели и използвайки други медии, като Usenet, търсачки, уеблогове, ICQ, IRC и SMS.
SPAM
SMS

8

Онлайн тормоз

Виртуалният тормоз се упражнява чрез интернет или чрез мобилниите телефони под формата на обидни или злонамерени послания, електронни писма, коментари в чата или други още по-крайни форми като уебсайтове, създадени с намерение за причиняване на вреда на отделен индивид или група от хора.

Упражняващите онлайн тормоз използват също така мобилни телефони, за да снимат другите в неудобни ситуации или да изпращат обидни sms-и или mms-и. Формите на онлайн тормоз имат много по-голям ефект от всички форми на „обикновен“ тормоз, тъй като извършителите се чувстват прикрити зад анонимността си, а жертвите не могат да се скрият от своя преследвач – те са жертви ден и нощ, навсякъде, където и да са.



9

Вируси

Вирусът е саморазмножаваща се програма, която се разпространява като вмъква копия от себе си в друг изпълним код (програми) или документи.

В компютърния свят троянският кон, наричан още троянец, е злонамерена програма, за която се твърди, че притежава някаква полезна цел, а всъщност би причинила нещо съвсем различно при изпълнението си, например: превземането на канали в IRC, изтриване на съдържание от твърдия диск, кражба на поверителни данни (пароли, информация за банкови сметки и кредитни карти) и др.

10

В компютърния свят троянският кон, наричан още троянец, е злонамерена програма, за която се твърди, че притежава някаква полезна цел, а всъщност би причинила нещо съвсем различно при изпълнението си, например: превземането на канали в IRC, изтриване на съдържание от твърдия диск, кражба на поверителни данни (пароли, информация за банкови сметки и кредитни карти) и др.

11

Кои сектори са най-силно засегнати от киберзаплахи

Случаи на сериозни заплахи, регистрирани от Агенцията на Европейския съюз за киберсигурност между април 2020 г. и юли 2021 г.

Източник: Агенция на Европейския съюз за киберсигурност (ENISA) 2021 г.

© EU/EP

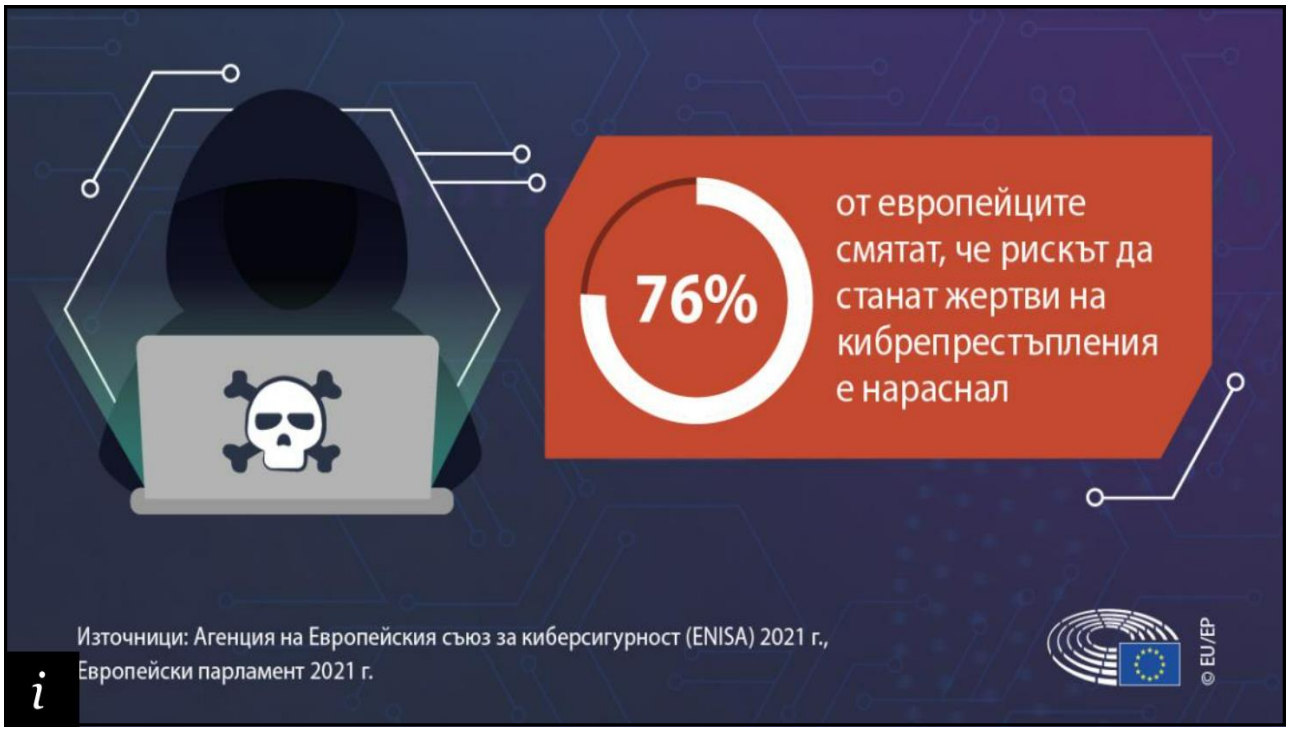
12


Основни заплахи за киберсигурността
Рансъмуер
Това се смята за най-опасната заплаха към момента
Криптоджакинг
Престъпник използва тайно компютърните устройства на жертвата, за да генерира криптовалута. През първото тримесечие на 2021 г. зловредният софтуер за добив на криптовалута се е увеличил със 117%
Атаки, насочени спрямо данни
В 85% от случаите на проникванията в данни има човешки елемент. Манипулирането на хора или човешки грешки са сред основните начини.
Източници: Агенция на Европейския съюз за киберсигурност (ENISA) 2021 г.,

13


Основни заплахи за киберсигурността
Заплахи срещу достъпността и верността
Атаки, които спират достъпа на потребители на дадена система до тяхната информация
Имейл атаки
COVID-19 все още е основна тема на имейл атаките
Заплахи за веригата на доставки
Например, атаки на доставчик на услуги, за да се получи достъп до данните на потребител. Около 58% от атаките на веригата на доставки целят сдобиването с данни
Източници: Агенция на Европейския съюз за киберсигурност (ENISA) 2021 г.,

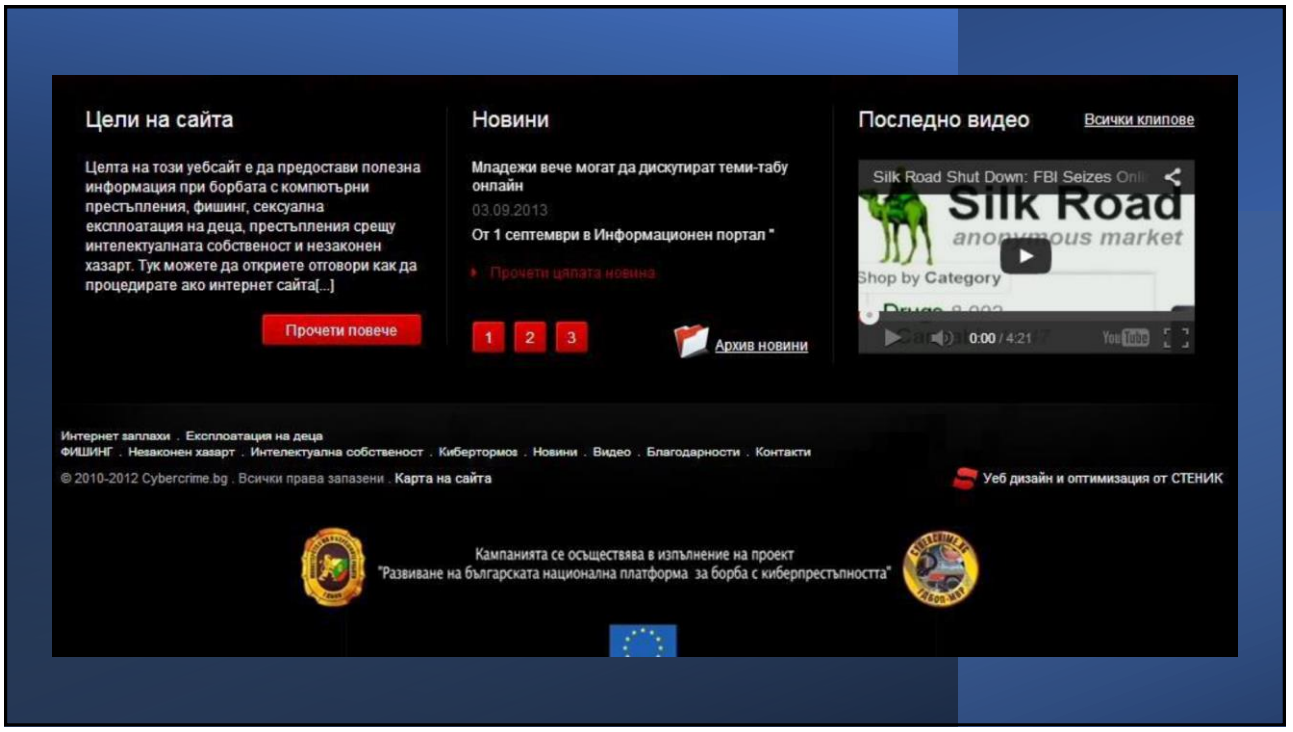
14


76%
от европейците смятат, че рискът да станат жертви на кибрепрестъпления е нараснал
Източници: Агенция на Европейския съюз за киберсигурност (ENISA) 2021 г., Европейски парламент 2021 г.
© EU/EP

15


Начало
Карта на сайта
Контакти
CyberCrime
Официален сайт за борба с компютърните престъпления
Подай сигнал
WWW.CYBERCRIME.BG
е ФИШИНГ и как да се предпазим от него? Кои са другите ални заплахи в ИНТЕРНЕТ, как да ги разпознаваме и ализираме? [Научи повече]
Защитени ли са децата ни в глобалната мрежа? Какво знаята децата и техните родители за безопасното изп интернет! [Научи повече]
тернет заплахи
Експлоатация на деца

16


Цели на сайта
Целта на този уебсайт е да предостави полезна информация при борбата с компютърни престъпления, фишинг, сексуална експлоатация на деца, престъпления срещу интелектуалната собственост и незаконен хазарт. Тук можете да откриете отговори как да процедирате ако интернет сайта[...]
Прочети повече
Новини
Младежи вече могат да дискутират теми-табу онлайн
03.09.2013
От 1 септември в Информационен портал "
Прочети цялата новина
1 2 3
Архив новини
Последно видео
Всички клипове
Silk Road Shut Down: FBI Seizes Onli
Silk Road
anonymous market
Shop by Category
0:00 / 4:21
Интернет заплахи . Експлоатация на деца
ФИШИНГ . Незаконен хазарт . Интелектуална собственост . Кибертормоз . Новини . Видео . Благодарности . Контакти
© 2010-2012 Cybercrime.bg . Всички права запазени . Карта на сайта
Уеб дизайн и оптимизация от СТЕНИК
Кампанията се осъществява в изпълнение на проект
"Развиване на българската национална платформа за борба с киберпрестъпността"

17


КИБЕРПРЕСТЪПНОСТ
ГДБОП
БОРБА С КИБЕРПРЕСТЪПНОСТТА
ГДБОП-МВР
Сигнализирайте отдел Киберпрестъпност при ГДБОП-МВР, ако сте жертва или свидетел на киберпрестъпление.
Изпратете ни имейл с подробно описание на инцидента.
ПОСОЧЕТЕ СВОИТЕ ИМЕНА, АДРЕС И ТЕЛЕФОН.
Прикачете скрийншот, снимка или логове.
Сигналите се получават и обработват в работни за България дни от 09:00 до 17:00 часа.
Обажданията се таксуват според тарифния Ви план.
Тук не се подават спешни сигнали до МВР!
Ако животът или имуществото Ви са в непосредствена опасност, наберете телефон 112.
112 се набира безплатно от всеки телефон в България.
Подайте сигнал за киберпрестъпление на
имейл report@cybercrime.bg
на телефон 0885 525 545
или посетете ГДБОП-МВР в град София, бул. "Цариградско шосе", № 133А

18

КИБЕРПРЕСТЪПЛЕНИЕ

- Компютърно престъпление (киберпрестъпление) - всеки тип престъпление, което включва компютър и компютърна мрежа.

19

PHISHING (ФИШИНГ)

- Това е широко използван похват от компютърни престъпници за получаване на важна информация.
- Явлението се нарича „фишинг” („phishing” – “зарибяване”, произлиза от fishing - риболов), защото електронните съобщения, които се разпращат, са като „въдици”.

20

ФОРМИ НА ФИШИНГ

- E-mail фишинг

Фишинг e-mail-те служат за кражба на Вашата самоличност чрез интернет пространството - потребителски имена, пароли, банкови сметки, адреси, електронни пощи и т.н.

В повечето случаи те искат от Вас да въведете лични данни или Ви пренасочват към интернет страници или телефони, където да го направите.

- Измамни връзки
- Лотарийна измама

21

ФОРМИ НА ФИШИНГ E-MAIL

- електронни писма изпратени от Вашата банка или финансова институция
- "spear phishing"
- "телефонен фишинг"
- фишинг писмата може да съдържат официални лога или други отличителни знаци, взети директно от законните интернет сайтове
- фишинг e-mail-те могат да съдържат препратки към маскирани, измамни интернет сайтове, които наподобяват на външен вид оригиналните

22

ИЗМАМНИ ВРЪЗКИ

- Може да съдържат официални лога или други отличителни знаци, взети директно от законните интернет сайтове!
- Може да съдържат препратки към измамни интернет сайтове, които наподобяват на външен вид оригиналните
- „Печатна грешка" или "cybersquatting"

Примерно адресът на Майкрософт - "www.microsoft.com" може да се срещне като:
www.micosoft.com
www.mircosoft.com
www.verify-microsoft.com

23

ЛОТАРИЙНАТА ИЗМАМА

- Една от най-използваните форми за този тип измами е съобщение "Вие спечелихте от лотарията", в което се твърди, че сте спечелили голяма сума пари или че ще Ви бъде изплатена голяма сума пари в замяна на почти никакви усилия от Ваша страна.

24

СЪВЕТИ ЗА ИЗБЯГВАНЕ НА ФИШИНГ ИЗМАМИ

1. Отнасяйте се с подозрение към всяко имейл съобщение, което иска спешно лични финансови данни.

2. Не използвайте линковете към други страници в имейли или чат съобщения, ако подозирате, че съобщението може да не е автентично.
   Въведете сами уеб адреса на страницата в уеб браузъра.

3. Избягвайте да попълвате формуляри в имейл съобщения, които искат Вашите лични финансови данни.

25

СЪВЕТИ ЗА ИЗБЯГВАНЕ НА ФИШИНГ ИЗМАМИ

4. Проверявайте дали използвате уеб сайт със сигурна връзка, когато изпращате данни за кредитна карта или друга важна информация през Вашия Интернет браузър.

5. Ако има предупреждения, че адресът на уеб сайта не отговаря на този сертификат, затворете сайта.

6. Винаги обновявайте своя уеб браузър и проверявайте дали са инсталирани обновленията за сигурност.

26

СЪВЕТИ ЗА ИЗБЯГВАНЕ НА ФИШИНГ ИЗМАМИ

7. Инсталирайте лента с инструменти за браузъра си, която сравнява адреса на сайта със списък с известни фишинг сайтове.
8. Редовно проверявайте онлайн сметките си.
9. Редовно проверявайте банковите, кредитните и дебитните си извлечения.
10. Докладвайте за фишинг и други измами в сайта Cybercrime или на адрес reportphishing@antiphishing.org

27

СЪВЕТИ ПРИ КРАЖБА НА ЛИЧНИ ДАННИ

- Кражба на самоличност се извършва, когато някой използва личните Ви данни като имена, ЕГН, осигуровки, номера на кредитни/дебитни карти или друга идентифицираща Ви информация без Вашето знание и съгласие, за да извърши измама или други престъпления.
- Ако такава информация е попаднала в измамник, Вие трябва да:
  - ❑ Съобщите за кражбата на органите на МВР, както и на компании, издали тази информация- банки и т.н.
  - ❑ Поискайте от банката Ви да блокира сметките и картите Ви и да се свържат с Вас ако има активност по тях.
  - ❑ Ако са открити сметки на Ваше име ги закрийте.
  - ❑ Ако кредитната/дебитната Ви карта е откраднатa поискайте да се издаде нова такава, с нов номер на сметката и нов PIN номер.

28

ИЗМАМА 419

Историята на НИГЕРИЙСКОТО ПИСМО

Получавате e-mail от различни африкански държави, в който се твърди, че сте избран от някой човек, за да посредничите в голям трансфер на пари, при който можете да получите огромна част от сумата.

История на Измама 419

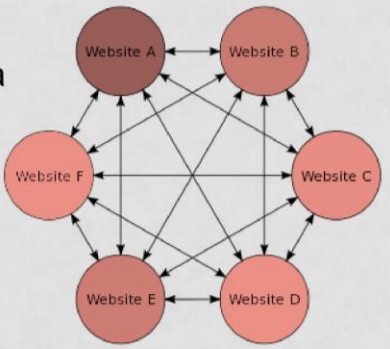
Първия вариант на подобен тип измама бил приложен през далечната 1588, когато хора получавали писма, за които се твърдяло, че са изпратени от испански затворник, държан в крепост. Въпросният затворник обещавал да подели своето богатството, ако му изпратите пари, с които до успее да под-купи надзирателите на замъка.

Измамата 419 е навлязла през ранните 90 години, когато няколко безработни нигерийски студенти я прилагат върху мнозина бизнесмени, заинтересо-вани в петролния сектор. След многократния им успех, престъпни групи започват да прилагат системата върху по-голям брой хора. Ранния вариант на 419 бил изпращан чрез писмо, факс или телекс. По-късно интернет технологията

29

ФАРМИНГ

- Измамниците завладяват домейн името на уебсайта на законна компания и прехвърлят потребителите към собствената си „спуфинг" версия на същата Интернет страница.
- Така те събират личните данни, които вие въвеждате на лъжливия сайт.
- За съжаление, адресът на страницата изглежда нормално във Вашия уеб браузър и обикновените потребители могат да направят твърде малко срещу фарминга.
- За да се спре завладяването на домейн имена, е нужно техническо решение.



30

ШПИОНСКИ СОФТУЕР

- Spyware - програма, която тайно събира информация за Интернет страници, които посещавате, и я изпраща на рекламодатели или на други заинтересовани лица.
- Програмата влиза в компютъра Ви чрез вирус или друг свален от Мрежата софтуер.
- Той нарушава тайната на съобщенията и забавя компютъра.

31

КИБЕРТОРМОЗ

- Тормозът е всякакъв вид системно малтретиране и насилие- вербално, психологическо или физическо, извършвано от индивид или група спрямо друг/и.
- Тормозът е във всички случаи неморално и неприемливо поведение.
- Той не трябва никога да бъде пренебрегван или игнориран

- **Кибертормозът** представлява тормоз, който се извършва по Интернет и други комуникационни технологии.
- Например могат да се използват СМС-и, обаждания, имейли, чат съобщения, друг вид комуникация и/или клипове.
- В България клиповете и съобщенията са много разпространен метод.

32


КОГА ДА СПОДЕЛЯ И ПОТЪРСЯ ПОМОЩ?
проблеми в семейството ти
ако нещо неочаквано и сериозно се е случило
ако си объркан и не знаеш как да подредиш нещата
HELP
ако някой упражнява насилие над теб
ако някой те заплашва
ако се чувстваш заплашен или несигурен
проблеми в училище

33


ИНТЕРНЕТ Е ГЛОБАЛНА СВОБОДА!
БЛАГОДАРЯ ЗА ВНИМАНИЕТО!
Георги Сачков
МССТ 6390
ЗНС
Киберпрестъпността като заплаха за национална сигурност

34