Мария Цекова Тодорова

ТГ"Васил Априлов"- гр. Червен бряг

Рискови отношения онлайн- кражба на самоличност!

Цели:

Разбиране на рисковете при използване на Интернет и последствията от достъпа до личните ни данни и злоупотребата с тях.

Разграничаване на различни видове кражба на самоличност.

Да се разберат основните защити от кражба на лични данни.

Начало на урока – 10 минути. Встъпителна част

Дискусия по следните въпроси:

- Какво се разбира под фразата: кражба на идентичността /самоличност/?
- Позволявали ли сте на приятел да се представи в интернет пространството от ваше име?
- Използва ли някой друг вашето име при работа на компютър?
- Предоставяли ли сте паролите, които използвате на други лица?
- Известни ли са ви случай на кражба на самоличност? / примери/
- С каква цел се краде чужда самоличност?

Учениците споделят личното си мнение и гледна точка при определяна на проблема, свързан с кражбата на идентичност. Възможни са даване на примери. Дискусията завършва с изводи за огромните възможности, които ни предоставя интернет, но и за опасностите от невярна, погрешна или изкривена информация.

Речник:

Фишинг- е злонамерен опит за придобиване на информация като потребителско име, парола и детайли на лични сокументи, като извършителят приема чужда самоличност при електронни комуникации

Троянски кон (Trojan) - злонамерена компютърна програма, която се представя като полезна, а всъщност причинява нещо съвсем различно при изпълнението си,например: изтриване на съдържание от твърдия диск, кражба на поверителни данни (пароли, информация за банкови сметки и кредитни карти) и др.

Защитна стена (firewall)- специализиран хардуер или софтуер, който проверява мрежовия трафик, преминаващ през него и разрешава или забранява достъпа по определени правила.
Интернет- е глобална система от свързани компютърни мрежи, която чрез стандартен комплект протоколи TCP/IP обслужва милиарди потребители по целия свят.
Онлайн социалната мрежа- платформа за изграждане на социална мрежа или социални взаимоотношения между хора, които споделят общи интереси, дейности, история или познания.
Лични данни- Лични данни са всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци (например ЕГН, № лична карта и др.)

Изложение – 18 мин

План на урока

1. Видове кражба на самоличност
   а/ Създаване на нов профил
   б/ Присвояване на чужд профил
   в/ Криминален профил
   г/ Кражба на медицинска самоличност
   д/ Кражба на трудова самоличност.
   е/ Кражба на бизнес самоличност
   ж/ Клониране на самоличност
2. Защита от кражба на лични данни

Видове кражба на самоличността

Присвояването на чужда самоличност е сред най-предпочитаните от кибер престъпниците методи за онлайн измама. Целта често е извличане на финансова изгода и основни мишени са номера на кредитни карти, банкови сметки, социални осигуровки и т.н. Кражбата на самоличност може да се използва и за достъп до компрометираща информация, изнудване, прикриване на истинската самоличност и ред други незаконни дейности.

а/ Създаване на нов профил

За създаването на нов профил измамника използва лична информация, като номер на социалната осигуровка (в САЩ), ЕГН или номер на личната карта, за да открие нов акаунт на името на жертвата. Обикновенно това е нова кредитна карта, банкова сметка или заем, сключване на договор с мобилен оператор и други.
Тъй като измамниците предоставят фиктивен адрес за получаване на известия и извлечения от финансовите институции, откриването на измамата може да стане след месеци и дори години.
Най-добрите методи за защитата срещу подобно престъпление са да пазите личните си

данни "*лични*" във всички възможни случаи. Освен това ако редовно следите балансите по сметките си, можете по-лесно да засечете неправомерни действия с тях. Широко разпространени са и услугите за мониторинг на кредитното състояние на клиента (т.нар. кредитни бюра), с които бързо се установява, ако бъдат открити нови сметки на негово име. За съжаление повечето такива услуги все още не са добре познати в България.

б/ Присвояване на чужд профил е много подобна на горната, но вместо създаване на нов акаунт, измамника се възползва от вече съществуващ - например банкови сметки, кредитни и дебитни карти, разплащателни сметки, мейл акаунти, дори телефонни номера. Обикновенно престъплението е наказуемо, когато е свързано с финансови измами. Те обаче се засичат и поправят трудно, тъй като банките не са склонни да затварят сметки и да възстановяват откраднати суми без предварително щателно разследване, което може да се проточи дълго.
Защитата от подобна измама отново е свързана с редовни банкови извлечения и справки в кредитните бюра. Освен това потребителите трябва да внимават за фишинг сайтове, да не предоставят лична информация (особено идентифицираща, като PIN номер на карта) по електронна поща или телефон, да сканира редовно комютъра си за вируси и spyware.

в/ Криминален профил - е измама, при която някой прикрива извършено престъпление зад чужда самоличност. Обикновенно това става с фалшива лична карта или шофьорска книжка, но все по-разпространена става и онлайн алтернативата. Например, ако някой хакне частна WiFi мрежа и извърши непозволени действия (сваляне на цифрово видео, музика или нелицензиран софтуер, включване в атака срещу уеб сайт и т.н.), те могат да се проследят обратно до източника и жертвата да се превърне едновременно и в обвиняем. Хакването на лични мейл акаунти и профили в социални мрежи и други сайтове също е неприятна разновидност на този тип измама, която може да се използва за заплахи, изнудване, опит да се откраднат данни на жертвата или нейни приятелите и други.Най-добрия начин потребител да се защитата от "криминална кражба на самоличността" е да използва силни пароли, при това различни за всеки негов профил в мрежата. Освен това не бива да пази ценна информация в архива на електронната си поща или другаде онлайн (особено пароли за достъп до други акаунти или номера на кредитни карти, PIN идентификатори и други). Редовният ъпдейт на антивирусния софтуер, както и ползването на защитни стени също е препоръчително.

г/ Кражба на медицинска самоличност- една от най-опасните измами, тъй като може пряко да застраши жертвата. При този вид заплахи, измамника използва лични данни като име на жертвата, номера на здравни или социални осигуровки и други, за да получи "безплатни" медицински грижи, медикаменти или трудно достъпни рецепти. Тъй като здравната история на всеки пациент се пази в обща система, всяка фалшива информация в нея може да доведе до вземане на фатални решения, касаещи

действителната личност.
Предвид организацията на здравната система, кражбата на медицинска самоличност е разпространена предимно в САЩ, но експерти предупреждават, че този вид кражба на самоличност ще става все по-популярна и отвъд океана.
Тази измама не е много разпространена в България. И това е така, защото нивото на здравната ни система е изключително ниско. Няма електронни здравни досиета, а за получаване на определени лекарства, заплащани или дотирани от единствената ни здравна каса не е проблем да се ползват подставени лица.

д/ Кражба на трудова самоличност. Напоследък има множество случаи, при които хора се водят фиктивно на работа, без да знаят. В същото време по ведомости "получават" заплати и дори непознати за тях работодатели им внасят осигуровки. Машинацията се прави, за да могат фирмите да си намаляват данъците и да точат ДДС с кухи обороти. Това ставало най-вече със строителни обекти. Разминаването излиза наяве, след като се засекат данните между регистрациите на безработните и информационните масиви на Националния осигурителен институт, обясняват експерти, които вече са се сблъскали с такива измами. За да се предпазим е необходимо да следим личната си кореспонденция с Националния осигурителен институт. Най-малко веднъж годишно НОИ изпраща писмо, в което уведомява всеки гражданин за осигурителния му статус с данни за осигурителите и периода за осигуряване. Ако сме родени след 1959 г. то такива писма следва да получаваме и от избрания от фонд за задължително допълнително осигуряване. Ако по някаква причина не сме получили такива писма, тои ниобходимо да се регистрираме в съответните справочни системи на официалните сайтове на НОИ или съответния осигурител и там провереме статуса си. Така може да открием и дали работодателите са били коректни към нас и са внасяли осигуровки върху пълния обем от трудовото ни възнаграждение.

е/ Кражба на бизнес самоличност е друга бързо разпространяваща се измама напоследък. При нея, както подсказва и името, целта на измамника е получи кредит от името на бизнес организация или да отклони финансови разплащания в своя полза. Съвременните фирмени регистри и дори само фирмената информация, достъпна в Агенцията по вписванията дава възможност на недоброжелатели да се сдобият не само с личните данни на лице, представляващо дадена фирма, но и с копия от оперативни документи, като заявления, платежни нареждания, решения на управителните органи и пр. Със съвременните технологии изработването на дубликат на фирмения печат е лесно. От там нататък остава само едно фалшифицирано пълномощно и пътят за източване на фирмените сметки е отворен. Практиката показва, че най-често зад кражбата на бизнес самоличност стоят бивши или настоящи служители, имащи достъп до оперативните документи на фирмата. Стриктният контрол върху персонала и ограниченият достъп до важни фирмени ресурси е един от методите за защита срещу подобно престъпление. Хубаво е разплащания над определени суми да се правят по банков път и да се избягват чести тегления на големи суми в брой, особено когато това не е наложително.

ж/ Клониране на самоличност
Това е особен вид измама, която включва микс от горните. Разликата е, че обикновенно измамника действа в продължителен период от време и се стреми да се сдобие със всякаква лична информация за жертвата. Мнозина определят клонирането като най-

сериозната от всички видове кражби на самоличност, тъй като трудно се засича и доказва. Освен това, в много случаи, когато измамника извлече достатъчно ползи от жертвата, той може да клонира друга самоличност и процеса започва отначало. Клонирането поражда и някои притеснения относно въвеждането на електронните документи за самоличност, тъй като в крайна сметка те могат да се хакнат както аналоговите си събратя.
Кражбата на идентичност и на-бързо развиващата се престъпност в Европа. Криминални групи крадат личната ви информация като име, адрес, рожденна дата,за да си открият банкови сметки , да си усигурят заеми, да получат кредитни карти или документ за самоличност- паспорт или шофьорска книжка. Крадците могат използвайки нашето име да натрупат големи дългове, което в последствие да се отрази на нашата сигурност и дори да бъдем подведени под съдебна отговорност като длъжници.

Как да се предпазим? При изгубване или кражба на лични документи, особено на лична карта, незабавно трябва да уведомите съответното териториално управление „Полиция“! Ако става дума за банкова карта, то уведомете обслужващата ви банка за незабавно блокиране.

Защита от кражба на лични данни

/ Учениците могат да дадат различни предположения за предотвратяване на кражба на лични данни! Учителят изслушва и записва на дъската, след което обяснява основните форми на защита, изброени по-долу/

1. Инвестирайте в сигурен и широкоспектърен софтуер за защита, който предпазва от вируси, шпионски софтуер (спайуеър), рекламен софтуер (адуеър), хакери, нежелани съобщения (спам), фишинг измами и кражби на идентичност.

2. Винаги осъществявайте достъп до интернет през защитна стена. Тя добавя ниво на сигурност между вашия компютър и интернет, като по този начин пречи на хакерите да откраднат вашата самоличност, да унищожат файловете ви и да използват вашия компютър, за да атакуват други потребители.

3. Използвайте компютър, за който знаете, че е безопасен. Хакерите могат лесно да изтеглят вашите важни данни, ако те се изпращат по незащитена интернет връзка. Ако трябва да изпратите поверителна информация или да направите онлайн транзакция, използвайте компютър, за който знаете, че е сигурен и не забравяйте, че има много нива на сигурност. Някои компютри имат само минимална защита, докато други, като например тези с McAfee Total Protection, имат пълна сигурност.

4. Пазете се от фишинг измами. Те използват подправени имейли и уеб сайтове, маскирани като законен бизнес, за да привлекат нищо неподозиращи потребители да разкрият частни сметки или потребителски имена и пароли за вход. Дори и да имате защитен компютър, пак можете да посетите злонамерен сайт, без да го осъзнавате. Законните фирми никога няма да ви помолят да обновите своята лична информация през електронната поща. Винаги проверявайте уеб адресите, преди да предоставите вашата лична информация.

5. Защитете вашата безжична мрежа. Изложените сте на риск, ако осъществявате достъп до интернет през безжична връзка. Тъй като радиовълните на безжичната мрежа преминават през стени, хакер с обикновена антена може да ви атакува от километри разстояние, за да открадне вашата информация и да използва вашата безжична мрежа за собствената си комуникация. Затова винаги използвайте допълнителна защита за вашата безжична мрежа.

6. Никога не инсталирайте потенциално нежелани програми като шпионски и рекламен софтуер на вашия компютър. Много безплатни програми, които сте изтеглили чрез интернет, въпреки че изглеждат безвредни, са специално разработени да ви наглеждат, да следят вашите потребителски имена и пароли за достъп, да препращат вашата конфиденциална информация или да пренасочат браузера ви към фалшиви сайтове. Някои от тези програми могат да бъдат инсталирани на компютъра ви чрез едно просто кликване върху рекламна връзка в интернет. Със защитен софтуер вие можете да спрете тези програми от инсталиране. Никога не инсталирайте доброволно програми от подобни сайтове, освен ако не сте запознати предварително с дадения уеб сайт и програмата и сте прочели внимателно крайното споразумение.

7. Не отговаряйте на верижни имейли. Дори и да имате защита на вашия компютър, някои верижни имейли са препратени от ваши приятели и могат да поискат лична информация. Не изтегляйте файлове, пратени от семейство и приятели, освен ако не знаете съдържанието на файла и знаете, че то е безопасно.

8. Наблюдавайте вашите кредитни справки и бъдете наясно с вашата кредитна информация. Най-малко веднъж годишно проверявайте вашата кредитна история. Това е един от най-добрите начини да установите дали някой използва вашата лична финансова информация без ваше знание.

9. Правете редовно архивиране на важната за вас информация. Съхранявайте копие на вашите важни данни на преносими медии. Използвайте софтуер с инструменти за бекъп, ако е възможно, и съхранявайте резервните копия, които ще ви послужат в извънредни ситуации.

/ Възможно е да се добавят още варианти, споменати от учениците-Н-р: Престъпниците крадат идентичността като се сдобиват с личната ни информация!Могат да се преровят кошчетата за боклук за лични документи и после да се свържат с нас като се представят за служители на закона , компания или банка. Необходимо е всички финансови документи не просто да се хвърлят, а да се накъсат на малки парчета и никога да не се дава лична информация на някой, който се е свързал с нас по телефон или и-мейл.

Винаги да следим сметките си. Трябва да зннаем за какво сме похарчили парите си и да проверяваме отчетите си по сметка, която получаваме.

Никога да не се използват банкови пароли за регистрация в интернет страници.

Ако решим да не използваме кредитнати си карта- не можем просто да я унищожим-н-р като я срежем. За дезактивация трябва да информираме доставчика си иначе картата ни

ще остане активна. Личните документи е желателно да стоят на сигурно място! На крадците е по-лестно да ги отмъкнат тях, вместо някаква техника./

Заключителна част – 7 минути.

Учениците изказват становища , обобщавайки от получената за часа информация как оптимално могат да се възползват от интернет и да се предпазят от опасностите , свързани с предоставяне на лична информация . В края на урока трябва да се разбират опасностите и формите на предпазване при работа с компютър, използване на wi-fi, пароли, проследяване на съмнителни линкове и предоставяне на лични документи пред непознати хора.

/Възможност за домашна работа- изготвяне на плакат на тема: Рискови отношения онлайн- кражба на самоличност!/