КИБЕРПРЕСТЪПЛЕНИЯ И БЕЗОПАСНОСТ В ИНТЕРНЕТ

Презентация за ученици

Лектор: инж. Метин Хюсеин
Системен администратор
Районен съд – Генерал Тошево

1. **Киберпрестъпление** е всеки тип престъпление, който включва компютърна техника и компютърна мрежа.

- Целта на престъплението е умишлена вреда върху репутацията на жертвата или причиняване на физическа или морална щета на жертвата директно или индиректно, използвайки телекомуникационни мрежи като Интернет (чат, имейли, форуми и групи) и мобилни телефони (SMS/MMS).
- Такива престъпления застрашават също така националната сигурност.

2. Phishing (фишинг)

- разпращат електронна поща, която претендира, че идва от почтена компания, и се опитва да убеди получателя да даде важна лична или финансова информация.
- Фишинг e-mail-те служат за кражба на Вашата самоличност чрез интернет пространството - потребителски имена за достъп, 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.

3. ФОРМИ НА ФИШИНГ

- Може да изглеждат като електронни писма, изпратени от Вашата банка или финансова институция, с която имате редовни бизнес отношения или от сайта на Вашита социална мрежа.
- "spear phishing“ - маскирани са като писма от някой, който Вие познавате. Тези писма използват унифицирана форма за масови съобщения от добре известни на "жертвата" компании, учреждения или сайтове като eBay и PayPal. Подателят е човек, който може да е от институцията, в която работи получателят или по принцип човек, чиято работа предполага връзки с клиенти или служители на компанията.

3. ФОРМИ НА ФИШИНГ

- "Телефонният фишинг“ - изисква се от Вас да проведете телефонно обаждане. "Телефонният фишинг" Ви препраща директно към отдела за поддръжка, на който да позвъните. Съответно от другата страна чака човек, който да вземе Вашия номер на сметка, личния Ви идентификационен номер, парола или друга ценна лична информация. Като причина за провеждане на телефонният разговор, често се твърди, че регистрацията Ви ще бъде прекратена или ще има проблеми с нея, ако не предприемете действия.

"Ако не отговорите до хх часа, Вашата регистрация ще бъде прекратена“

3. ФОРМИ НА ФИШИНГ

- **Може да съдържат официални лога или други отличителни знаци, взети директно от законните интернет сайтове! Също така може да съдържат и убедителна информация, отнасяща се до Вас, която измамниците са намерили в социалните мрежи.**
- **„Печатна грешка" или "cybersquatting„ - Може да съдържат препратки към маскирани, измамни интернет сайтове, които наподобяват на външен вид оригиналните, където искат от Вас да въведете лична информация. Примерно адресът на Майкрософт - "www.microsoft.com" може да се срещне като:**
  www.micosoft.com
  www.mircosoft.com
  www.verify-microsoft.com

3. ФОРМИ НА ФИШИНГ

- *Лотарийната измама* е често срещана фишинг 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. Лотарийната измама често включва препратки към големи компании като Yahoo например.

4. СЪВЕТИ ЗА ИЗБЯГВАНЕ НА ФИШИНГ МЕЙЛИ

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 .

Вместо това се обадете по телефона на Вашата компания или сами въведете уеб адреса на страницата в уеб браузъра.

3

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

4. СЪВЕТИ ЗА ИЗБЯГВАНЕ НА ФИШИНГ МЕЙЛИ

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.

4. СЪВЕТИ ЗА ИЗБЯГВАНЕ НА ФИШИНГ МЕЙЛИ

6

Инсталирайте лента с инструменти за браузъра си, която да ви помогне в борбата с фалшиви сайтове. Тези ленти сравняват адреса на сайта, на който сте попаднали, със списък с известни фишинг сайтове.

7

Редовно проверявайте онлайн сметките си.

8

Редовно проверявайте банковите, кредитните и дебитните си извлечения, за да проверите дали всички парични преводи са легитимни .

4. СЪВЕТИ ЗА ИЗБЯГВАНЕ НА ФИШИНГ МЕЙЛИ

9

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

10

Докладвайте за фишинг и други измамни имейли в сайта Cybercrime

или на адрес reportphishing@antiphishing.org

5. СЪВЕТИ ПРИ КРАЖБА НА ЛИЧНИ ДАННИ

Кражба на самоличност се извършва, когато някой използва личните Ви данни като име и фамилия, 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.**

5. СЪВЕТИ ПРИ КРАЖБА НА ЛИЧНИ ДАННИ

- Свържете се с органите на МВР, за да подадете жалба.
- Свържете се с всички други институции/организации, които работят с личните Ви данни.
- Записвайте имената и телефоните на всички, с които разговаряте за случая. Добре е да потвърждавате телефонните обаждания с писма. Пазете копия на цялата кореспонденция.

6. ИЗМАМА 419

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.

From: Mr. Manager National bank of Fujairah Dubai

Asaad Aleelwi

Скрито копие: Мен

From: Mr. Manager National bank of Fujairah Dubai
Branch, UAE DUBAI.

Hello friend,

My name is Dr Asaad Aleelwi, I am the regional manager of the National bank of Fujairah Dubai in the City of Dubai UAE. I got your information during my search through the Internet. I am 58 years of age and married with 2 lovely kids. It may interest you to hear that I am a man of PEACE and don't want a problem, I only hope we can assist each other. If you don't want this business offer kindly forget it as I will not contact you again.

I have packaged a financial transaction that will benefit both of us, as the regional manager of the National bank of Fujairah Dubai; it is my duty to send in a financial report to my head office here in the city of Dubai at the end of each year. On the course of the last year 2020 end of year report, I discovered that my branch in which I am the manager made NINE million five hundred and fifty thousand dollars [9,550.000.00] which my head office are not aware of and will never be aware of. I have since placed this fund on what we call SUSPENSE ACCOUNT without any beneficiary.

As an officer of the bank I can not be directly connected to this money, so this informed my contacting you for us to work so that you can assist receive this money into your bank account for us to SHARE. While you will have 50/50 of the total fund. Note there is practically no risk involved, it will be bank to bank transfer or through ATM CARD. all I need from you is to stand as the original depositor of this fund who made the deposit with our branch so that my Head office can order the transfer to your designated bank account. If you accept this offer to work with me, I will appreciate it very much. As soon as I receive your response I will give you more details on how we can achieve it successfully once you contact me strictly through my personal email address: (asaadaleelwi14@gmail.com).

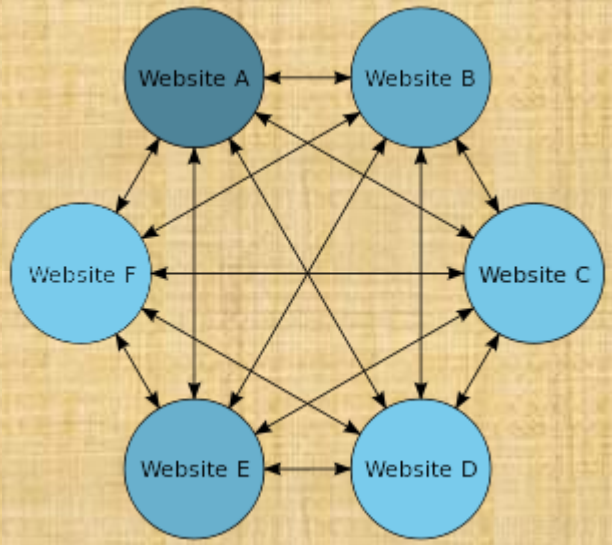
Kind regards,
Dr. Asaad Aleelwi,

7. СПУУФИНГ

- **СПУУФИНГЪТ /от английската дума spoof-пародия, измама/ е имитация на електронно съобщение или на уебсайт, направена от измамници, за да се създаде впечатление, че съобщението или сайтът принадлежат на някой друг.**
- **Фишинг атаките обикновено започват с разпращането на непоискани „спууф" съобщения, които изглеждат като изпратени от законна компания. Така че спууфингът е основна част от фишинга.**

8. ФАРМИНГ

- Измамниците завладяват домейн името на уебсайта на законна компания и прехвърлят потребителите към собствената си „спууфинг” 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.



9. 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.

10. ДЕТСКАТА ПЕДОФИЛИЯ

- Продажбата на детска порнография носи огромни печалби.
- Престъпниците влизат в контакт с малолетните и непълнолетните често представяйки се за техен връстник.
- Подмамват ги да им дадат техни снимки или видеозаписи.

11.КИБЕРТОРМОЗ

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

- **Обидни коментари, унизителни снимки или видео.**
- **Виртуалните заплахи понякога се пренасят в реалния живот и може да се стигне до физически нападения и боеве.**
- **Наблюдава се и обратното-често жертвата в реалния живот става насилник във виртуалния.**

12. СЕКСТИНГ

- Изпращане на снимки или видео, текст с еротично или сексуално съдържание- най-често през мобилен телефон или сайтове.
- Обикновенно е между двойка партньри.
- Но в последствие ако те се разделят, то някой от тях би могъл да злоупотреби със снимките, публикувайки ги.

13. КАК ДА СЕ ЗАЩИТИМ?

14. КОГА ДА СПОДЕЛЯ И ПОТЪРСЯ ПОМОЩ?

15. КЪДЕ ДА ПОДАМ СИГНАЛ?

Гореща онлайн линия за подаване на сигнали

www.web112.net

ТЯ води Борба с вредното и незаконно съдържание и поведение онлайн

web112.net
гореща линия за безопасен интернет

16. КЪДЕ ДА ПОДАМ СИГНАЛ?

Център за безопасен интернет

www.safenet.bg

Създаден е за съвети за деца и тийнейджъри, учители и родители, тестове и игри.

онлайн

CyberCrime

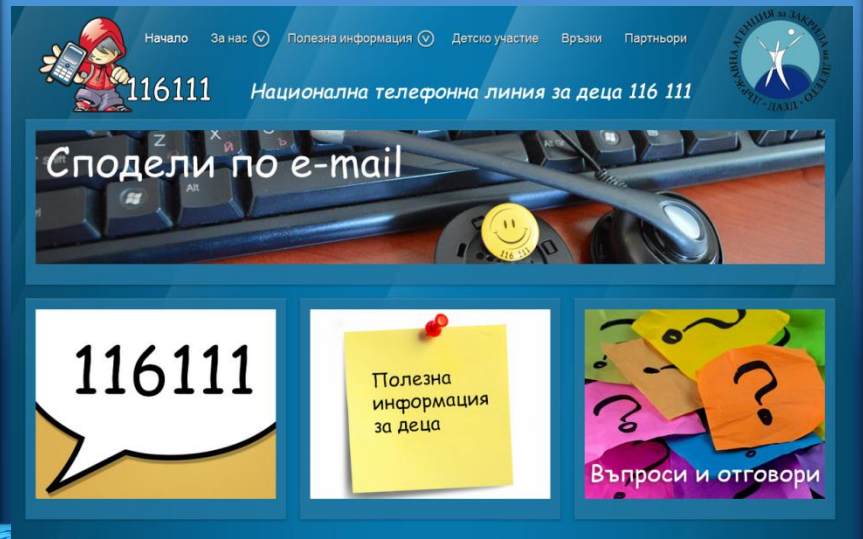
Официален сайт за борба с компютърните престъпления

www.cybercrime.bg

17. КЪДЕ ДА ПОДАМ СИГНАЛ?

- Споделете с някого, на когото имате доверие.
- Разговорът с родител, приятел или учител обикновено е първата стъпка за решаване на всеки проблем.

116 111



ИНТЕРНЕТ Е ГЛОБАЛНА СВОБОДА!

НО ИНТЕРНЕТ НЕ Е БЕЗОПАСЕН!

ВИНАГИ ВНИМАВАЙ!

ЗАЕДНО МОЖЕМ ДА НАПРАВИМ ИНТЕРНЕТ ПО-ДОБЪР И БЕЗОПАСЕН!

БЛАГОДАРЯ ЗА ВНИМАНИЕТО!

Източници: www.safenet.bg , www.cybercrime.bg , www.google.bg