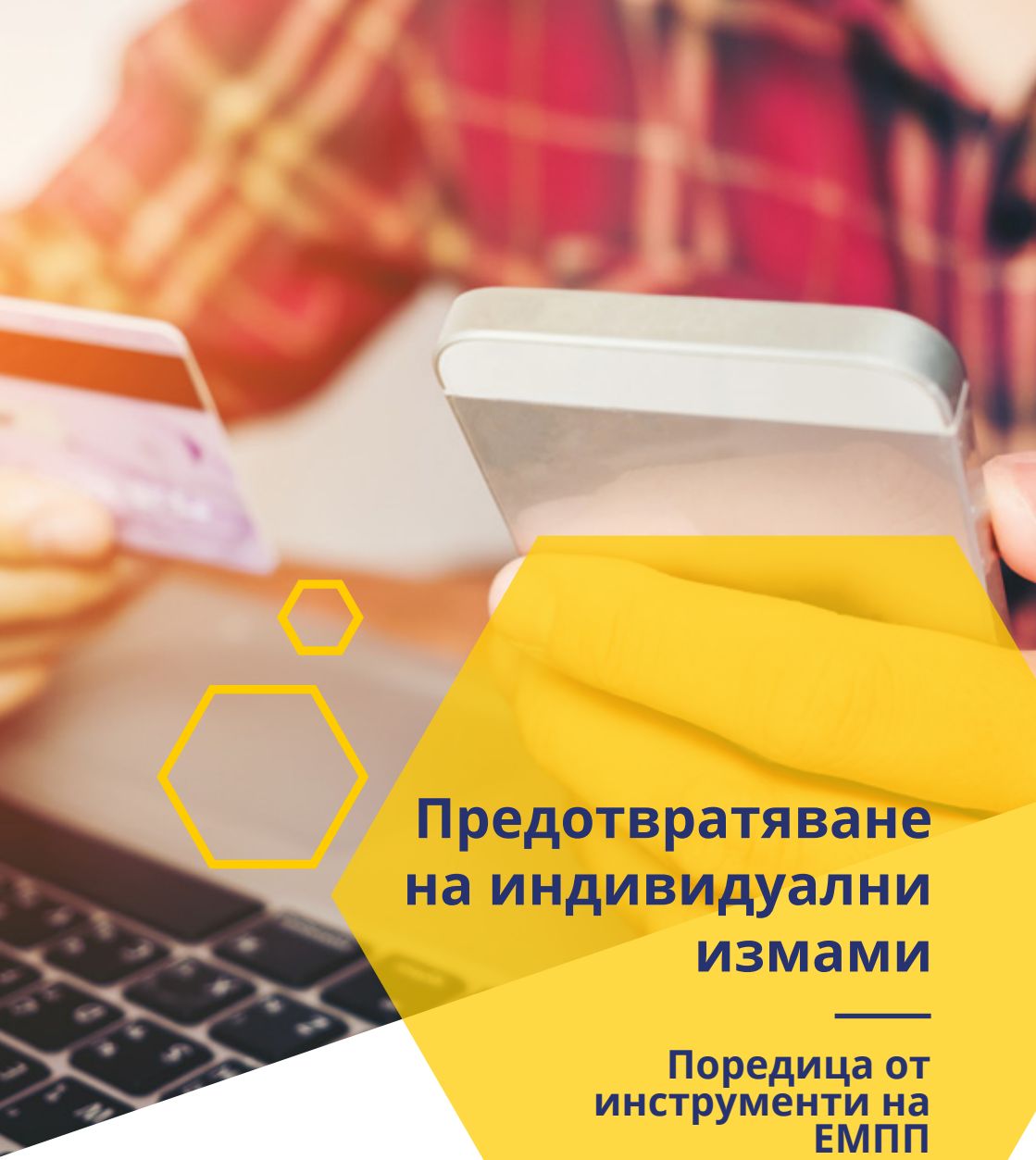


Предотвратяване на индивидуални измами

Поредица от инструменти на ЕМПП

№ 13

EUCPN
EUROPEAN CRIME PREVENTION NETWORK

eu2018bg.bg
Българско председателство на Съвета на Европейския съюз

Individual fraud is a type of fraud in which individual citizens are being targeted by criminals and are persuaded into a cooperative mindset. The essential tactic to nudge the victim into this compliant relationship is called social engineering. This allows the offender to obtain the confidence from the victim that is crucial to the success of the scam.

БЛАГОДАРНОСТИ

Позовавания
ЕМПП (2018 г.). Поредица от инструменти на ЕМПП № 13 „Предотвратяване на индивидуални измами “.. Брюксел

Правна информация
Съдържанието на настоящата публикация не отразява непременно официалното становище на която и да е държава членка на ЕС или на която и да е агенция или институция на Европейския съюз или на Европейските общности.

Автори/редактори
Жорн Ване, длъжностно лице по въпросите на изследванията, секретариат на ЕМПП, Брюксел, Белгия
Феб Лиагр, длъжностно лице по стратегията и политиката в Брюксел, секретариат на ЕМПП, Брюксел, Белгия

В рамките на проекта „По-нататъшно прилагане на многогодишната стратегия за ЕМПП и неформалната мрежа за административен подход“ – Секретариат на ЕМПП, ноември 2018 г., Брюксел

С финансовата подкрепа на програмата на Европейския съюз „Предотвратяване и борба с престъпността“ Европейска комисия — Генерална дирекция „Вътрешни работи“

Този набор от инструменти е разработен в тясно сътрудничество между Секретариата на ЕМПП и българското председателство. Бихме искали да им благодарим за положените по време на това председателство усилия и за организирането на семинар по темата за телефонните измами.

Освен това бихме искали да благодарим на всички национални представители на ЕМПП, на заместниците и на звената за контакт с академичните среди за постоянната им подкрепа за нашата дейност, за споделянето на експертен опит и за предоставянето на информация за настоящия набор от инструменти.

Бихме искали по-специално да благодарим на експертите, които проявиха желание да участват в семинара, организиран от нас във връзка с този набор от инструменти:

- Марк Бътън, Университет в Портсмут, Обединено кралство
- Майкъл Уил, Европол, AP Furtum
- Симеон Димчев, отдел „Измами“ в Главна дирекция „Национална полиция“, България
- Шарлота Маурицсон, Национален център за борба с измамите, Швеция
- Андрис Боманс, Център за киберсигурност, Белгия
- Константин Лица, Отдел за борба с измамите, Румъния
- Аурелиан Бокан, главна дирекция на полицията на Букурещ, Румъния
- Романа Мазалова, проект „Nedáme se“, Чешка република

СЪДЪРЖАНИЕ

03

Примери от практиката 72

Endnotes 86

ЦИТИРАНИ ИЗТОЧНИЦИ 87

ПРЕДГОВОР

13ият набор от инструменти в поредицата, публикуван от Секретариата на ЕМПП, е насочен към основната тема на българското председателство: измамите, със специално внимание към телефонните измами. Тъй като измамите обхващат широк кръг от теми, решихме да стесним фокуса до индивидуалните измами. Това понятие обхваща измамите, извършени срещу физически лица от физически лица или престъпни организации. Тези измами, които все повече се увеличават, се превърнаха в печеливш трансграничен бизнес, като някои специалисти дори наричат извършителите „скамър предприемачи (scampreneurs)". Ето защо за такива престъпления е необходим общ за ЕС подход. Това е видно и в документа за политиката, който е изготвен в писмен вид с този набор от инструменти.

Наборът от инструменти се състои от три части. В първата се прави опит за създаване на актуална разузнавателна картина на индивидуалните измами. В рамките на втората част се обсъждат интересни добри практики, както и някои препоръки относно начините за предотвратяване на измами по телефона. Въпросните добри практики са изброени в третата част. На читателя се предоставя и резюме.

КРАТКО ИЗЛОЖЕНИЕ

13-ият набор от инструменти в поредицата, публикуван от Секретариата на ЕМПП, е насочен към предотвратяването на индивидуални измами. Българското председателство (първата половина на 2018 г.) реши да се съсредоточи върху:

> *„[...] въпроси , свързани с измама, по-специално телефонни измами. Този вид престъпност се превърна в печеливша престъпна дейност през последните години, която се развива както на национално, така и на трансгранично равнище. Престъпните групи, специализирани в тази дейност, се развиват динамично и поразяват по-широк кръг от жертви. Като се има предвид активното участие на жертвите, въвличането им в престъпните сценарии и травматизиращите последици за тях, трябва да бъдат положени сериозни превантивни усилия, като се вземат предвид особеностите на местно, национално и трансгранично равнище."*

Индивидуалните измами са вид измама, при която престъпниците се насочват към отделни граждани. Жертвите биват убедени да сътрудничат и след това стават жертва на измама. Настоящото ни разбиране за този вид измама е свързано главно със съвременните му форми, най-вече т.нар. „фишинг". Важно е обаче да се отчете, че индивидуалните измами са свързани с определена възрастова група. Технологичното развитие през последните десетилетия само позволява тези измами да се развият в много по-голям мащаб, отколкото някога се е считало за възможно. Кой не е получавал някога фишинг имейл?

Както се посочва ясно в обосновката от българското председателство, жертвите активно участват в своята виктимизация. Целта на извършителя е да вземе парите на жертвата, но той може да получи достъп до тях само като убеди жертвата да му ги даде. Основната тактика за склоняване на жертвата към такова поведение се нарича **„социален инженеринг"**. Това позволява на извършителя да спечели доверието на жертвата, което е от решаващо значение за успеха на измамата. Социалната психология ни предлага по-добро разбиране на това явление. Като използват обичайните социални принципи и „човешките слабости", извършителите са в състояние да активират т.нар. периферен път на убеждаване. За прекия път са необходими много съобразителност и познавателни усилия. За периферния обаче не е нужна

прецизна подготовка и се реагира почти несъзнателно. Например като се преструва на служител на властта, да речем полицейски служител, нарушителят може лесно да подчини своите жертви. Тези социални и познавателни правила от практиката имат ежедневна употреба, но позволяват на нарушителите да се възползват от тях за собствена изгода.

Въпросните измамни тактики се използват в широк **спектър от измами**.. т.нар. измами 419, измами на възрастни жени, романтични измами, CEO измами ... възможностите са безкрайни като креативността на измамниците. Гамата от измамни схеми позволява на измамниците да се насочат към много голяма аудитория едновременно или да възприемат по-индивидуализиран подход. Вторият случай се среща все по-често. Измамниците са осъзнали, че при умело таргетиране на жертвите „възвръщаемостта на инвестициите“ е по-висока. Фишинг имейлите стават все по-сложни и са адресирани до определена целева група. Последната изненадваща стъпка в тази еволюция е свързана с комбинацията от нова и по-стара технология: телефонът. Т.нар. вишинг, или гласов фишинг, дава възможност за комбиниране на предимствата на интернета и телефона. Едно онлайн телефонно обаждане не струва почти нищо, трудно може да бъде проследено и може да бъде направено автоматично. Използването на телефона има допълнителни предимства: хората му вярват повече и убеждаването е по-ефективно поради по-интимната обстановка. Показателен факт за нарастващото ниво на сложност: извършителите на престъпления дори наемат местни носители на съответния език, за да могат телефонните разговори да звучат възможно най-автентично.

Настоящото ни разбиране за индивидуалните измами обаче е ограничено. Броят на тези престъпления е огромен **и неуточнен**, тъй като много от тях не се съобщават. Жертвите не знаят, че са станали такива, не възприемат станалото достатъчно сериозно, не смятат, че съобщаването ще доведе до нещо, или просто не знаят къде да съобщят. В допълнение, поради активната роля, която жертвата играе за собственото си виктимизиране, усещането за самообвинение и притеснението възпират жертвите да разкажат своята история. При някои измами дори има „вградени“ механизми за предотвратяване на съобщаването, тъй като жертвите трябва да предприемат незаконни действия в рамките на схемата, което ги инкриминира в процеса. Съобщаването на измама би довело до чувство за съучастничество.

Фактът, че броя на измамите не е известен, е довел и до **мита**, че възрастните хора са основните жертви на това престъпление, тъй като те са лесна плячка.

Някои изследвания опровергават този мит, въпреки че трябва да останем предпазливи поради ограничените налични проучвания. При все това се съобщава, че по-младите хора и тези на средна възраст са по-податливи на измами. Според друг разпространен мит жертвите обикновено са описвани като необразовани или неграмотни финансово, а изглежда, че е обратното. Едно от възможните обяснения се нарича „несъответствие между знанието и действието" (knowing-doing gap), при което хората успешно разпознават сигналите на измама, но не отнасят тези знания към собственото си положение.

За съжаление, съществуването на т. нар. **„списъци на вече измамените"** не е мит. Извършителите на телефонни измами могат да се свързват с жертвите на случаен принцип или чрез търсене в публичните регистри, но също така споделят помежду си списъци с набелязани лица, които вече са били измамени. Използването на такива списъци е показателно за високото равнище на повторна виктимизация. Например някои измамници ще се опитат да „помогнат" да възстановите загубите си...

Тъй като контролът от страна на полицията на това престъпление е изключително труден, необходимостта от превенция е голяма. Въпреки това са проведени малко академични изследвания и изследвания за оценка на индивидуалните измами. Все пак можем да установим някои общи констатации. Най-популярната тактика за превенция е информирането на обществеността. Това може да се направи чрез обща кампания за повишаване на осведомеността, но особено когато се предоставя под някаква форма на обучение, трябва да се отбележат някои положителни ефекти. По същество подобни обучения се опитват да премахнат несъответствието между знанието и действието, което споменахме по-горе. Друга ключова тактика е да се работи с жертвите. Поради активната им роля и съществуващия риск от многократна виктимизация жертвите следва да получават подкрепа и да бъдат наясно със своето специфично положение.

По време на българското председателство секретариатът събра редица **добри практики** по този въпрос. Те могат да бъдат категоризирани според целевата група. Първата категория е насочена към цялото население. Това са кампании за повишаване на осведомеността, като примерите от България, Швеция, Белгия или Европол. Те включват радиоемисии, плакати, листовки, сувенири и др., които предоставят полезна информация на обществеността и показват как да се предпазвате от посегателство. Втори набор от дейности е насочен

към възрастните хора. Тук се използват повече интерактивни методи, какъвто е случаят в Чешката република. Възрастните хора участват в интерактивен образователен сценарий, в който се запознават с най-разпространените измамни схеми и как да реагират на тях. Този „приложен на живо опит" би трябвало да им даде възможност да реагират адекватно в реални ситуации. Оценката на този проект доказа, че това предположение е вярно, тъй като групата е отказала фалшиви сделки два и половина пъти повече, отколкото контролна група, която не е гледала разиграването на сценария. Последната категория включва превантивни дейности, насочени към жертвите. Примери от Австралия, Обединеното кралство и Канада показват необходимостта от такъв вид превенция. Въпреки това, дори и в световен мащаб, има малко услуги за подпомагане на жертвите на отделни измами.

И накрая, секретариатът на ЕМПП организира семинар с участието на различни експерти, който да изготви някои препоръки относно начините за предотвратяване на измами по телефона. Те са структурирани в съответствие с петте стратегии за превенция на ситуационната престъпност. Първата възможна стратегия е да се увеличат усилията,които извършителят трябва да положи, за да успее измамата. Това вече може да бъде постигнато чрез ограничаване на публикуването и достъпа до телефонни номера. Друга техника би могла да бъде ограничаване на количеството телефонни номера, което едно лице може да има или най-малкото да свърже с банкова сметка или идентификационен номер.

Втората стратегия е да се увеличат рисковете. Тук обменът на информация е от ключово значение. Този обмен не следва да спира на границите на публичния или частния сектор или на национално равнище. Всички партньори имат важна роля в попълването на информационния пъзел. По принцип познаването на това, с което се занимавате, увеличава шансовете за превенция на подобни случаи. Излишно е да се посочва, че съобщаването следва да стане и да се прилага по-лесно. Необходимо е да се събере информация, преди тя да бъде споделена. Направени бяха и други препоръки, за да се намали анонимността на обаждащия се, като се направи почти невъзможно да се проследи местоположението Ви. В това отношение би могъл да представлява интерес и софтуер за гласово разпознаване.

Намаляването на ползите, които могат да бъдат постигнати чрез извършването на това престъпление, е трета стратегия за предотвратяване на измами по телефона. Тук основната препоръка е изземването на незаконно

придобитите активи. За тази цел следенето на паричните потоци е от решаващо значение за откриване на съмнителни сделки. Нашите експерти препоръчаха общоевропейска инициатива, която да улесни банковия сектор.

Друга стратегия е да се намалят провокациите. В това отношение важното е да не се споделя твърде много информация за това как точно е извършена измамата, тъй като това ще попречи на действия на имитатори. Това би могло да спомогне за намаляване на определени форми на повторна виктимизация.

Последната стратегия е да се премахнат оправданията. Това е насочено основно към повишаване на осведомеността относно телефонните измами и начините да се защитите сами. Добрите практики от предходните години са показани като ключови примери в това отношение. Кампаниите за повишаване на осведомеността следва да разпространяват едно и също послание. Поради това е необходимо да се установят и да бъдат последователни, доколкото е възможно, публично-частните партньорства и международното сътрудничество: просто кажете „не“.

ВЪВЕДЕНИЕ

Не липсват примери за дейности с цел измама от страна на престъпници, които се опитват да получат спечелени с честен труд пари и/или лична информация, както и не липсват хора, които да попадат в тях (Crosman, 2017 г.). Кой не е получавал „изключителна оферта“ в електронната си пощенска кутия или не е чувал за измама с Microsoft, при която Ви предлагат да поправят компютъра Ви, работил изправно допреди минути?

Противно на разпространеното убеждение, тези видове измами са всичко друго, но не и нещо ново. Мошеничеството и измамите съществуват от векове (Murphy & Murphy, 2007 г.). Сегашното разбиране по отношение на персоналните измами е неразривно свързано с новите технологии, като например интернет, но измами се случват откакто хората могат да говорят и притежават активи. (Button & Cross, 2017 г.). Действително интернет предостави нови възможности на престъпниците за измама на много по-голям брой жертви от когато и да било. (Whitty, 2013 г.). Нови и по-стари технологии, като например телефон, се комбинират, за да се подготвят прецизно атаките и да увеличат максимално печалбата. Обхватът и ефективността са се увеличили, като разходите са се понижили, но основните техники са останали непроменени. (Crosman, 2017; Button & Cross, 2017; Button, McNaughton, Kerr, & Owen, 2014). Тези нови развития, в съчетание с вредното въздействие — финансово, емоционално, релационно,... – тези видове престъпления наложиха (Button, Lewis, & Tapley, 2009; 2014 г.), необходимостта от превенция, а България реши да обърне специално внимание на темата по време на своето председателство на ЕМПП през първата половина на 2018 г.:

„В контекста на превенцията българското председателство ще се съсредоточи върху въпроси, свързани с измами, по-специално телефонните измами. Този вид престъпност се превърна в печеливша престъпна дейност през последните години, която се развива както на национално, така и на трансгранично равнище. Престъпните групи, специализирани в тази дейност, се развиват динамично и поразяват по-широк кръг от жертви. Като се има предвид активното участие на жертвите, въвличането им в престъпните сценарии и травматизиращите последици за тях, трябва да бъдат положени сериозни превантивни усилия, като се вземат предвид особеностите на местно, национално и трансгранично равнище.“

Този набор от инструменти предоставя полезна информация за въпросните видове измами и мошеничества и тяхното предотвратяване. Първата част от работата ще се базира на съществуващата литература, за да се хвърли светлина върху тази тема, която е предмет на все по-задълбочено проучване от специалистите. До неотдавна (криминологични) изследвания са третирали като относително второстепенни измамите за сметка на други престъпления, но това отношение претърпява обрат. (Button & Cross, 2017; Button, Lewis, & Tapley, 2009;Button, Lewis, & Tapley, 2014; Titus & Gover, 2001; Levi, 2008; Button, Tapley, & Lewis, 2012).

Във втората част ще покажем някои добри практики, свързани с това престъпление, и ще дадем някои препоръки и съвети за превантивни мерки, насочени по-специално към измами по телефона. Тези препоръки се основават на семинар, проведен с различни експерти от целия Европейски съюз. На последно място, в трета част ще се изброят някои добри практики, събрани по време на изготвянето на този набор от инструменти.

01

ЧАСТ 1:
ПРЕГЛЕД НА РАЗУЗНАВАТЕЛНАТА ИНФОРМАЦИЯ

1. Въведение

Първата част от набора от инструменти ще проучи актуалната литература по темата за измамите и мошеничествата. По-конкретно, в този набор от инструменти ще се съсредоточим върху измамите на индивидуално равнище, извършвани основно (но не само) чрез използването на ИКТ (Button, Tapley, & Lewis, 2012). Измамата е много разнородно правонарушение и обхваща широк спектър от видове поведение (Button, Lewis, & Tapley, 2014). Levi и Burrows (2008 г.) го определят, както следва:

> *„Измама е получаването на финансова полза или причиняването на загуби чрез пряко или косвено заблуждаване; това е механизъм, чрез който лицето, извършващо измами, печели незаконно предимство или причинява незаконни загуби" (Levi & Burrows, 2008 г., стр. 7)*

Като цяло, можем да заявим, че всички видове измама включват някакъв вид измама или заблуда с намерението тя да доведе до някакъв вид печалба (Button, Lewis, & Tapley, 2009; Murphy & Murphy, 2007; Button и Cross, 2017 г.). Категоризирането на измамите според вида на жертвата (Levi, 2008 г.) отговаря на следните видове:

Сектор на жертвите	Подсектор на жертвите	Примери на измама
Лични	Финансови услуги	- Измама с чекове - Фалшифициране на интелектуална собственост и продукти, продавани като оригинални - Фалшифициране на пари - Измама с подправяне на данни - Незаконно присвояване - Търговия с вътрешна информация/пазарна злоупотреба - Застрахователна измама - Измама със заеми - Измама с разплащателни карти - Измама с възлагане на поръчка
	Нефинансова измама	- Измама с чекове - Фалшифициране на интелектуална собственост и продукти, продавани като оригинални - Фалшифициране на пари - Измама с подправяне на данни - Незаконно присвояване - Измама с игри - Измама със заеми - Измама с разплащателни карти - Измама с възлагане на поръчка
	Физически лица	- Измами с благотворителни организации - Измами на потребители - Фалшифициране на интелектуална собственост и продукти, продавани като оригинални - Фалшифициране на пари - Измами във връзка с инвестиции - Измама тип пенсионна
Обществени	Национални органи	- Измама с облаги - Незаконно присвояване - Измама с възлагане на поръчка - Данъчна измама
	Местни органи	- Незаконно присвояване - Измами по отношение на общински данъци - Измама с възлагане на поръчка
	Международни (но засягащи обществеността)	- Измама с обществени поръчки (от национални срещу други - главно, но невинаги чуждестранни дружества за получаване на чуждестранни договори) - Измама със средства по линия на ЕС

Ако се съсредоточим върху сектора на пострадалите физически лицаq и по-специално върху подсектора на физическите лица като жертви, има още много различни начини за измама, както се вижда от същата илюстрация. В рамките на този набор от инструменти обаче ще се съсредоточим върху измамите с потребители, определени от Levi и Burrows (2008 г.) като::

> *„широка категория, включваща измами, свързани с лотария/ награди; обаждания от измамници и други измами, основани на комуникация; „непочтени „описания на продукти и услуги (като например някои „алтернативни продукти за здраве“ или „сексуални средства“); измами с игри (например „уговорени“ надбягвания и мачове, на които са направени залози (включително спред залагания); закупуване на стоки и услуги, които не са изпратени от доставчика“* (Levi & Burrows, 2008 г., стр. 7).

Други термини, които се разпространяват в литературата, са „индивидуални измами“ (Button, Tapley, & Lewis, 2012 г.) и измами с масов маркетинг (Button, Lewis, & Tapley, 2009; Whitty, 2018 г.; 2015 г.; Wood, Liu, Hanoch, Xi, & Klapatch, 2018 г.), въпреки че последните поставят по-силен акцент върху техниките за масова комуникация, които се използват (Button и Cross, 2017 г.). За целите на последователността в този набор от инструменти по-долу ще се използва терминът „индивидуални измами“, тъй като той отговаря в най-голяма степен на нашата основна тема. Настоящото схващане за този вид измами действително е тясно свързано с новите технологии, но въпреки това е важно да се отчете, че индивидуални измами съществуват откакто можем да говорим и имаме частна собственост. Развитието на технологиите просто промени начините за извършване на този вид престъпления и даде възможност за разгръщането им в по-голям мащаб (Button и Cross, 2017 г.; Leukfeldt & Stol, 2011; Crosman, 2017 г.). Следователно можем да класифицираме тези нови форми като „престъпления, извършвани чрез кибернетични средства“, т.е. традиционни престъпления, които могат да бъдат увеличени по мащаб и обхват с използването на ИКТ. Фишингът вероятно е най-добрият известен пример за това развитие и придобива огромен мащаб (De Kimpe, Walrave, Hardyns, Pauwels, & Ponnet, 2018 г.).

Без категоризиране на всички видове индивидуални измами като кибер измами, този набор от инструменти ще бъде съсредоточен върху съвременните форми на измама и техните съвременни смесени онлайн/офлайн характеристики. В следващите глави ще разгледаме най-напред по-задълбочено използването на тактики за убеждаване, по-специално в областта на социалното инженерство, които са в основата на повечето от тези видове измами (Button, McNaughton, Kerr, & Owen, 2014; Европол, 2017 г.). Тъй като българското председателство реши да се съсредоточи върху измами, при които жертвата действително има активно участие, наложително е да се проучи как извършителите склоняват хората да сътрудничат (Button и Cross, 2017 г.). След това ще бъде направен общ преглед на различните видове индивидуални измами. Накрая, ще разгледаме и профилите на жертвите и извършителите.

https://cyberessentialsdotblog.wordpress.com/2017/02/25/phishing-evolved/

2. Изкуството на убеждаването

Независимо от вида измама е наложително да се изгради връзка с жертвата. Извършителят трябва да спечели благоразположението на жертвите си чрез доверие, съчувствие и убеждаване, за да може схемата да проработи (Crosman, 2017 г.). Използваните в днешно време средства може да се различават; техниките като цяло остават едни и същи (Maggi, 2010 г.). **Социалният инженеринг** е основната тактика за получаване на доверие, чрез която се заблуждава лицето, за да бъде то убедено неволно да разкрие чувствителна информация или да извърши действия, които по принцип не би извършило (Европол, 2017; Atkins & Huang, 2013; Европол, 2016 г.). По-конкретно, ще разгледаме измама, основаваща се на взаимодействието между хората: социалното инженерство се възползва от естествената склонност на жертвата да се хареса. Освен това има и втора категория социален инженеринг, която включва компютърна измама, например с използването на зловреден софтуер, който е инсталиран в електронното писмо, ключови устройства за регистриране на данни или фалшиви изскачащи прозорци (Atkins& Huang, 2013; Singh и Imphal, 2018 г.).

Съмнителните отношения между жертвата и извършителя са от ключово значение при индивидуалните измами. Извършителят зависи до голяма степен от способността да изгражда отношения на доверие с жертвата си, за да успее в своето зловредно намерение (Atkins & Huang, 2013). Всъщност извършителят трябва да насърчава жертвите да извършват действия, които не възнамеряват да предприемат и които дори може да бъдат в техен ущърб (Йебоа-Боатенг & Amanor, 2014; Олман, 2007 г.). По-голямата част от литературата по тази тема трябва да се намира в проучвания в по-широката рамка на социалната психология (Rusch, 1999 г.). Според тази литература:

> *„Социалните инженери често се опитват да убедят потенциалните жертви, като предизвикват у тях силни емоции, например вълнение или страх, докато други използват начини за установяване на междуличностни отношения или създаване на чувство на доверие и ангажираност"* (Workman, 2008 г., стр. 1).

Освен това Atkins и Huang (2013 г.) добавят, че „социалните инженери разчитат на когнитивните предубеждения или социалните грешки в психическия процес, за да инициират и упражнят злонамереното си въздействие и да предизвикат автоматични емоционални реакции у своите жертви“ (Atkins и Huang, 2013 г., стр. 24). Тези автоматични емоционални реакции насочват към т.нар. периферен път в рамките на модела за вероятност за преработка на информацията (Elaboraation Likeholder Model). Въпросният модел изглежда има по-скоро хегемонална позиция в литературата относно измамните схеми и причините, поради които хората попадат в тях. По същността си той приема, че има два пътя на убеждаване. Едниният е основният, той изисква в голяма степен мислене и поради това се нуждае от много обработване. При втория път — периферния, на практика не е необходима обработка, защото вниманието всъщност е съсредоточено върху емоционални фактори, например привлекателност или усещане за доверие (Petty & Cacioppo, 2012; Petty & Cacioppo, 1986; Rusch, 1999 г.; Bullée, Montoya, Pieters, Junger, & Hartel, 2018; Whitty, 2013 г.). Измамниците оказват натиск върху своите жертви по периферния път и обикновено използват предизвиканите негативни емоции, например алчност, самота или страх, а в последно време са започнали да включват обичайни и легитимни бизнес въпроси (например т.нар. CEO измами) (Workman, 2008 г.; Jakobsson, 2016 г.). В литературата са определени някои принципи за насочване на жертвите по периферния път, (с) които извършителите (зло)употребяват (Jakobsson, 2016 г.). Много е важно обаче да се отбележи, че всички тези принципи — тези практически методи — имат ежедневна употреба и приложение. Ключовият фактор тук е, че извършителите на измами създават среда, в която могат да прилагат съответните „оръжия за убеждаване“, в повечето случаи комбинация от такива, за собствена изгода. Сега ще обсъдим трите най-влиятелни автори, определени от литературата в това отношение (Ferreira, Coventry и Lenzini, 2015 г.).

От трите най-често се цитира Cialdini и неговите „шест принципа на влияние“ (Rusch, 1999 г.; Workman, 2008 г.; Ferreira, Coventry, & Lenzini, 2015; Bullée, Montoya, Pieters, Junger, & Hartel, 2018; Cialdini, 2001 г.).

1. Авторитет:

Този принцип описва склонността на хората да изпълняват изискванията на длъжностни лица. В правилната ситуация има голяма вероятност хората да са отзивчиви към твърденията на представители на властта. Използват се и символи на властта, например униформи, пропуски и значки, или телефонни

разговори, при които лесно може да се твърди представителство от името на властите.

Пример: Този принцип е много показателен за измами, при които извършителите се представят за полицаи. Ние, разбира се, вярваме и се подчиняваме на полицаите въз основа на тяхната униформа, значки,... Представете си, че ви се обади човек, който твърди, че е полицейски служител и се нуждае от вашия ПИН код колкото е възможно по-бързо, за да блокира сметката Ви, която е станала обект на посегателство от страна на престъпници. Единственото, което ще „хванат" обаче, ще бъдат парите по Вашата сметка.

2. Дефицит:
Хората отдават по-голяма стойност на неща, които се считат за дефицитни. Даден артикул или оферта се представят за налични в малко количество или само за ограничен период от време. В резултат на това артикулът или офертата се възприемат като по-привлекателни и желани.

Пример: Много фишинг имейли посочват в заглавието, че офертата е „ограничена", „остават само 50 бройки", „последна бройка",...

3. Харесване и сходство:
Хората са склонни да харесват подобни на себе си по отношение на интереси, нагласи и убеждения. Съвсем човешко е да харесваме тези, с които си приличаме. Идентифицирането на дадено лице като такова с характеристики, еднакви или сходни с нашите, също ни дава силен подтик към установяване на ментална връзка в отношенията си с това лице.

Пример: Този принцип се проявява особено при лидерите на мнение в социалните медии. Част от техния успех се дължи на факта, че се представят като „съседското момче или момиче". Вие несъмнено бихте искали да изглеждате по същия начин. Също така бихте искали същата риза, каквато носи любимият Ви футболист. Измамниците лесно се възползват от това, като се позовават на известни личности в своите схеми.

4. Реципрочност:
Това е добре познато социално правило, което ни задължава да отвърнем с

това, което сме получили. Има и такава поговорка: „Каквото повикало - такова се обадило“. Човек, който е получил някаква услуга, дори и да не я е искал, може да се чувства сериозно задължен да спази правилото за реципрочност, като се съгласи да върне услугата на съответното лице. Дори ако тази услуга коства значително повече.

Пример: Ако се предложи нещо със стойност, например безплатна мостра, хората се чувстват задължени да върнат услугата, като закупят целия продукт или услуга. Даже тази безплатна за тях мостра все още да не е получена или да не съществува изобщо.

5. Ангажираност и последователност:
Друго социално правило е последователността в поведението и ангажиментът за това. Ако обещаем нещо, най-вероятно ще изпълним обещанието си, защото в противен случай изглеждаме неблагонадеждни или неотзивчиви. Последователността се активира, като се търсят и искат по-малки първоначални ангажименти, които могат да бъдат изпълнени по-лесно.

Пример: Класическата измама с нигерийския принц (вж. по-долу), известна също като измама 419, при която обикновено се отправя първо искане за по-скромна „услуга“, на което жертвата може по-лесно да се отзове. След това ще бъде отправено по-голямо искане, което ще е трудно да се отхвърли или откаже, тъй като жертвата няма да бъде последователна спрямо предишното си поведение.

6. Социално одобрение/съответствие:
Последният принцип се проявява и в много социални ситуации. За да решим кое действие е най-подходящо, ние се консултираме с други хора (сходни групи, ролеви модели,...). Това може да доведе до действия, които са в противоречие със собствения ни интерес, но ни позволяват да бъдем приети в рамките на групата.

Пример: Във Facebook можем да видим дали дадена страница или продукт се счита за популярен въз основа на броя харесвания. Измамниците съвсем лесно могат да създадат нова страница с фалшиви харесвания и този принцип за социално одобрение може да се използва, за да се убеди жертвата, че страницата наистина съществува и е популярна.

Принципите на Cialdini са определени първоначално въз основа на резултати от маркетинг, но са доказали значението си в литературата в областта на социалното инженерство, а измамниците използват тези принципи за извличане на собствена изгода. Някои автори обаче формулират различни, макар и сходни принципи, които се отнасят в по-голяма степен към измамите (40). Един от тях е Gragg и неговите „седем психологически стимула“ (40,49):

1. Състояние на силен афект

Този стимул действа чрез силна емоция, за да се даде възможност на извършителя да постигне повече от това, което би било разумно възможно при нормална ситуация. Така например предизвикването на изненада или гняв у жертвата ще попречи на рационалното мислене.

Пример: Обещанието, че потенциалната жертва може да спечели наградата от милиони, най-вероятно ще предизвика силни емоции и ще действа като мощна бариера за логическо и рационално оценяване на предложенията.

2. Претоварване

Ако жертвата има твърде много информация за обработване едновременно, това ще се отрази отрицателно върху оценката на информацията и би довело до решения, които по принцип не биха били взети.

Претоварването може да бъде предизвикано и от неочаквана перспектива. Една нова перспектива изисква време, за да се осмисли, но при липса на такова време може да се стигне до намаляване на капацитета за обработване на информацията и съответно до лоши решения.

Пример: За да се съобразят с ОРЗД (Общ регламент относно защитата на данните), дружествата в целия свят изпратиха огромно количество електронни съобщения, за да поискат от своите клиенти да потвърдят дали са съгласни с подновената политика за защита на личните данни. Измамниците обаче не закъсняха да се възползват от това претоварване и започнаха да изпращат подобни съобщения, които съвсем нямаха за цел да се защити неприкосновеността на личните данни на хората.

3. Реципрочност:
Подобно на принципа на Cialdini, човек трябва да върне услугата, когато му е предоставено или обещано нещо.

Пример: При измамата 419 на жертвите се обещават големи възнаграждения. Те се чувстват естествено склонни в замяна да прехвърлят пари.

4. Измамни отношения
Тук измамникът изгражда връзка въз основа на неверни обещания с цел да експлоатира другото лице.

Пример: При тази измама се използва отношението на възрастните хора към техните внуци. С фалшиви обещания те изграждат отношения на доверие и ги експлоатират за своя изгода.

5. Вменяване на отговорност и морално задължение
При задействане на този стимул набелязаната жертва чувства само частично отговорност за действията, които ще извърши. Тези действия ще се извършат по-лесно, особено когато набелязаната жертва счита, че това е нейно „морално задължение".

Пример: При CEO измамите на жертвата може да се внуши, че носи отговорност, ако не подпише голям договор, ако не извърши авансово плащане.

6. Авторитет
Отново, подобно на Cialdini, хората в съвременното общество се чувстват задължени да спазят разпорежданията на длъжностните лица и това лесно може да бъде използвано от измамниците.

Пример: Ако използваме същия пример като по-горе, как ще си позволите да откажете, ако изглежда, че заповедта идва от самия висш ръководител?

7. Интегритет и последователност

Този последен стимул също е подобен на „ангажираността и последователността“ по Cialdini. При хората се наблюдава тенденция да следват предишни ангажименти, дори и те да са потенциално вредни за тях самите.

Пример: Това може да се използва за продължаване на измамата, но също и за започване на измамна схема, като се поискат от дадено лице действия, които то обикновено би извършило, или като се разиграе сценарий, при който изглежда, че жертвата вече се е ангажирала с нещо.

Stajano (2011 г.) е друг влиятелен автор, формулирал „седем принципа на измамите“, които измамниците използват:

1. Принцип на отвличане на вниманието

Докато жертвата е разсеяна с нещо, което привлича интереса й, измамникът може да действа и жертвата най-вероятно няма да забележи.

Пример: При уличните измами от типа „тука има, тука няма“ измамниците често говорят за наградата, която жертвите може да спечелят, и им показват пример за наградата. Всичко се случва по време на играта, когато жертвата е отклонила вниманието си.

2. Принцип на обществения ангажимент

Подобно на „авторитета“ при Cialdini и Gragg, Stajano твърди, че измамниците използват „приспиването на подозрителността“, за да действате според техните желания.

Пример: Измамниците могат да се престоря на законни работници и да влязат в дома на жертвата под този предлог. Веднъж влезли вътре, те лесно могат да извършат обир на дома.

3. Принцип на стадото

В съответствие със „социалното одобрение“ по Cialdini, този социален принцип позволява дори подозрителните жертви да „свалят гарда“, ако считат, че се намира в същото положение като останалите.

Пример: Някои фишинг измами по електронна поща разпространяват твърденията, че лекуват оплешивяване. Често те използват цитат от доволен „клиент“, за да покажат, че средството действа. Жертвата може да е по-малко подозрителна, тъй като очевидно други също са купували продукта.

4. Принцип на непочтеността

До известна степен подобен на „вменяването на отговорност и морално задължение“ от Gragg, този принцип гарантира, че ще Ви бъде по-трудно да намерите помощ. След като сте разбрали, че сте били измамени, вече сте въвлечени в престъпна схема, поради което е по-малко вероятно да отидете в полицията. Това може да се постигне и чрез порицаване на жертвата.

Пример: В много случаи на измами пострадалият се срамува от попадането в капан. Това ще го възпре да съобщи за престъплението. Измамниците специално разработват подобни измамни схеми, за да накарат жертвата да се срамува (вж. също по-долу).

5. Принцип на заблудата

Измамниците знаят как да манипулират и ще накарат жертвата да повярва, че всичко е реално, дори и да не е.

Пример: На практика почти всички измами се възползват от този принцип. Нещата и хората никога не са това, което изглеждат в измамите. Ако изглежда прекалено добре, за да е истина, вероятно не е.

6. Принцип на нуждата и алчността

Също свързан с принципа на „дефицита“ на Cialdini, този принцип означава, че измамниците манипулират Вашите нужди и желания, за да получат това, което искат.

Пример: Когато се намирате в държава с различна валута, ще трябва да си обмените пари. Тази потребност може лесно да бъде използвана от измамниците за понижаване на обменните курсове.

7. Принцип на времето

Вменявайки на жертвата чувство за неотложност и времеви натиск, тя най-вероятно ще вземе решение по-бързо. Така има по-малко обмисляне, а това е в полза на извършителя, тъй като жертвата се поддава по-лесно.

Пример: В много измами с електронна поща пострадалият ще бъде принуден да вярва, че трябва да бъде бърз, ако не иска да пропусне този „единствен шанс".

Ferreira, Coventry и Lenzini (2015 г., стр.3) правят следното сравнение между трите основни групи принципи, използвани от измамниците с цел злоупотреба:

	C	G	S
1	Авторитет	Авторитет	Обществен ангажимент
2	Социално одобрение	Вменяване на отговорност	Стадо
3	Харесване и сходство	Измамни отношения	Заблуда
4	Ангажираност и последователност	Интегритет и последователност	Нечестност
5	Дефицит	Претоварване	Време
6	Реципрочност	Реципрочност	Нужда и алчност
7	-	Състояние на силен афект	Разсейване

Сега, когато сме наясно с някои от ключовите техники и принципи, които извършителите на измами използват и злоупотребяват с тях, ще разгледаме различните измами, които съществуват.

3. Открийте Вашата измама

Както вече споменахме на друго място, тактиките на измамниците са все същите, в днешно време различни са средствата, които използват. В този раздел правим неизчерпателен преглед на разнообразието от измами, които съществуват днес. На първо място, се дават някои примери за измами въз основа на тяхното съдържание. След това се предоставя класификация въз основа на начина на доставка.

Въпреки че криминологичните изследвания едва наскоро проявиха интерес към този вид престъпления *измамата* 419, по-известна като *измамата с нигерийския* принц, получи значително повече внимание от страна на специалистите (Whitty, 2015 г.; Whitty, 2018 г.; Mba, Onaolapo, Stringhini и Cavallaro, 2017 г.). Както подсказва името — и въпреки че Нигерия няма принц — произходът на тази измама обикновено е от Нигерия. Това затруднява правоприлагащите органи да заловят извършителите (Мба, Onaolapo, Stringhini и Cavallaro, 2017 г.). При класическия сценарий на жертвата се предлага процент от голяма сума пари, но само ако помогне за изнасянето на парите от страната. Жертвата бива убедена да заплати допълнителните такси, за да прехвърли парите. Разбира се, не е необходимо да се споменава, че парите и принцът никога не са съществували. (Murphy и Murphy, 2007 г.).

Този вид индивидуални измами се наричат „измами с предварителни такси". Трябва дасе плати малка сума, за да се получи много голяма сума (Мба, Onaolapo, Stringhini и Cavallaro, 2017 г.). *Романтичните измами* също могат да се включат в тази категория (Whitty, 2018 г.), но загубите при тях не са само парични. Наистина, от емоционална гледна точка този вид измама има опустошителни последици и се дължи на интимната връзка, която трябва да бъде изградена, за да сработи измамата.

> *„Престъпниците се преструвaт, че започват връзка, с намерението да измамят жертвите си с големи суми пари. Измамниците създават фалшиви профили в сайтове за запознанства и в социални мрежи с откраднати снимки (например атрактивни модели, офицери от армията) и измислена идентичност. Те развиват онлайн връзка с жертвата извън сайта, „сприятелят" се с жертвата (изграждат изключително лична връзка с жертвата) до момента, в*

https://blog.eset.ie/2017/09/18/email-phishing-is-old-but-not-dead/

> *който счетат, че тя е готова да сподели с тях с парите си. Установено е, че тази измама води до „двоен удар“ — финансова загуба и загуба на връзка“* (Whitty, 2018 г., стр. 105)

Също изградена на фалшиви отношения, макар и по различен начин, е измамническата схема с *баба и дядо*. Както беше обяснено в предишни изследвания на ЕМПП (ЕМПП, 2017 г.), възрастните хора са подведени да смятат, че в действителност са разговаряли с роднина. Твърди се, че в болницата се намира внук, когото не са виждали отдавна и за който незабавно трябва да се преведат пари, за да се плати за операция. (Jakobsson, 2016 г.). Те дълго време не са го чували и вероятно няма повече да го чуят...

Друга „прочута“ измама със същите характеристики е измамата с *техническа поддръжка* (Marzuoli, Kingravi, Dewey и Pindrop, 2016 г.). В много случаи тази техническа поддръжка идва от Microsoft и се информира жертвата по телефона или по електронната поща за скрит компютърен проблем. *„Може още да не сте забелязали, но Вашият компютър е заразен с вирус“*. Срещу малка сума

член на персонала ще може да реши проблема Ви дистанционно (Harley, Grooten, Burn и Johnston, 2012 г.; BulléeJ.-У. , Montoya, Junger и Hartel, 2016 г.). Тъй като много хора са запознати с тази измама, нейните извършители наскоро са се върнали с по-усъвършенствани фалшиви уебсайтове за поддръжка, които подканват жертвата да се обръща към самия център за поддръжка, който най-вероятно има специален телефонен номер (Rauti и Leppänen, 2017 г.).

От 13-те държави членки, които отговориха на нашия въпросник, следните телефонни измами бяха най-често срещани: измама на баба и дядо, фалшив полицай, лотарийна измама, измама с легален бизнес, измама със злополука (с роднини).

Други примери са *измамите с лотарийни игри, хазарт, бизнес възможности, вериги от писма, телемаркетинг и др.* (Button, Lewis, & Tapley, 2014; Button и Cross, 2017 г.; Button, Lewis, & Tapley, 2009; Jakobsson, 2016 г.; Stajano и Wilson, 2011 г.). Button (2017 г.) ни дава класификация въз основа на осем категории най-често срещани измами.

1. Измами с инвестиции на потребители

При тях акциите се продават на жертвите, като им се описват като много печеливши. В действителност не струват нищо или изобщо не съществуват.

2. Измами с потребителски стоки и услуги

Тази измама включва продажба на несъществуващи продукти и услуги или на такива, които се различават значително при доставката.

3. Измами с трудова заетост

На жертвата се предлага фалшива или неадекватна услуга за осигуряване на заетост или обучение, което води до заетост.

4. Измами с награди и безвъзмездни средства

Жертвата или бива подведена да повярва, че играе на реална лотария и

заплаща своята такса за участие, или бива уведомявана, че вече е спечелила и трябва първо да плати такса, за да може да получи наградата.

5. Измами с фирми фантоми за събиране на дългове

Често, като се представят за доверени лица или организации, измамниците притискат жертвата да плати задължения, които не дължи.

6. Измами с благотворителна дейност

В този случай лицето, извършващо измами, действа като легитимна благотворителна организация, за да получи дарения от физически лица.

7. Измами въз основа на връзка и доверие

Романтичната измама, измамата с баба и дядо, измамата със злополуки ... са класически примери за измами, които злоупотребяват с интимността на личните отношения.

8. Измама със самоличност

Тя включва използването на лична информация от жертвата за извършване на други измами или престъпни дейности. Не включихме тези измами в настоящия набор от инструменти, тъй като при тях не е необходимо активно участие на жертвата в сделката.

Списъкът е внушителен като креативността на измамниците, а те могат да достигнат до всички групи от населението. Измамниците обаче могат да използват и по-целенасочен подход. Такъв е случаят с *измамите с компрометирани бизнес имейли* (Jakobsson, 2016 г.). Тук жертвата е избрана, тъй като работи за определено дружество или има специфична позиция в това дружество. Най-вероятно след известно разузнаване извършителят действа като началник на жертвата (CEO измама) или друга надеждна трета страна (измама с правомощия) и моли за привидно нормално плащане (Европол, 2017 г.). Например шефката ви изпраща електронно писмо, за да извършите превод до фирма X. Това е спешен въпрос, ето защо се използва нейният„личен“ електронен адрес и тя просто ви моли да го направите.

Нито дружеството, нито адресът на електронната поща са правилни, но изпълнявате разпореждането (Jakobsson, 2016 г.). Съгласно последната *Оценка на заплахата от организирана престъпност в интернет* (Европол, 2018 г.) 65% от всички държави членки са докладвали случаи на измама с висши ръководители (CEO измами) и над половината от тях посочват нарастване на тези случаи.

https://www.europol.europa.eu/socta/2017/fraud.html

Друг начин да се класифицират тези измами е да се разделят според начина, по който се осъществява контактът с жертвата. Логично, контактът може да е лична среща, в ситуация от реалния живот или по дистанционен път, чрез комуникационни средства като имейл или телефон. Въпреки това е наложително да не се се фокусираме върху един единствен начин за контакт, който осигурява сработването на измамата. Извършителите могат лесно да превключват между електронна поща, телефон, уебсайт ... Това им позволява да планират атаките си възможно най-прецизно (Button и Cross, 2017 г.).

Класически примери на **измама лице в лице** са тези с фалшиви полицейски служители, които принуждават жертвата да плати предполагаема глоба или да предостави деликатна информация. Подобни са и измамите с мними майстори, които искат да извършат някакви работи в жилището. За удобство на жертвата те предлагат да изпълнят работите, докато жертвата е на работа или на почивка ... Други често срещани примери са ролки с фалшиви пари, измамите от типа „тука има, тука няма“ или продажбата на фалшиви предмети (Stajano и Wilson, 2011 г.).

Ролка с фалшиви пари: например обмен на чуждестранна валута с фалшиви пари

„Тука има, тука няма“: класическата игра, където топката е скрита под чаша, която след това се смесва с две други чаши, като жертвата трябва да познае къде е топката, а това е невъзможно, защото топката не е под никоя от тях

В повечето случаи на социално инженерство обаче извършителите се въздържат от физически контакт, тъй като това им осигурява по-голяма защита. Освен това използването на електронна поща или телефон е идеално за насочване на жертвите към периферния път (Workman, 2008 г.). Както Anderson (2016 г.) описва тази еволюция от американска гледна точка:

> *Неотдавна, през 80-те години на миналия век, проблемът с измамите е бил предимно местен проблем или проблем, свързан с изпращането на писма. Извършителите набелязват жертвите си, като ходят от врата на врата, механиците заблуждават*

относно необходимостта от ремонти в местния автосервиз, а продавачите им продават фалшивите си стоки на местния панаир или изпращат фалшивите си обещания по пощата. Днес измамниците извършват масови измами на националния и дори на международния пазар, където се свързват с потенциалните жертви чрез телемаркетинг, късни телевизионни реклами или интернет. Измамниците в Индия казват на потребителите, които са потърсили техническа поддръжка в интернет, че компютрите им имат 133 проблема, които те могат да поправят дистанционно, ако просто се платят съответните такси. Вместо да се ограничават до лични посещения или използване на американската поща, доставчиците на множество фалшиви продукти могат да пускат реклами в късните телевизионни предавания, да рекламират продуктите си в интернет или да изпратят компютърно генерирани телемаркетинг обяви на милиони потребители за няколко минути. (Anderson, 2016 г., стр. 4)

Революцията в комуникационните технологии позволи на извършителите да индустриализират старите измами при ниски разходи и да измислят нови видове измами. (Button и Cross, 2017 г.; Button , McNaughton, Kerr и Owen, 2014 г.). Това е известно като *престъпление, използващо кибер пространството*, т.е. традиционно престъпление, което се усъвършенства с използването на ИКТ (Whitty, 2018 г.; Button и Cross, 2017 г.). Дигиталната среда създаде атмосфера на анонимност, която извършителите на измами с удоволствие възприеха. (Agustina, 2015 г.). Наред с тази (предполагаема) анонимност и ниските разходи, размерът на достижимите цели се е увеличил до такава степен, че светът е в безизходно положение. (Leukfeld и Stol, 2011 г.). Дори по-лошо, глобализацията на измамите възпрепятства правоприлагащите органи да намерят и/или задържат извършителите. Някои, със съзнанието за пълния потенциал на технологичните промени, дори са станали „скамър предприемачи". (Button и Cross, 2017 г.).

Най-често срещани сред „индустриалните измами" са тези от типа фишинг (Европол, 2017 г.; Европол, 2016 г.). Целите са същите, както при всекидневните измами, но най-вероятно измамникът действа като доверен или законен субект, а жертвата бива подведена да разкрие лична и/или финансова информация. (Singh & Imphal, 2018; De Kimpe, Walrave, Hardyns,

Pauwels, & Ponnet, 2018; Moreno-Fernández, Blanco, Garaizar, & Matute, 2017 г.). Това е най-лесният метод за достигане до огромно количество потенциални жертви. Съобщава се, че извършителите се свързват със своите жертви 95% от времето чрез електронна поща. 40% от държавите членки подчертаха разследванията за фишинг - явление, което продължава да се увеличава година след година. От 2015 до 2016 г. се наблюдава значително увеличение от 65% на броя на фишинг атаките (Европол, 2017 г.). Трябва да бъдем предпазливи с тези цифри, заради проблемите при съобщаването (вж. по-долу), но въпреки това те са тревожни.

Фишингът е много често срещано явление. Повече от 30% от възрастното население е получило най-малко един фишинг имейл. В рамките на студентското население това число дори се повишава до над 50%. Нещо повече, на практика 1 от 14 потенциални жертви отваря връзка или прикачен файл, водещ до възможна виктимизация. (De Kimpe, Walrave, Hardyns, Pauwels, & Ponnet, 2018 г.).

При ниски нива на риск за извършителя загубите за жертвата могат да бъдат значителни: финансови загуби, вреда на репутацията, кражба на самоличност,.... (Олман, 2007 г.).

Тук говорим за измамнически фишинг, което предполага използването на тактики от социалното инженерство. За пълнота, има и форма на фишинг, която се основава на зловреден софтуер или компютърна измама, като се използват ключови устройства за регистриране на данни, хакерство, троянски коне ... за постигане на целите на измамниците, както вече беше споменато по-горе и в предишни публикации. (ЕМПП, 2017 г.).

До съвсем неотдавна измами с електронна поща бяха доста лесно откриваеми. Те се характеризираха с лоша граматика, правописни грешки и доста необичайни истории. Измамниците обаче са осъзнали, че с прецизно таргетиране на жертвите получават по-висока „възвръщаемост на инвестициите“. Таргетирането на атаката увеличава вероятността за прочитане на електронното писмо двадесет пъти. (Jakobsson, 2016 г.). Тази еволюция проправи пътя за едно ново и по-голямо разнообразие от фишинг форми и по-професионални и бъдещи доверие начини на действие.

(Европол, 2017 г.; Jakobsson, 2016 г.; Ollmann, 2007 г.). Фишингът става все по-целенасочен. Ако преди извършителите изпращаха колкото е възможно повече имейли, в днешно време измамниците правят проучвания и използват това знание, за да изглеждат по-естествени и правдоподобни; CEO измамата е идеалният пример за това. (Jakobsson, 2016 г.). Измамата с електронни писма от името на ръководството (spare фишинг) е друг термин, който указва насочването към конкретна група. Измамите с пълномощия (whale фишинг) пък са насочени към *високопоставени* лица (Singh и Imphal, 2018 г.). Съществуват и други варианти, като фарминг, където се хоства фалшив уебсайт, за да се заблуди жертвата (Европол, 2014 г.) или смишинг - форма на фишинг, която използва SMS или онлайн текстови съобщения. (Европол, 2018 г.).

Тъй като фишингът става все по-сложен, изненадващата последна стъпка включва подновен интерес към по-стара технология: телефона (Maggi, 2010 г.). Телефонните измами стават все по-популярни под названието вишинг, тъй като използват и потенциала на интернет. (Европол, 2017 г.). Вишингът - буквално фишинг на глас, използва телефонния канал за заблуда на жертвите. (Maggi, 2010 г.). Телефонният канал обаче също е претърпял някои промени. Voice Over Internet Protocol (VOIP) дава възможност да се осъществи телефонно обаждане чрез интернет. (Singh и Imphal, 2018 г.). Това води до някои ползи. Използването на този протокол намалява значително разходите за обаждания, извършителите са по-трудни за проследяване и са в състояние да измислят информацията за повикващия. (Ollmann, 2007 г.). Спуфингът е измама с фалшифициране на информация, която се предава от повикващия. Това не е всичко, измамниците могат също да „роботизират" повикванията до своите жертви. Извършва се компютъризирано автоматично набиране, което доставя предварително записано съобщение. (Marzuoli, Kingravi, Dewey, & Pindrop, 2016 г.). Днес хората се използват, за да дават информация на непознати или дори на машини, тъй като центровете за обаждания са много актуални в днешното общество. (Маги, 2010 г.). Измамниците лесно се възползват от това развитие.

Телефонните измами имат много по-висока ефективност и доходността винаги е по-голяма, отколкото при обикновения фишинг. (Yeboah-Boateng & Amanor, 2014 г.). Този успех се дължи на факта, че вишингът съчетава най-доброто от двата свята - този на личните взаимоотношения и този на комуникационните технологии. Силата на телефона по интернет е, че дава на извършителя възможността да създаде правдоподобна личност много по-бързо. Освен това човекът, който стои зад линията, все още може да бъде този, който иска

https://www.pinterest.co.uk/pin/760897299514084725/

да бъде и да се радва на анонимност. Така се съчетава интимната обстановка с невъзможността да се забележат измамите в реалния живот чрез визуални улики. Човек наистина може да планира атаката си оптимално, като разговаря в реално време и контролира времето за предаване на съобщението. (Ollmann, 2007 г.). Организираните престъпни групи дори започнаха да наемат местни носители на езика, за да бъдат възможно най-правдоподобни и професионални. (Европол, 2016 г.).

Освен тези предимства, традиционно хората имат по-голямо доверие на телефона, отколкото на интернет. Според последния Евробарометър по комуникационни технологии в ЕС (Европейска комисия, 2018 г.) 60% от респондентите смятат, че телефонът е по-надежден и им предлага по-голяма защита от интернет. Освен това телефонният достъп е почти универсален, с 97% с достъп у дома спрямо 70% с достъп до интернет у дома. Освен това телефонното обаждане все още е най-използваният метод за комуникация, като 92% от респондентите често получават или извършват телефонни разговори в сравнение със 72%, които пращат електронни писма (European Commission, 2018). Това дълбоко доверие, разбира се, лесно се използва от измамници, при това, докато спамът на електронната поща е довел до многомилиардна антиспам индустрия, телефонните измами и мошеничества не са под толкова голяма защита (Gadhave & Sirsat, 2015).

4. Проучване на номерата

Като цяло има голяма неяснота по тази тема (Button, McNaughton, Kerr, & Owen, 2014). Най-голямата трудност при получаването на точна представа за тези видове престъпления е, че голяма част от тях не се съобщават (van de Weijer, Leukfeldt, & Bernasco, 2018; Crosman, 2017). Дори наличните данни дават изопачена представа, тъй като вероятно има подценяване на проблема поради липсата на докладване (Bidgoli & Grossklags, 2017). Причините за този проблем обаче са добре известни. Една от тях е, че жертвите често дори не знаят, че са се свързали с измамник (Bidgoli & Grossklags, 2017; Button & Cross, 2017). В проучване със 745 жертви, направено от Button, Tapley и Lewis (2012), 40% от анкетираните не са знаели, че са жертва, докато не са били уведомени от трета страна. Друга причина за несъобщаване е предполагаемата тежест на престъплението от гледна точка на жертвата. Например масовите фишинг атаки ще доведат до голяма обща сума, отделните случаи имат сравнително малки загуби. Жертвите често смятат, че подаването на жалба не си струва неприятностите и на всичкото отгоре е малко вероятно нарушителите да бъдат задържани (Bidgoli & Grossklags, 2017; Button & Cross, 2017). Освен това съобщаването на полицията не се подразбира. Има многобройни инстанции, на които да се съобщи за измама, а полицията също не приема това непременно като приоритет (Button & Cross, 2017). Според проучване на Евробарометър по киберсигурността (European Commission, 2017) само половината от респондентите биха отишли в полицията, ако получат измамни електронни писма или телефонни обаждания, 18% от тях изобщо не биха съобщили, четири процента дори не знаят къде да отидат. Това се потвърждава и от други изследвания (Button & Cross, 2017; Bidgoli & Grossklags, 2017; Button, McNaughton, Kerr, & Owen, 2014).

Може би най-големите положителни странични ефекти за нарушителя при социалното инженерство на жертвата са чувствата на самообвинение и срам на жертвата след това. Това от своя страна е още една причина, поради която степента на докладване е толкова ниска (Cross, Richards, & Smith, 2016; Titus & Gover, 2001). При CEO измамата например жертвите се страхуват от щети върху репутацията в дружеството или дори губят работата си (Europol, 2016). Жертвите често се обвиняват, тъй като са имали активно участие в изпълнението на престъпната схема и са притеснени, че са попаднали в нея (Bidgoli & Grossklags, 2017; Button, McNaughton, Kerr, & Owen, 2014). Виждайки себе си като неразделна част от престъплението и срамувайки се от действията си, те се страхуват, че полицията няма да им повярва или няма

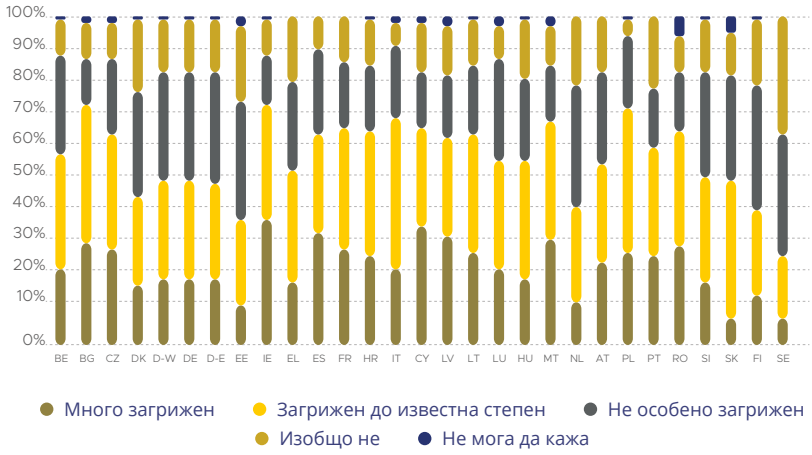
ги приеме сериозно(Button, Tapley, & Lewis, 2012). Така не само че активното участие на жертвата в престъплението затруднява нашето разбиране за проблема, а може дори да доведе до вторична виктимизация (Button & Cross, 2017). Някои измами, като измамата 419, имат вграден механизъм за предотвратяване на съобщаването, тъй като жертвата също предприема незаконни действия чрез прехвърляне на незаконни пари в някои случаи (Button, Lewis, & Tapley, 2009) (вж. по-горе), а измамниците специално създават неудобни схеми, за да избегнат съобщаването (Button, McNaughton, Kerr, & Owen, 2014).

Ако измамите бъдат докладвани на официалните институции, те най-вероятно ще бъдат поставени под общото понятие за „измама", което прави много трудно да се изолират индивидуалните измами (Button & Cross, 2017). Във въпросник, който беше изпратен на държавите членки при подготовката на този инструментариум, открихме подобни наблюдения. В единадесет от 13-те държави членки, които отговориха, телефонните измами се отчитат като „измама".

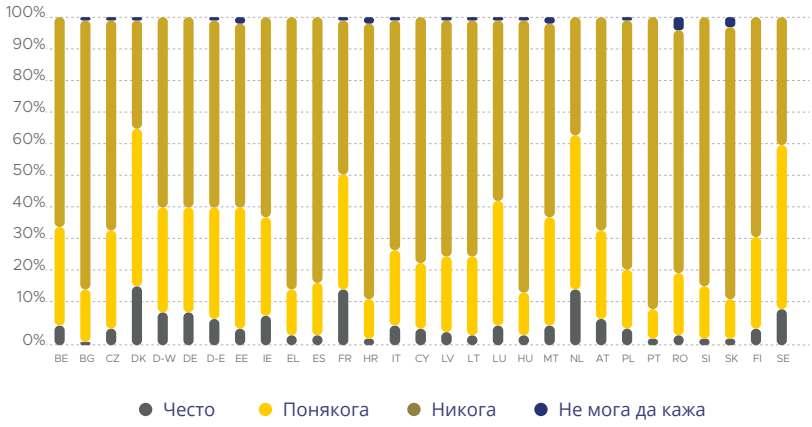
Решението на проблема с официалната статистика е използването на проучвания на виктимизацията. Същите проблеми се поставят обаче и от специалистите. Много от проучванията не правят разлика между измами, които са извършени онлайн или чрез „старите" методи, или включват инидивидуалните измами под общия знаменател на измамите. И отново, продължава да е налице нежелание да се докладва, все още има жертви, които не знаят, че са жертва или които смятат, че техният конкретен случай не си струва да се докладва (Button & Cross, 2017; Button, McNaughton, Kerr, & Owen, 2014). Независимо от тези критични въпроси, Специалното проучване на Евробарометър за киберсигурността (European Commission, 2017) направи специална анкета по домовете на почти 30 000 граждани на ЕС по някои въпроси, свързани с измамни електронни писма или телефонни обаждания. Levi (2017) описва това проучване като „обикновено международно сравнително събиране на данни за виктимизирането при измами в ЕС" (Levi, 2017, p. 4).

Във всички държави членки, с изключение на пет, най-малко половината от анкетираните от Евробарометър изразиха известна загриженост, че са жертва на измамни електронни писма или телефонни обаждания, като най-висок е процентът в Ирландия и България (73%). Дания (45%), Нидерландия (42%), Финландия (41%), Естония (38%) и Швеция (27%) са изключения от тези общи

До каква степен сте лично загрижени за това, че сте попаднали или сте станали жертва на следните ситуации: получаване на измамни електронни писма или телефонни обаждания с молба за лични данни (включително достъп до компютъра, данни за вход, банкова инфор



Колко често сте попадали или сте ставали жертва на следните ситуации: получаване на измамни електронни писма или телефонни обаждания с молба за лични данни (включително достъп до компютъра, данни за вход, банкова информация или информация за плащане)



констатации. Интересно е обаче, че три от тези страни имат най-висок процент съобщаване от самите жертви. В Дания (66%), Нидерландия (64%), Швеция (61%) повече от половината от анкетираните са получили измамни електронни съобщения или телефонни обаждания. Словакия (14%), Хърватия (14%) и Португалия (11%) отчитат най-ниските проценти.

Освен огромното неизвестно число, има и малко изследвания на виктимологията на това престъпление (Whitty, 2018; Button, Lewis, & Tapley, 2014). Повечето проучвания на профилите на жертвите също се фокусират върху онлайн измами, така че следните твърдения се основават главно на тези констатации. Както беше показано обаче в раздела за различните видове измами, има голямо разнообразие от измами, чрез които почти всеки в обществото може да стане потенциална жертва. Това затруднява изготвянето на общи заключения относно типологията на жертвите. Въпреки това проучванията показват, че определени групи са особено уязвими към специфични измами. Потребителските инвестиционни измами например са по-разпространени сред възрастните хора и работещото население, тъй като те имат действителните средства за инвестиране (Button & Cross, 2017).

Може би най-важното допълнение към виктимологичните проучвания около тази тема е премахването на мита, който съществува за нивото на разпространение сред различните възрастови групи. Общото мнение, особено в медиите, е, че жертви на престъплението са предимно възрастни хора (Button, Lewis, & Tapley, 2009). Противно на това популярно мнение обаче, проучванията показват, че по-младите пълнолетни са най-разпространената група жертви (Button, Lewis, & Tapley, 2009; Ross, Grossmann, & Schryer, 2014). Това популярно схващане произтича от стереотипа, че възрастните хора нямат финансови умения, че са по-доверчиви, имат по-слаби когнитивни функции, ... Подобни заключения несъмнено са правилни до известна степен, но е важно да се разбере защо се таргетират най-вече възрастни хора. Ако обърнем внимание върху привлекателността на целевата група, възрастните хора имат лесен достъп до спестявания, по-вероятно е да имат частна собственост, повече допълнителни кредитни линии (Barnes, 2017). Това според Button и Cross (2017) е основната причина да се таргетира в такава голяма степен тази група. По-младите хора и тези на средна възраст обаче са по-податливи на въпросните измами (Button & Cross, 2017; De Kimpe, Walrave, Hardyns, Pauwels, & Ponnet, 2018; Whitty, 2018). Повечето от проучванията наистина заключават, че има по-малък риск по-възрастните потребители да станат жертва на индивидуална измама. От друга страна, при възрастното население измамите

са най-вероятното престъпление, с което ще се сблъскат (Button & Cross, 2017). Все пак това остава амбивалентна тема, която се нуждае от допълнително проучване, тъй като някои специфични видове измами, като например измами с инвестиции или лотарийни измами, показват по-голямо разпространение сред възрастните хора (Anderson, 2016).

По-конкретно, като уязвими са идентифицирани предимно млади хора (15-25 години) (De Kimpe, Walrave, Hardyns, Pauwels, & Ponnet, 2018; Sheng, Holbrook, Kumaragur, Cranor, & Downs, 2010). Това може да е свързано с по-ниски нива на образование, по-малко години онлайн, по-малък досег с материали за обучение и по-малка аверсия към риска (Sheng, Holbrook, Kumaragur, Cranor, & Downs, 2010). Последното се изтъква също от Button, Lewis и Tapley (2009), тъй като хората с по-положително отношение към поемането на финансови рискове и лицата с нисък самоконтрол се възприемат като по-податливи. В проучване на De Kimpe, Walrave, Hardyns, Pauwels и Ponnet (2018) се твърди, че високото ниво на доверие или „съответствие" води до по-висока чувствителност, което е положителен предиктор за отговор на фишинг писма. Смята се също, че силното чувство за дълг е положително свързано с виктимизацията. Въпреки това в рамките на академичните проучвания се обсъжда дали опитът в интернет и технологичните познания водят до по-малка чувствителност към фишинг или точно обратното, тъй като техническите умения означават и по-високо ниво на излагане на заплахи (De Kimpe, Walrave, Hardyns, Pauwels, & Ponnet, 2018). В допълнение, Button (2017) твърди, че според проучванията, макар жертвите на измами да се представят като необразовани и финансово неграмотни, изглежда е обратното. Те предлагат три възможни обяснения за това явление. Първият е „несъответствието между знанието и действието", с което се има предвид, че хората често разпознават сигналите на измамата, но не успяват да приложат това знание към своето положение. Второто обяснение се нарича „клопка за експерти" и се отнася до капана, в който попадат финансово грамотните хора, тъй като те са прекалено уверени и пренебрегват опасностите. Последното обяснение може да означава, че дори жертвите да имат достатъчно финансови познания, те нямат такова ниво на грамотност по отношение на убеждаването и тактиката на социалното инженерство (Button & Cross, 2017).

Когато се проучва по какъв начин действително се осъществява контакт с отделните жертви, в литературата са посочени и някои техники за подбор, които се използват от измамниците. Например при някои телефонни измами извършителите просто избират напосоки номера от телефонните указатели

или регистрите на публичните дружества. Други обаче използват т.нар. „списъци на измамени". Тези списъци са регистри с вече измамени лица, които се споделят и продават сред измамниците (Wood, Liu, Hanoch, Xi, & Klapatch, 2018). Levi (2008) описва това по следния начин:

> *„След като някой се е регистрирал за лотария или друг продукт чрез интернет, поща или телефон, скоро ще получи купища „предложения" от други измамници"* (Levi, 2008, p. 404)

Използването на такива списъци показва също така висока степен на повторно виктимизиране (Button, Lewis, & Tapley, 2009). Също така изглежда, че за повечето телефонни измами са отговорни сравнително малък брой извършители. В едно изследване на Marzuoli, Kingravi, Dewey и Pindrop (2016) за анализ на екосистемата за измами е използвана системата за откриване на хакери, известна като „honey pot". От 8 000 000 получени телефонни обаждания изследователите са анализирали 40 000. Само 1,8% от извикващите източници са отговорни за 66% от жалбите. Тези констатации насочват към т.нар. „скамър предприемачи", понятие, което отчита предприемаческия дух на някои измамници, които диверсифицират своите измамни схеми и се опитват да максимизират ефективността (Button, Lewis, & Tapley, 2009; Button, McNaughton, Kerr, & Owen, 2014).

Въпреки това не всички измамници са еднакво професионални и организирани. В бизнеса с телефонни измами някои извършители импровизират и променят операциите в момента, в който правоохранителните органи ги забелязват. Други мрежи са по-големи и с по-формална организация, имат някаква йерархия, разделение на труда и ставки на заплащане. Тези видове измамници може да се включват и в традиционната организирана престъпност (например търговията с наркотични вещества) или да се фокусират единствено върху измами (Levi, 2008; Barnes, 2017; Button, Lewis, & Tapley, 2009).

Що се отнася до произхода на измамниците, нигерийците почти по дефиниция участват в измамата с нигерийския принц, но като цяло нарушителите от западноафриканските държави са активни във всички видове измами (Button, Lewis, & Tapley, 2009; Levi, 2008; Button & Cross, 2017). В рамките на интернет измамите, източноевропейските престъпни групи (от Русия, Румъния, Литва,

..) са изградили особени умения и репутация (Button, Lewis, & Tapley, 2009; Levi, 2008). Трансграничните измами са особено разпространени, което затруднява прилагането на закона и националната политика за справяне с тези проблеми (Button & Cross, 2017). Ето защо е толкова необходимо да се предотвратят тези престъпления.

5. Заключения

В първата част на този набор от инструменти сме представили обобщение на текущата **разузнавателна картина** на индивидуалните измами. Тъй като измамата е престъпление с много различни форми, обхващащо широк спектър от дейности, ние сме ограничили фокуса си до индивидуалните измами, като същевременно подчертаваме смесените понастоящем онлайн и офлайн характеристики на този вид престъпления.

В основата на повечето индивидуални измами е техника, наречена социално инженерство. Това е основната тактика за спечелване на доверието на жертвите и убеждаването им да следват измамната схема. По принцип жертвата има много активна роля в изпълнението на схемата, което води до чувство на срам и вина. Показахме мястото на **социалното инженерство** в рамките на изследвания по социална психология и някои от основните принципи на изкуството на убеждаването.

Има обаче много различни **форми и видове** измама. Ние категоризирахме тези видове въз основа на тяхното съдържание или на използвания начин за контакт (лично или с използването на ИКТ). В допълнение към огромното разнообразие от форми, несъмнено нараства и нивото на усъвършенстваност и сложност. А и това вероятно е само малка част от разбирането за проблема, тъй като има огромни **неизвестни** около този вид престъпления. Жертвите не съобщават за това престъпление поради различни причини: чувството на срам, субективното усещане за тежестта на претърпените загуби, неведението за факта, че са били жертви, или по въпроса къде да докладват...

Проучванията на виктимизацията, например от Евробарометър, все пак предлагат решение на тази липса на докладване пред официалните органи. Независимо от това продължава да е жизненоважно да се направят повече изследвания върху тежестта на това престъпление и профила на жертвите. По този начин дейностите по превенция могат да бъдат по-фокусирани и ефективни. Сега ще пристъпим към разглеждане на актуалните добри практики в тази област.

02

ЧАСТ 2:
ДОБРИ ПРАКТИКИ

1. Въведение

Във втората част на настоящия набор с инструменти ще разгледаме по-задълбочено как да се предотвратят индивидуални измами. Както беше обяснено в предишната част, решаването на този въпрос е изключително трудно за полицията Button (2017) твърди, че полицията не разполага с необходимите средства за разследване на повечето от тези измами, което прави превенцията още по-важна (Europol, 2016). В допълнение към тази опасност, предотвратяването на измами обикновено получава малко академично внимание. Това затруднява изготвянето на заключения относно ефективността, въпреки че в тази област съществуват многобройни дейности (Button & Cross, 2017). В тази част от инструментариума ще разгледаме част от академичните идеи за предотвратяване на индивидуални измами, но също така ще покажем някои добри практики. И накрая, ще отправим някои препоръки, със специален акцент върху предотвратяването на измами по телефона.

Най-често срещаната тактика за предотвратяване на индивидуални измами е образованието на обществеността. Техническите мерки, като филтри за спам, софтуер за проверка на правописа, мониторинг на фалшиви домейни на уебсайтове... всички вършат някаква работа. Те обаче остават реактивни, тъй като в крайна сметка са замислени като отговор на определени методи (Jakobsson, 2016; Moreno-Fernández, Blanco, Garaizar, & Matute, 2017). Извършителите могат да се адаптират към тези мерки, показателно за което е непрекъснато нарастващото им ниво на сложност. Освен това тези технически и процедурни мерки не са 100% безопасни, тъй като в системите и хората винаги ще има недостатъци. Въпреки това всяка мярка за сигурност ни води до по-безопасно изходно ниво и е важно да се справим с това сложно престъпление.

Необходимостта от затваряне на „пробойната в сигурността“ е най-вероятната причина за множеството превантивни усилия за образоване на обществеността и за повишаване на осведомеността (Workman, 2008). Както вече споменахме, голяма част от тези усилия остават неоценени (Mears, Reisig, Scaggs, & Holtfreter, 2016), но могат да се направят някои общи констатации. Онлайн обученията, контекстното обучение[1], обучението в реална среда[2] и интерактивните игри[3] са доказали своята ефективност в подобряването на сигурността на потребителите (Sheng, Holbrook, Kumaragur, Cranor, & Downs,

2010). Хората се обучават например да разпознават определени езикови характеристики (Tabron, 2016) или да използват специални разпознавателни тактики (Moreno-Fernández, Blanco, Garaizar, & Matute, 2017). Тези обучения са от ключово значение за затваряне на „несъответствието между знанието и действието", за което споменахме по-рано. Повишаването на осведомеността води до по-добро разбиране на явлението, но не непременно до засилено прилагане на това знание към конкретната ситуация (Moreno-Fernández, Blanco, Garaizar, & Matute, 2017). Комбинацията от повишаване на осведомеността и обучение носи най-много ползи (Cross, Richards, & Smith, 2016; Europol, 2016; Bullée J.-W. , Montoya, Junger, & Hartel, 2016). Изследване, проведено от Sheng, Holbrook, Kumaragur, Cranor и Downs (2010) смеси обученията и показа 40% подобрение след въвеждането на учебни материали в сравнение с контролната група (комбинация от онлайн, контекстуално и реално обучение и интерактивни игри).

Характерно за този вид престъпления е активното участие на жертвата и високата степен на повторна виктимизация (Button, Lewis, & Tapley, 2009; Cross, Richards, & Smith, 2016). Поради тази активна роля жертвата често е обвинявана и порицавана. Кампаниите за повишаване на осведомеността следва да се съсредоточат и върху този аспект, за да дадат възможност на жертвите и тяхната среда да осъзнаят, че случилото се не е по тяхна вина, а резултат от злонамерено действие от страна на нарушителя (Burgard &

„Превенцията на ситуационните престъпления може да бъде характеризирана като мерки (1), насочени към високо специфични форми на престъпност (2), които включват управление, проектиране или манипулиране на непосредствената околна среда по възможно най-систематичен и постоянен начин (3), така че да се намалят възможностите за извършване на престъпление и да се увеличат евентуалните рискове за различните нарушители" (Lab, 2010, p. 192). По същество идеята е да се предотврати престъпността чрез намаляване на характеристиките на ситуации, които улесняват извършването на престъпление. Манипулират се специфични ситуационни характеристики, за да се блокират възможностите за престъпления (Jacques & Bonomo, 2017).

Schlembach, 2013). Много емоционални щети могат да бъдат предотвратени в това отношение. Освен това жертвите следва да бъдат информирани и за риска да станат жертва за втори път, например поради наличието на „списъци с измамени" (Cross, Richards, & Smith, 2016).

Има една академична публикация, която представлява особен интерес за тази тема. Неотдавна Mark Button и Cassandra Cross публикуваха книга, озаглавена *Cyber frauds, scams and their victims (Кибепрестъпления, измами и техните жертви)* (2017). Освен че предлагат многобройни идеи за този тип престъпления, има цяла глава, посветена на предотвратяването на кибернетичните измами и мошеничества.. Авторите развиват идеята си около рамката за превенция на ситуационната престъпност. Следвайки работата на Clarke,те са адаптирали 25-те техники за превенция на ситуационните престъпления (Cornish & Clarke, 2003) в контекста на кибер измами и мошеничества.

Тези 25 техники могат да бъдат категоризирани в пет широки стратегии (ефективни в превенцията на престъпността):

1. Увеличаване на усилието, свързано с извършването на престъпление
2. Увеличаване на риска, свързан с извършването на престъпление
3. Намаляване на ползите от престъпното деяние
4. Намаляване на подбудите, които иначе биха могли да предизвикат престъпление
5. Премахване на оправданията за престъпното деяние, които извършителите биха могли да използват

Button и Cross (2017, p203) обобщават труда си във фигурата по-долу. Препращаме всички заинтересовани читатели към тази книга, тъй като тя съдържа много задълбочен преглед на кибернетичните измами и мошенически практики и съчетава много изследователски идеи.

	Увеличаване на усилието	Увеличаване на рисковете
Индивидуални	> Защита на сметки със сложни пароли, антивирусна защита > Защитни регистрации > Да се предприемат мерки за затрудняване на намирането на лична информация за трети лица	> Редовно почистване на компютри от вируси, шпионски софтуер > Проверка на уебсайтове, електронни писма и обаждащи се
Организация	> Подходящи контроли за защита на личната информация на клиентите > Основни проверки: проверка дали клиентите са тези, за които се представят	> Обмен на информация: съпоставяне и анализ на данни > Проверка на гласа и местоположението на клиентите
Полицейски органи	> Прекъсване на дейността на измамниците > Специална тактика за залавяне на престъпници (Scambaiting) > Преследване и санкции за измамници с помощта на гражданското, регулаторното или наказателното право	> Обмен на информация: съпоставяне и анализ на данни > Централно докладване > Публикуване на информация за предполагаеми измами, съмнителни уебсайтове > Фалшиви схеми за предупреждаване на потенциалните жертви

Намаляване на изгодата	Намаляване на подбудите	Премахване на оправданията
Ако измамникът е известен и разполага с активи, да се инициира граждански иск за обезщетение или да се поиска обезщетение чрез наказателен процес		
Ако измамникът е известен и разполага с активи, да се инициира граждански иск за обезщетение или да се поиска обезщетение чрез наказателен процес		Общувайте с клиентите, за да ги информирате за рисковете и добрите практики за намаляване на риска
> Ако измамникът е известен и разполага с активи, да се инициира граждански иск за обезщетение или да се поиска обезщетение чрез наказателен процес > Мониторинг на финансовите трансфери към трети страни с висок риск, за да се идентифицират възможните жертви и да се предупредят за потенциална виктимизация	> Ограничение на информацията за това как са извършени някои измами > Регулиране на рекламни и промоционални дейности	> Съобщаване на широката общественост и рисковите групи за рисковете и добрите практики > Рекламни кампании: телевизия, радио, вестници, специализирани публикации, онлайн > Медийно отразяване > Специализирани уебсайтове > Листовки по пощата > Електронни писма, текстове, туитове в социалните медии > Дейности на Общността и на групите по интереси > Драматизирани сюжети

2. Ако звучи прекалено добре, за да е истина, вероятно не е.

В този раздел ще разгледаме някои от добрите практики, с които се запознахме по време на българското председателство. Проектите и кампаниите се обсъждат в различни категории, всяка от които представлява целевата група: с универсална, подбрана или предписана превенция, съответно цялото население, специфична рискова група или хора, които вече са били жертви. Всички тези кампании и проекти също могат да бъдат намерени в третата част на този инструментариум.

Универсална превенция

Именно българското председателство реши да се съсредоточи върху измамите и мошеническите практики и това чувство за неотложност се отрази върху политиката на националната полиция. На този проблем, и по специално на телефонните измами, е посветен цял „отдел за измами“ в Генерална дирекция „Национална полиция“. Те действат реактивно, но превенцията също е основна задача за справяне с тази престъпност. Като част от работата се осъществяват информационни кампании за повишаване на информираността и осведомеността на населението за това престъпление. Разпространяват се например информационни брошури, но също така се дават съвети чрез национални радио предавания. Друг пример от България са стикерите,

които се раздават. Те съдържат превантивни съобщения и хората трябва да ги залепят на телефона си. Идеята е, че когато се обаждат, те запомнят превантивното съобщение, защото виждат стикера.

В Швеция работи подобен орган по предотвратяването на измами: Шведски център за национални измами. Тяхната превантивна работа е насочена към повишаване на осведомеността чрез традиционните медии и каналите на социалните медии, но също и към изграждане на външни партньорства с органите на властта и с бизнеса. Някои кампании имат двойна цел. Освен за повишаване на осведомеността за опасностите от измами чрез медийни кампании, те използват медиите и за ограничаване на определени приложения със сериозни проблеми в сигурността, които се използват от измамници. Това медийно отразяване накара разработчиците на приложения да подобрят сигурността.

На европейско равнище, всяка година през октомври се провежда Европейски месец на кибернетичната сигурност[4]. Тази кампания на равнище ЕС има за цел да насърчи кибернетичната сигурност сред гражданите и организациите и да открои простите стъпки, които могат да бъдат предприети за постигането на тази цел. Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA), Европейската комисия, Европол и в частност Европейският център за киберпрестъпления и широк кръг публични и частни партньори от държавите членки работят заедно за постигането на тази цел и организират многобройни събития и кампании през месеца. През третата седмица на кампанията от 2018 г. фокусът беше върху кибернетичните измами. Целта беше да се информира широката общественост относно начините за идентифициране на заблуждаващо съдържание с цел да защитят себе си и финансите си онлайн. Европейският център за киберпрестъпления, Европейската банкова федерация (EBF) и други партньори обединиха сили, за да организират кампания за повишаване на осведомеността по тази тема. По-долу можете да намерите някои примерни материали.

ROMANCE SCAM

Scammers target victims on online dating websites, but can also use social media or email to make contact.

WHAT ARE THE SIGNS?

Someone you have recently met online professes strong feelings for you, asking to chat privately.

Their messages are often poorly written and vague.

Their online profile is not consistent with what they tell you.

They may ask you to send intimate pictures or videos of yourself.

First they gain your trust. Then they ask you for money, gifts or your bank account/credit card details.

If you don't send the money, they may try to blackmail you. If you do send it, they will ask for more.

ARE YOU A VICTIM?

Don't feel embarrassed!
Stop all contact immediately.
If possible, keep all communication, such as the chat messages.
File a complaint with the police.
Report it to the site where the scammer first approached you.
If you have provided your account details, contact your bank.

WHAT CAN YOU DO?

- **Be very careful** about how much personal information you share on social network and dating sites.
- **Always consider the risks.** Scammers are present on the most reputable sites.
- **Go slow** and ask questions.
- **Research** the person's photo and profile to see if the material has been used elsewhere.
- **Be alert** to spelling and grammar mistakes, inconsistencies in their stories and excuses such as their camera not working.
- **Don't share** any compromising material that could be used to blackmail you.
- If you agree to meet in person, **tell family and friends** where you are going.
- **Beware of money requests.** Never send money or give credit card details, online account details, or copies of personal documents.
- **Avoid sending them upfront payments.**
- **Don't transfer money** for someone else: money laundering is a criminal offence.

EUROPOL EC3 | European Cybercrime Centre

EBF

EUCPN

#CyberScams

BANK VISHING CALLS

Vishing (a combination of the words Voice and Phishing) is a phone scam in which fraudsters try to trick the victim into divulging personal, financial or security information or into transferring money to them.

WHAT CAN YOU DO?

- **Beware** of unsolicited telephone calls.
- **Take the caller's number** and advise them that you will call them back.
- In order to validate their identity, **look up the organisation's phone number** and contact them directly.
- **Don't validate the caller using the phone number they have given you** (this could be a fake or spoofed number).
- Fraudsters can find your basic information online (e.g. social media). **Don't assume a caller is genuine** just because they have such details.
- **Don't share** your credit or debit card PIN number or your online banking password. Your bank will never ask for such details.
- **Don't transfer money** to another account on their request. Your bank will never ask you to do so.
- If you think it's a bogus call, **report it to your bank.**

EUROPOL EC3 European Cybercrime Centre | EBF | EUCPN

#CyberScams

Друга кампания за повишаване на осведомеността е антифишинг кампанията, проведена от белгийския Център за киберсигурност (CCB). Тази класическа кампания предостави информация за разпознаването на електронни писма, съдържащи измама. Кампанията беше разпространена чрез видеоклипове, подписи по електронна поща, банери, плакати, но и на уеб страница. Освен съвети за информация и превенция, уебсайтът предостави и тест, който позволява на хората да проверят доколко са защитени от фишинг. След теста се показват превантивни материали, информиращи какви стъпки и действия могат да се предприемат за по-нататъшно подобряване на сигурността. Освен това хората могат да изпращат електронни писма, които считат за съмнителни, на електронен адрес на CCB. След това CCB проверява тези електронни писма и линкове към измамнически уебсайтове и ги поставя в черния списък на четирите основни браузъра (Internet Explorer, Mozilla Firefox, Google Chrome и Safari). Постигнатото е резултат от партньорството на ЕС за

Инициативата на ЕС за борба с фишинга е проект, който се финансира от Европейската комисия и има за основна цел прекъсването на измамнически уебсайтове. The objective is to operationally prevent phishing scams from fooling victims by blocking the websites that are used for this purpose. It is based on a public-private partnership dedicated to fight phishing.

More information:
https://ec.europa.eu/home-affairs/financing/fundings/projects/HOME_2013_ISEC_AG_INT_4000005246_en

антифишинг инициатива. След поставянето им в черния списък, въпросните уебсайтове са блокирани за други потребители. Механизмът на ССВ е в състояние всеки ден да поставя пет уебсайта в списъка, което способства за изграждането на много интересен механизъм за групова превенция.

Селективна

Както вече беше отбелязано в предишните раздели, при този вид престъпност много внимание се обръща на възрастните хора. Това вече беше изяснено в набора от инструменти по отношение на престъпления, насочени към възрастните хора, изготвен по време на словашкото председателство. Редица проекти, които през тази година се включиха в конкурса на Европейската награда за превенция на престъпността, бяха посветени на този вид престъпления, насочени към възрастните хора. Например германският проект „Здравей, бабо, имам нужда от пари", който беше на второ място, се фокусира върху телефонни измами, включващи номера с внука. Чрез интерактивна сценична игра възрастните хора се информират за това престъпно явление, като в същото време целта е да се намали субективното чувство на несигурност.

По същия начин чешката програма ‘„Nedáme se“ (или „Не се предаваме“) е интерактивна образователна игра, в която се пресъздават четири вида често срещани измамни манипулативни схеми, използвани срещу възрастните. Това са рекламни кампании, продажба на парфюми на улицата, телемаркетинг и продажба на домашни любимци. Освен актьорите, полицай и автора на пиесата, на сцената се появява психологът доц. д-р Романа Мазалова. Те влизат в пиесата и си взаимодействат с публиката, като така ги обучават на нови стратегии за защита. Затова пиесата е не само приятна, но и се превръща в нова образователна форма срещу т.нар. „Шмекери“ или измамници. В

проекта участваха общо хиляда възрастни хора. Експериментално беше проучен образователният ефект на тази сценична игра върху публиката. Резултатите потвърдиха, че възрастните, които са видели играта, се оказват по-успешни в защитата срещу измамни продавачи. Експериментът сравнява 130 възрастни, които са гледали сценичната игра, с контролна група. Половин година след гледането на пиесата експерименталната група отказваше фалшива сделка 2,5 пъти по-често от групата, която не е гледала пиесата.

Друг проект, фокусиран върху работата с възрастни хора, е проектът „Цената на приятелството" от Румъния. Проектът е насочен към намаляване на риска по-възрастните хора да станат жертви, като се следват тези цели: познаване на нагласата и поведението на целевата група, повишаване на нивото на превантивни знания на възрастните хора и повишаване на капацитета за самозащита. Целевата група бе съставена от хора над 60 години, които са членове на местни клубове за възрастни. През 2017 г. полицията е провела общо 34 превантивни информационни дейности. Информацията обхваща рисковете, свързани с възрастта, но също така и предотвратяването на виктимизацията в случай на измамни схеми, като например фалшиви телефонни кампании. Бяха проведени и онлайн обучителни курсове за възрастни хора. Освен това беше организиран „бал за безопасност на възрастните", поставящ началото на публична информационна кампания.

Освен повишаване на осведомеността в тази целева група, в България се реализира интересен механизъм. Българската секция за измами има редица добри партньорства с частни субекти, като банковия сектор. В по-голяма степен ситуационен по характер, този механизъм за превенция въвежда система за контрол, когато лице, навършило 50 години, изтегли сума от над 3000 евро. Когато това се случи, банковият служител ще получи предупреждение и може да зададе някои въпроси, за да провери дали възрастният човек не участва в манипулативна схема.

Предписана

Друг набор от превантивни дейности е насочен към хора, които вече са били жертви. Специфичните интервенции са насочени към предотвратяване на трайната виктимизация и многократното попадане на жертвата в различни измамни схеми. Проектът Sunbird в Австралия например е насочен към финансови транзакции между Западна Австралия и някои западноафрикански държави. Полицията наблюдава такива транзакции и прави списък на тези, които изглеждат незаконни. След това се установява контакт с жертвите и им се обяснява защо полицията смята, че те могат да бъдат жертва на измама. Според оценките 73% от хората, с които полицията се е свързала, престават да изпращат пари в тези държави (Button & Cross, 2017).

В Обединеното кралство Action Fraud, националният център за отчитане на измами и киберпрестъпления, редовно докладва за най-новите измами и мошенически практики (Button & Cross, 2017). Те също така насочват жертвите към определени групи за подкрепа, за да помогнат на засегнатите от престъплението, или им предоставят информация към кого трябва да се обърнат5. Така може да се помогне на жертвите да намалят емоционалните щети, както и да възстановят загубени пари, или да се дадат съвети как да действат жертвите в бъдеще, ако се свържат отново с тях. Поради съществуването на списъци с вече измамени (вж. по-горе) има реална опасност това да се случи.

Както вече беше споменато, жертвите страдат от различни негативни ефекти, дължащи се на тяхната виктимизация. Наред с другото, жертвите са изразили силна нужда просто да бъдат изслушани и признати за жертви. Всъщност съществуват — дори и в световен мащаб — малко услуги за подкрепа на тези жертви. Рядък пример за такава програма за подкрепа се намира в Канада: Службата за помощ на възрастни хора. Персонал от по-възрастни доброволци и връстници осигурява чрез телефонна услуга подкрепа за жертвите на измами. Те предлагат съвети и предупреждения, изслушват и дават увереност (Cross, 2016). Такава инициатива не само предлага подкрепа на отделните жертви, но също така спомага за повишаване на нивото на докладване, което от своя страна подобрява информирането на полицията и превенцията.

3. Предотвратяване на измами по телефона: как да Ви помогна?

Секретариатът на ЕМПП организира семинар на тема индивидуални измами. Редица експерти се събраха и обсъдиха своите идеи и превантивна работа в тази област. Семинарът се състоеше от три части. Първо, обсъди се разузнавателната картина на индивидуалните измами. Това е отразено в първата част от настоящия набор с инструменти. Второ, различни проекти бяха представени и обсъдени с групата, което е отразено в раздела по-горе. Накрая, беше организиран метод на световното кафене, за да се изготвят препоръки относно предотвратяването на измами по телефона. По този начин експертите обсъдиха своите препоръки в по-малки групи. Ето експертите, които участваха в семинара:

- Марк Бътън, Университет в Портсмут, Обединено кралство
- Майкъл Уил, Европол, AP Furtum
- Симеон Димчев, отдел „Измами“ в Главна дирекция „Национална полиция“, България
- Шарлота Маурицсон, Национален център за борба с измамите, Швеция
- Андрис Боманс, Център за киберсигурност, Белгия
- Константин Лица, Отдел за борба с измамите, Румъния
- Аурелиан Бокан, главна дирекция на полицията на Букурещ, Румъния
- Романа Мазалова, проект „Nedáme se“, Чешка република

Ние съчетахме препоръките от примера на Button (2017) по-горе и използвахме петте широки стратегии на Clarke като ръководна рамка. От само себе си се разбира, че те не изключват взаимно, а могат да бъдат комбинирани в различни проекти. Както вече бе споменато, това са:

1. Увеличаване на усилието
2. Увеличаване на риска
3. Намаляване на изгодата
4. Намаляване на подбудите
5. Премахване на оправданията

Увеличаване на усилието

Първата възможна стратегия е да се увеличат усилията, които извършителят трябва да положи, за да успее измамата. Идеята тук е, че когато усилията са прекалено големи, нарушителят ще се въздържа от извършване на престъпление. Както стана ясно в първата част на този набор с инструменти, нарушителите могат да намерят потенциалните си жертви в легитимни списъци. Организациите открито публикуват данните за контакт на хората, но хората също споделят своите телефонни номера свободно и доброволно. Например можете да видите телефонни номера на профили във Facebook, страници на LinkedIn... Ограничаването на публикуването на телефонни номера в тези списъци и профили в социалните медии вече може да затрудни извършителя на престъплението да се свърже със своите жертви.

Друг начин за увеличаване на усилията е да се ограничи достъпът до използването на телефонни номера. Изключително лесно е да закупите предплатена карта или нов телефонен номер. Това позволява на нарушителите да продължат да променят номерата, което затруднява правоприлагащите органи да ги проследява. Една идея от семинара беше да се ограничи телефонният номер на дадено лице, като се свърже с банковата му сметка или с идентификационния му номер. В това отношение е препоръчително да се осъществява цялостно сътрудничество с мобилните компании. Това не само увеличава усилията за нарушителя, но също така намалява анонимността и увеличава риска от задържане.

С нарастването на онлайн обажданията остава доста лесно да се свържете с потенциалните жертви и да измислите местоположението си, за да изглежда достоверно. Засиленото използване на пароли, криптирането и осигуряването на почти пълна невъзможност да се фалшифицира местоположението също следва да увеличи усилията, които нарушителят трябва да предприеме, за да се свърже с жертвите и да ги измами.

Т.нар. scam baiting също се споменава като възможна тактика, въпреки че това само по себе си не е достатъчно. Въпросната тактика се изразява в това, че полицейските органи или друга организация могат да се опитат да измамят измамниците, като ги подведат да полагат безполезни усилия и им губят времето. Докато са заети да преследват тези цели, те не могат да измамят невинни жертви.

Увеличаване на риска

От решаващо значение за предотвратяването на измами е да знаете с какво си имате работа. Споделянето на информация е от ключово значение тук. Тъй като измамите могат да бъдат докладвани на различни инстанции, например полицията, но също и частни организации, обменът на информация между публичния и частния сектор е задължителен. Това би позволило по-бърза реакция и по-адекватни превантивни мерки, като по този начин се увеличи рискът. Ето защо трябва да бъдат включени и други заинтересовани страни, освен правоприлагащите органи. Мобилните компании, банките, организациите с нестопанска цел ... - всички имат своята роля и своята важна част за информационния пъзел. Това сътрудничество не трябва да спира и на националните граници. Тук Европол играе ключова роля като посредник за обмен на информация и трансгранични дейности. Поради факта, че този вид престъпност все повече придобива международен мащаб, за споделяне на информация трябва да се търсят и трети страни. Информацията може да бъде споделена и с широката общественост. Ако хората знаят от името на кои фирми се представят измамниците, ше бъдат бдителни.

Разбира се, тази информация трябва най-напред да бъде събрана и жертвите трябва да бъдат по-добре запознати с възможностите за докладване. Кампаниите за повишаване на осведомеността например също биха могли да насочат вниманието към това как докладването на престъплението води до успешно разследване и адекватни решения. Наличието на централна система за докладване за жертвите, с достъп до всички участници на място, също би направило процеса на докладване много по-лесен и би намалило задръжките на жертвите, за да могат действително да докладват.

Друга стратегия за увеличаване на рисковете е да се намали анонимността. Както беше споменато в рубриката „увеличаване на усилията“, развитието на ИКТ позволи да се прихваща местоположението, откъдето се обаждате. По този начин жертвата може да бъде накарана да повярва, че говори с някой от нейната държава, а вместо това да говори с чужбина. По-трудното локализиране на Вашето местоположение ще доведе до повишена експозиция и риск от залавяне. Такъв механизъм може да се използва например от банките. Те може да използват софтуер за разпознаване на глас и услуги за местоположение, за да проверят дали данните съответстват на обичайните данни на клиента. Сравняването с „обичайните“ характеристики също е нещо, което се използва в примера на някои банки в България (вж. по-горе), където

банковият служител бива предупреден, когато човек над 50 години иска да изтегли по-голяма сума от обикновено.

Според експертите от семинара кампаниите за повишаване на осведомеността следва също така да обясняват рисковете и санкциите на нарушителите, за да ги възпират. Тези санкции следва освен това да бъдат засилени, за да се противопоставят на очакваните ползи за нарушителите. За особено подходящи в това отношение се считат финансовите санкции. Заедно с по-специализирано обучение и ресурси за правоприлагане, това престъпление следва да се третира като вид организирана престъпност и да се наказва съответно.

Намаляване на изгодата

Този трети набор от мерки за предотвратяване на измами по телефона включва намаляване на облагите, които биха могли да бъдат получени с извършването на това престъпление. Основната препоръка в тази връзка е да се изземат активите, които се получават чрез телефонни измами. Важна стъпка е да се следи паричният поток. Австралийският пример, посочен по-горе, ни показва точно за какво става дума и колко ефективно може да бъде откриването на подозрителни транзакции. Експертите изразиха необходимостта от инициатива на равнище ЕС за адаптиране на банките към европейската перспектива. Друга препоръка е да се конфискува на първо място оборудването и ресурсите, необходими за извършване на престъплението.

Намаляване на подбудите

По време на семинара не бяха формулирани конкретни препоръки за намаляване на подбудите. При все това, следвайки Button (2017), можем да кажем, че в някои случаи е важно да не се предоставя прекалено много информация за това как е извършена измамата, за да се предотвратят имитации. Освен това е известно, че измамниците ще се свържат с жертвите с предложение, което ще позволи например да се покрият загубите им. Разбира се, намерението е да се извърши втора измама. Повишаването на осведомеността по този въпрос е от решаващо значение.

Премахване на оправданията

Последният набор от препоръки е съсредоточен главно върху повишаване на осведомеността относно измамите по телефона и как най-добре да се предпазим от посегателство. Това включва класическата информационна кампания чрез различни канали като радиото, телевизията, флаерите... Информацията, която трябва да бъде споделена, може да обясни начина на действие при някои измами, но също и начините за защита. Това стана ясно с примерите от Румъния или Чешката република. Сценичното представяне например е интересен метод за осведомяване на хората как да прилагат защитни стратегии в своето конкретно положение. Публично-частните партньорства са също толкова важни за разпространението на превантивно послание, колкото и при споделянето на информация за инедтифициране на нарушителите. Това е споделена отговорност, която може да се осъществи и в рамките на общностни или сходни групи.

Разбира се, кампаниите трябва да бъдат оценени, за да се гарантира ефективност. Важен аспект в това отношение е разпространението на едно и също послание в различните организации, но също и в различните държави. Примерът от Европол (вж. по-горе) е добър пример за това. Добре би било също действително да се споделя информация за разнообразието от измами, които съществуват, и да се обяснява техният начин на действие. Посланието за това как да се предпазите обаче трябва да е възможно най-ясно и просто. *Просто кажете „не“.*

Повишаването на осведомеността следва да се съсредоточи и върху тези, които вече са били жертви. Те не само трябва да бъдат осведомени за рисковете от повторна виктимизация, но очевидно се нуждаят и от подкрепа. Тук трябва да се отбележат мрежите за подкрепа, чрез които жертвите споделят информация и се подкрепят взаимно за претърпените загуби (финансови и емоционални). Експертите споменаха и гореща линия, която да предлага на жертвите точната информация и съвет.

4. Заключения

В тази втора част на инструментариума разгледахме предотвратяването на индивидуални измами. Първо, бяха направени някои общи коментари въз основа на академични изследвания. Въпреки малкото академични проучвания за предотвратяване на индивидуални измами установихме, че най-често срещаната тактика за превенция е да се **образоват хората** как да разпознават измамите и как да реагират на тях. Едно проучване показа 40% подобрение след оценка на материалите за обучение, които са били дадени на експериментална група. Такива оценки обаче са оскъдни и можем само да препоръчаме повече изследвания и оценки по този въпрос.

Изследванията също така показаха необходимостта да се съсредоточим върху хора, които вече са били жертви. Това се дължи на високите нива на повторно виктимизиране, но също и на опасностите от вторична виктимизация чрез връстници, семейство, официални органи... **Жертвите** трябва да бъдат подкрепяни в техните загуби и да са информирани за опасността от повторно попадане в подобни схеми.

Второ, направихме преглед на някои **добри практики**, които съществуват в държавите членки. Те са категоризирани според тяхната целева група: универсални, селективни и предписани превантивни дейности. В третата част на този инструментариум читателят може да намери и всички тези проекти.

И накрая, въз основа на семинар с различни европейски експерти, ние формулирахме **препоръки** за това как да се предотвратят телефонните измами. Те бяха съсредоточени върху петте широки стратегии за превенция на ситуационните престъпления: увеличаване на усилията, увеличаване на риска, намаляване на изгодата, намаляване на подбудите и премахване на оправданията.

Factsheet

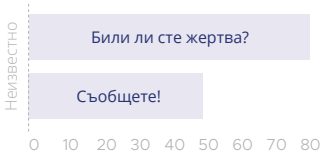
Предотвратяване на телефонни измами

КАК МОГА ДА ВИ ПОМОГНА?

СОЦИАЛЕН ИНЖЕНЕРИНГ

В основата на повечето индивидуални измами е техника, наречена социално инженерство. Това е основната тактика за спечелване на доверието на жертвите и убеждаването им да следват измамната схема. По принцип жертвата има много активна роля в изпълнението на схемата, което води до чувство на срам и вина.

НЕИЗВЕСТЕН БРОЙ



ТОВА СА СТЪПКИТЕ

01 Увеличете усилието

> Ограничете публикуването на телефонни номера
> По-силни пароли и криптиране
> Специална тактика за измама на измамници (Scambaiting)

02 Увеличете риска

> Споделяне на информация между всички участници
> Насърчаване на съобщаването
> Ограничаване анонимността на обаждащия се

03 Намалете изгодата

> Конфискация на незаконно придобито имущество
> Следете паричния си поток

04 Намалете подбудите

> Предотвратяване на подражатели
> Повишаване на осведомеността за измами при извличане

05 Премахнете оправданията

> Повишаване на осведомеността
> Оценяване на кампаниите
> Подкрепа за жертвите

Желаете ли да научите повече?
Посетете www.eucpn.org

03 ЧАСТ 3: ПРИМЕРИ ОТ ПРАКТИКАТА

„ИЗМАМАТА С БАБА Й ДЯДО“ — ЧУВАЛИ ЛИ СТЕ НЯКОГА ЗА ТОВА? (АВСТРИЯ)

Кратко описание:
Звъни се по телефона в дома на жертвата (баба). Без да подозира, жертвата приема, че повикващият е приятел или роднина. Жертвата започва да предполага кой се обажда, изрича няколко различни имена на членове на семейството (в повечето случаи имена на внуци или племенници), измамникът избира едно и твърди, че е този човек. След това обаждащият се описва своята извънредна финансова ситуация и моли жертвата за пари. В такива случаи не е необичайно жертвите да губят всичките си спестявания; често тази загуба води до сериозни емоционални страдания, дори физически заболявания.

Превенцията на престъпността се оказва трудна; потенциалните жертви често не могат да бъдат повлияни чрез послания или кампании. Беше установено, че банковият персонал има ключова роля в превенцията; така тази кампания, в сътрудничество с Австрийската национална банка и Търговската камара, бе насочена към информиране и мотивиране на широката общественост, и по-специално на банковия персонал; тя включва и информационен филм,

озаглавен „Измамата с баба и дядо".

Начало/продължителност:
Дата на стартиране на проекта: 01.04.2015 г.

Съобщение за печата (пресконференция): 18.02.2016 г.

Текущо: повишаване на осведомеността с печатна кампания, на базата на изготвения видеоклип

Основно проучване:
Отделът за превенция на престъпността и подкрепа на жертвите направи оценка на състоянието и въздействието, начина на действие и разпространението на този вид измама, заедно със звеното за икономически престъпления, звеното за измами, фалшификации и икономическа престъпност, и отдела за анализ на престъпността в Службата за криминално разузнаване на Австрия.

Бюджет:
Най-скъп беше клипът (7 000 евро), финансиран от Службата за криминално разузнаване на Австрия, и разходите за печатната кампания (1000 евро); пресконференцията беше финансирана и от Националната банка; разпространението на съдържание беше финансирано съвместно от трите заинтересовани страни.

Вид оценка:
Един от партньорите по проекта — Австрийската национална банка — организираха пътно шоу; през лятото на 2016 г. те посетиха всички провинции и области в Австрия. След обиколката служителите отделиха време и влязоха във всяка банка във всеки град, където бяха спрели по пътя, и разпитаха банковите служители дали са чували за измамата с баба и дядо, дали са гледали клипа и дали знаят как да реагират правилно, в случай че срещнат подозрително лице.

На 91% от служителите измамата с баба и дядо е била известна, те също са знаели как да реагират в случай на подозрение. Клипът е бил познат само на 19% средно, затова беше решено да се проведе друга кампания с информационни листове за промотиране на модела и клипа отново.

Орган, провеждащ оценката/ съгласуването:
Външен: Австрийската национална банка

Тип метод за събиране на данни:
Оценка на въздействието, извършена от Австрийската национална банка в 158 банки в цяла Австрия.
За повече информация: http://eucpn.org/document/granny-scam

ЗДРАВЕЙ, БАБО, ИМАМ НУЖДА ОТ ПАРИ (ГЕРМАНИЯ)

Кратко описание:
Възрастните хора са привлекателни за измамниците. Един от методите, станал популярен сред престъпниците, е „измамата с внука“, в която измамниците се представят за роднини на жертвата, като се преструват, че са в отчаяна ситуация и спешно се нуждаят от пари.

Проектът „Здравей, бабо, имам нужда от пари" предлага иновативна концепция за предотвратяване на престъпления по тази схема. Това е интерактивна сценична игра, която предлага преглед на преобладаващите техники и показва мерки срещу превръщането в потенциална жертва. Той също така намалява субективния страх от измамниците и насърчава човека да бъде по-уверен в себе си.

Публиката е активно ангажирана в изпълнението. Случайно подбрани членове на публиката участват в представянето като активни участници, докато актьорите импровизират и реагират спонтанно на включването на публиката. Реалните сюжети в основата на представлението способстват да се предаде чувството за неотложност, а забавният фактор осигурява дълготрайно впечатление.

Начало/продължителност:
Проектът стартира на 28.3.2012 г. и продължава да се изпълнява.

Основно проучване:
Налице е статистическо увеличение на „измамите с внуци“, идентифицирани от PKS (Статистика на престъпността в полицията). Проучен бе броят на случаите, както и произтеклите щети.

Броят на делата във федералната провинция Баден-Вюртемберг се е увеличил от 95 (2007 г.), 64 (2008 г.), 143 (2009 г.) до 311 през 2010 г. Финансовите загуби във федералната провинция Баден-Вюртемберг са се увеличили от 234 890 евро (2007 г.), 45 870 евро (2008 г.), 557 900 евро (2009 г.) до 1 108 131 евро през 2010 г.

Бюджет:
Написването и поставянето на пиесата е доброволен труд на Алън Матиаш, подкрепен от неговия театрален ансамбъл и партньорите

за сътрудничество (полиция и градски органи). Разходите за едно изпълнение — включително двама участници и оборудване — бяха общо 790-890 евро, в допълнение към пътните разходи.

Вид оценка:
Оценка на процеса и въздействието.

Орган, провеждащ оценката/ съгласуването:
Външен: Тереза Зиглер, студентка в университета по приложни науки в Кел.

Тип метод за събиране на данни:
Анкета, базирана на въпросник.
За повече информация:
https://eucpn.f2w.fedict.be/document/hello-granny-i-need-money

SILVER SURFER (СРЕБЪРЕН СЪРФИСТ) (ЛЮКСЕМБУРГ)

Кратко описание:
Проектът „Сребърен сърфист" е проект на възрастни граждани за възрастни граждани. Доброволците — възрастни граждани преминават специално обучение за създаване на информираност за безопасното използване на интернет. Те предават

своите знания на други възрастни граждани чрез конференции, например по време на събития за възрастни хора, в клубове за възрастни или в сдружения на възрастни. „Сребърни сърфисти" работят като мултипликатори.

Проектът е създаден през 2014 г. по инициатива на BEE SECURE и се основава на сътрудничество между Министерството на семейството, интеграцията и Големия регион на Люксембург, SECURITYMADEIN.LU, RBS-Center fir Altersfroen и SenioreSécherheetsBeroder.

Начало/продължителност:
Проектът стартира през 2014 г. и продължава да се изпълнява.

Основно проучване:
През 2013 г. партньорът SECURITYMADEIN.LU започна проучване по време на панаир за възрастни граждани. Резултатът показа, че анкетираните възрастни граждани използват компютъра само за обмен на електронни писма

(94%) или за връзка по Скайп (32%) с членове на семейството. Едва половината от тях знаеха за интернет измами. 32% вече са били жертви на фишинг атаки, а 12% са жертви на измама. Същото проучване беше повторено през 2014 г. на същия панаир. Резултатите са сравними и показват, че възрастните граждани използват интернет по-често (с 5% повече в сравнение с 2013 г.).

За повече информация:
https://eucpn.org/document/silver-surfer

НЕ СЕ ОПИТВАЙ ДА МЕ ЗАБЛУДИШ (ШВЕЦИЯ)

Кратко описание:
Проектът „Не се опитвай да ме заблудиш" беше създаден, за да предотврати престъпления срещу измами срещу възрастни хора чрез повишаване на осведомеността за тези престъпления и да улесни възможните жертви да разпознаят опитите за измама и да се защитят срещу тях.

Съгласно избраният за проекта метод се създава информационен пакет и структура за това как материалът може да се използва в активни срещи, където участниците да се обучават за различни ситуации, в които могат да станат жертви на измама и как могат да действат за предотвратяване на измамата.

Материалът следва да се използва на три различни срещи и включва ръководство за ръководителя на

срещата, три различни късометражни филма и три различни учебни ръководства. Всеки случай включва работа с един филм и едно учебно ръководство. Материалът е за самостоятелно обучение и се основава на различни случаи, които могат да бъдат използвани за дискусии и практически упражнения.

Начало/продължителност:
Проектът стартира официално на 16.9.2015 г. и продължава да се изпълнява.

Основно проучване:
Националният център за борба с измамите в шведската полиция анализира развитието на измамите в Швеция и отбеляза рязко повишаване на измамите срещу възрастни хора. Задълбоченият анализ показа кой начин на действие е бил използван в тези престъпления и кои места за набиране на жертви са били използвани. Този анализ беше използван за създаването на материала и примерите в проекта. Анализът се основава главно на данни за престъпления, докладвани на шведската полиция.

Бюджет:
Стойността на проекта не е уточнена. Тъй като проектът е приоритизиран, всички ресурси са взети от обикновената финансова рамка и затова не са уточнени. Полицията и организациите сами са произвели филмите и другите материали и затова разходите са били сравнително ниски.

Вид оценка:
Оценката на процеса все още не е приключила, но методът ще бъде оценен чрез измерване на осъществените срещи и и проучване на лицата, които са участвали, като се посочи мнението им за проекта и до какви промени е довел той по отношение на осведомеността им относно измамите и мерките, които да предприемат, за да не се превърнат в жертва. Оценката на въздействието все още не е направена, но ще се изготви анализ, като работата е започнала с анализиране на промените в докладваните престъпления от този тип и различията по отношение на извършените престъпления и опитите за престъпления.

За повече информация:
https://eucpn.f2w.fedict.be/document/do-not-try-fool-me

АВСТРИЯ: СПИСЪКЪТ ЗА НАБЛЮДЕНИЯ В ИНТЕРНЕТ

Кратко описание
Списъкът за наблюдение е проект за предотвратяване и борба с онлайн престъпления, като измама и други онлайн капани. От 2013 г. екипът на проекта проучва фалшиви сайтове и случаи на онлайн измами, с цел сериозно да информира широката общественост с новинарски статии на своя уебсайт. Неговите уникални характеристики са непрекъснатост и ефективна оптимизация на търсачките. Проектът също така допринася за борбата с онлайн престъпността основно чрез мрежата, която е създадена между платформи за електронна търговия, частни банки, правителствени органи и правоприлагащи органи в Австрия. От съществено значение за успеха на проекта е и тясното сътрудничество с органа за онлайн разрешаване на спорове „Интернет омбудсман“ и със заинтересованите страни и потребителите на уебсайта, които допринасят за докладването на случаи.

Начало/ Продължителност
Проектът стартира на 3 юли 2013 г. и продължава да се изпълнява.

Основно проучване
Извършен беше анализ на контекста от екипа на Интернет омбудсмана. Забелязаното нарастване на случаите на интернет измами подчертава необходимостта от увеличаване на усилията за повишаване на осведомеността. Размерът на делата се е увеличил с 18% през 2012 г. спрямо предходната година. На базата на тези данни, Интернет списъкът за наблюдение е създаден от Австрийския институт за приложни телекомуникации.

Бюджет
Списъкът за наблюдение е финансиран от австрийското Федерално министерство на труда, социалните въпроси и защитата на потребителите, Австрийската камара на труда, най-големият австрийски онлайн пазар willhaben.at и Bank Austria. Годишните разходи по проекта възлизат на приблизително 65 000 евро.

Вид оценка
През август 2014 г. е извършена вътрешна оценка на процеса под формата на онлайн проучване сред читателите на интернет страницата за наблюдение. Въз основа на тези констатации проектът беше доусъвършенстван, например

с използването на по-достъпен за възрастните хора език. Не е извършена външна оценка или оценка на въздействието, но се прави ежегодна вътрешна оценка на въздействието.

Орган, провеждащ оценката/ съгласуването
Вътрешен: от екипа на проекта и консултативен съвет с публични и частни заинтересовани страни

Тип метод за събиране на данни
Годишната оценка се основава на Google Analytics, като потребителска статистика, посетители на уебсайта, продължителност на посещенията, ... обратна връзка от потребители и партньори за финансиране, както и непрекъснато с проверки дали новините за интернет измами водят до изчезване на фалшиви сайтове.

Връзки към допълнителна информация
http://eucpn.org/document/watchlist-internet

ОТДЕЛ „ИЗМАМИ", ГЛАВНА ДИРЕКЦИЯ „НАЦИОНАЛНА ПОЛИЦИЯ" (БЪЛГАРИЯ)

Кратко описание:
В България цял „отдел измами" в Генерална дирекция „Национална полиция" работи по проблема с телефонните измами. Освен реактивната полицейска работа, основната им задача е осъществяването на превенция. Като част от работата се осъществяват информационни кампании за повишаване на информираността и осведомеността на населението за това престъпление. Разпространяват се например информационни брошури, но също така се дават съвети чрез национални радио предавания. Друг пример от България са стикерите, които се раздават. Те съдържат превантивни съобщения и хората трябва да ги залепят на телефона си. Идеята е, че когато се обаждат, те запомнят превантивното съобщение, защото виждат стикера.

МЕХАНИЗЪМ ЗА БОРБА С ИЗМАМИТЕ, ПЪРВА ИНВЕСТИЦИОННА БАНКА БЪЛГАРИЯ (БЪЛГАРИЯ)

Кратко описание:
Тази банка в България има действащ механизъм за откриване и предотвратяване на случаи на телефонни измами. Когато се изтеглят големи суми, които са несъвместими с определен списък от критерии от банката, служителят се предупреждава и подканва да провери дали клиентът е подложен на натиск. Алгоритъм изпраща доклад до служителя, когато тези критерии сочат към възможен случай на телефонна измама. Служителят може след това да провери клиента, съгласно „Списък за проверка на измамите по телефона“, като му задава въпроси например за целта на тегленето или като следи действията му.

#CYBERSCAMS (EC3, EUROPOL)

Кратко описание:
Всяка година през октомври се провежда Европейски месец на кибернетичната сигурност. Това е кампания на ЕС за повишаване на осведомеността, която насърчава кибернетичната сигурност сред гражданите и организациите, като посочва прости стъпки, които могат да бъдат предприети за защита на личните им, финансови и професионални данни. Основната цел е да се повиши информираността, да се промени поведението и да се осигурят ресурси за защита онлайн. Всяка седмица има конкретна тема и през третата седмица на изданието 2018 г. Европейският център за киберпрестъпност, Европейската банкова федерация (EBF) и партньорите от публичния и частния сектор обединиха усилията си, за да представят темата за кибернетичните измами.

7 общи онлайн финансови измами са показани на информационни

бюлетини и е обяснено как да се избегнат. Тези материали бяха разпространени в целия ЕС чрез кампания в социалните медии. След старта за всяка измама беше отделен по един ден.

Начало/продължителност:
Кампанията стартира официално на 17 октомври 2018 г. Материалите ще останат достъпни онлайн.

За повече информация:
https://www.europol.europa.eu/cyberscams

ДОКОЛКО СТЕ ЗАЩИТЕНИ СРЕЩУ ФИШИНГ? (БЕЛГИЯ)

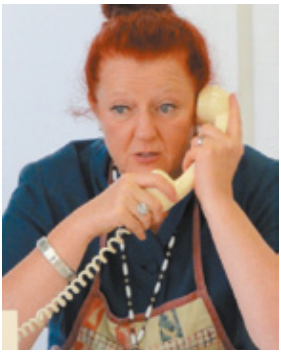
Кратко описание:
Тази кампания бе стартирана от белгийския Център за киберсигурност (CCB) по време на Европейския месец за киберсигурност (ECSM) през 2017 г. Целта на кампанията беше да информира обществеността за фишинг имейли и как да ги разпознаваме. Чрез разпространението на листовки, плакати, както и чрез мащабна кампания в (социални) медии проектът според твърденията е стигнал до около 2 милиона интернет потребители в Белгия.

Освен тази информационна кампания, обществеността беше поканена да изпрати съмнителни писма до CCB. Като се сканират тези електронни писма и се проверяват със сложен софтуер, всеки ден се блокират 5 подозрителни връзки.

Начало/продължителност:
Кампанията стартира официално на 2 октомври 2017 г. Материалите все още са достъпни онлайн и механизмът за препращане все още е активен.

За повече информация:
www.safeonweb.be

NEDÁME SE (НЕ СЕ ПРЕДАВАМЕ) (ЧЕХИЯ)



Кратко описание:
Програмата „Nedáme se" е интерактивна образователна сценична игра, в която се възпроизвеждат четири вида най-чести измамни манипулативни техники, използвани срещу възрастните. Това са рекламни кампании, продажба на парфюми на улицата, телемаркетинг и продажба на домашни любимци. Освен актьорите, полицай и автора на пиесата, на сцената се появява психологът доц. д-р Романа Мазалова. Те влизат в пиесата и си взаимодействат с публиката, като така ги обучават на нови стратегии за защита. Затова пиесата е не само приятна, но и се превръща в нова образователна форма срещу т.нар. „Šmejdi" (шмекери). Експериментално беше проучен възпитателният ефект върху аудиторията. Резултатите потвърдиха, че възрастните, които са видели играта, се оказват по-успешни в защитата срещу измамни продавачи.

Начало/продължителност:
2015 г.
За повече информация:
https://eucpn.org/document/czech-elderly-dont-swallow-bait

ЦЕНАТА НА ПРИЯТЕЛСТВОТО (РУМЪНИЯ)

Кратко описание:
Проектът е насочен към намаляване на риска по-възрастните хора да станат жертви, като се следват тези цели: познаване на нагласата и поведението на целевата

група, повишаване на нивото на превантивни знания на възрастните хора и повишаване на капацитета за самозащита. Целевата група бе съставена от хора над 60 години, които са членове на местни клубове за възрастни. През 2017 г. полицията е провела общо 34 превантивни информационни дейности. Информацията обхваща рисковете, свързани с възрастта, но също така и предотвратяването на виктимизацията в случай на измамни схеми, като например фалшиви телефонни кампании. Бяха проведени и онлайн обучителни курсове за възрастни хора. Освен това беше организиран „бал за безопасност на възрастните“, поставящ началото на публична информационна кампания.

Начало/продължителност:
Януари 2017 г.

За повече информация:
https://eucpn.org/document/price-friendship-project

РЪКОВОДСТВО ЗА БЕЗОПАСНОСТ ЗА ВЪЗРАСТНИТЕ (ФИНЛАНДИЯ)

Кратко описание:
Във Финландия, Финландската асоциация за благосъстояние на възрастните хора има регионални експерти по ремонт на дома, които предлагат на възрастните хора безплатни съвети. Те помагат в ситуации, в които възрастен човек е убеден да поръча скъпо обновяване на дома.

Възрастните хора могат да се свържат с тях относно:

- Измамни продавачи (по телефона, домашни посещения).
- Обновяване и ремонт, свързани с измами (скъпо, ненужно и т.н.)
- Съвети как да действате , ако продавачът окаже натиск за продажба
- Съвети за договори и анулиране в рамките на 2 седмици и др.

„ТРИКОВЕ СРЕЩУ СХЕМИ С ОБАЖДАНИЯ“ (НИДЕРЛАНДИЯ)

Кратко описание:
Организация на възрастни хора в Нидерландия създаде приложение за възрастни хора, което ги учи на опасностите от измами. Приложението симулира „ситуации на измама“, така че възрастните хора могат веднага да проверяват новите си умения. Например, симулира се лотария. Възрастният човек може да даде обичаен отговор, а приложението ще отбележи нивото на убедителност на отговора.

ACTION FRAUD (ВЕЛИКОБРИТАНИЯ)

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Кратко описание:
Action Fraud е националният център за отчитане на измами и киберпрестъпления в Обединеното кралство, в който трябва да съобщите за измама, ако сте били измамени, станали сте жертва на опит за измама или на киберпрестъпление в Англия, Уелс и Северна Ирландия. Те също така насочват жертвите към определени групи за подкрепа, за да помогнат на засегнатите от престъплението, или им предоставят информация към кого трябва да се обърнат.

За повече информация:
https://www.actionfraud.police.uk/

ENDNOTES

1 Потребителите например изпращат симулирани фишинг имейли, за да тестват уязвимостта, в края на теста получават допълнителна информация как да се предотврати това в бъдеще (Sheng, Holbrook, Kumaragur, Cranor, & Downs, 2010)

2 Тук потребителите веднага получават допълнителна информация, когато кликнат върху фалшива връзка (Sheng, Holbrook, Kumaragur, Cranor, & Downs, 2010)

3 Anti-Phishing Phill е добър пример за онлайн игра, която учи потребителите на добри навици, за да им помогне да избегнат фишинг атаки. В края на обучението потребителите са разпознали измамнически уебсайт по-добре от контролната група и са по-добре запознати със стратегиите, които предотвратяват превръщането им в жертви (Sheng, et al., 2007).

4 https://cybersecuritymonth.eu/about-ecsm/whats-ecsm

5 https://www.actionfraud.police.uk/support-and-prevention/ive-been-a-victim-of-fraud

ЦИТИРАНИ ИЗТОЧНИЦИ

Agustina, J. (2015). Understanding Cyber Victimization: Digital Architectures and the Disinhibition Effect. International Journal of Cyber Criminology, 9(1), 35-54.

Anderson, K. (2016). Mass-market consumer fraud: who is most susceptible to becoming a victim? Washington D.C.: FTC Bureau of Economics.

Atkins, B., & Huang, W. (2013). A study of social engineering in online frauds. Open Journal of Social Sciences, 1(3), 23-32.

Barnes, P. (2017). Stock market scams, shell companies, penny shares, boiler rooms and cold calling: the UK experience. International Journal of Law, Crime and Justice, 48, 50-64.

Bidgoli, M., & Grossklags, J. (2017). "Hello. this is the IRS calling": a case study on scams, extortion, impersonation, and phone spoofing. 2017 APWG Symposium on Electronic Crime Research (eCrime) (pp. 57-69). Scottsdale: AZ.

Bullée, J.-W., Montoya, L., Junger, M., & Hartel, P. (2016). Telephone-based social engineering attacks: an experiment testing the success and time decay of an intervention. Singapore Cyber-Security Conference, (pp. 107-114). Singapore.

Bullée, J.-W., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2018). On the anatomy of social engineering attacks: a literature-based dissection of successful attacks. J Investig Psychol offender Profil, 15, 20-45.

Burgard, A., & Schlembach, C. (2013). Frames of Fraud: a qualitative analysis of the structure and process of victimization on the internet. International journal of Cyber Criminology, 7(2), 112-124.

Button, M., & Cross, C. (2017). Cyber frauds, scams and their victims. London: Routledge.

Button, M., Lewis, C., & Tapley, J. (2009). Fraud typologies and the victims of fraud: literature review. National Fraud Authority.

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. Security Journal, 27(1), 36-54.

Button, M., McNaughton, N., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. Australian & New Zealand Journal of Criminology, 47(3), 391-408.

Button, M., Tapley, J., & Lewis, C. (2012). The 'fraud justice network' and the infra-structure of support for individual fraud victims in England and Wales. Criminology and Criminal Justice, 13(1), 37-61.

Cialdini, R. (2001). Influence: Sciende and practice. Boston : Allyn & Bacon.

Cornish, D., & Clarke, R. (2003). Opportunities, precipitators and criminal decisions: a reply to Wortley's critique of situational crime prevention. Crime prevention Studies, 16, 41-96.

Crosman, K. (2017). Phone and Television Scams in the Age of the Internet. Lewis & Clark L.Rev., 21, 791.

Cross, C. (2016). 'I'm anonymous, I'm a voice at the end of the phone': a Canadian case study into the benefits of providing telephone support to fraud victims. Crime Prevention and Community Safety, 18, 228-243.

Cross, C., Richards, K., & Smith, R. (2016). The reporting experiences and support needs of victims of online fraud. Trends & issues in crime and criminal justice, 518, 1-14.

De Kimpe, L., Walrave, M., Hardyns, W., Pauwels, L., & Ponnet, K. (2018). You've got mail! Explaining individual differences in becoming a phishing target. Telematics and Informatics, 35(5), 1277-1287.

EUCPN. (2017). Cyber Safety: A theoretical insight. . In E. Secretariat, EUCPN Theoretical Paper Series. Brussels: European Crime Prevention Network.

EUCPN. (2017). Organised Crime Targeting Elderly People: a theoretical overview. In E. Secretariat, EUCPN Theoretical Paper Series. Brussels: European Crime Prevention Network.

European Commission. (2017). Special Eurobarometer 464a: Europeans' attitudes towards cyber security. Brussels: European Commission.

European Commission. (2018). Special

Eurobarometer 462: E-Communications and Digital Single Market. Brussels: European Commission.

Europol. (2014). Internet organised Crime Threat Assessment. The Hague: Europol.

Europol. (2016). Internet Organised Crime Threat Assessment. The Hague: Europol.

Europol. (2017). Internet Organised Crime Threat Assessment . The Hague: Europol.

Europol. (2018). Internet Organised Crime Threat Assessment. The Hague: Europol.

Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of persuasion in social engineering and their use in phishing. International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 36-47). Cham: Springer.

Gadhave, U., & Sirsat, S. (2015). Review of Cyber-crimes and their impacts over the society. international Journal of Electronics, Communication & Soft Computing Science and Engineering, 357-359.

Harley, D., Grooten, M., Burn, S., & Johnston, C. (2012). My PC has 32,539 errors: how telephone support scams really work. Virus Conference, (pp. 1-8).

Jacques, S., & Bonomo, E. (2017). Learning from the Offenders' perspective on crime prevention. In B. Leclerc, & E. Savona, Crime Prevention in the 21st Century: insightful approaches for crime prevention initiatives (pp. 9-18). Springer.

Jakobsson, M. (2016). Understanding Social Engineering based scams. New York: Springer.

Lab, S. (2010). Crime prevention: approaches, practices and evaluations. LexisNexis Group.

Leukfeldt, E., & Stol, W. (2011). De marktplaats-fraudeur ontmaskerd: Internetfraudeurs vergeleken met klassieke fraudeurs. Secondant, 25(6), 26-31.

Levi, M. (2008). Organized fraud and organizing frauds: Unpacking research on networks and organization. Criminology & Criminal Justice, 8(4), 389-419.

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: overview and issues. Crime, law and social change, 67, 3-20.

Levi, M., & Burrows, J. (2008). Measuring the impact of fraud in the UK. British Journal of Criminology, 48, 293-318.

Maggi, F. (2010). Are the con artists back? A preliminary analysis of modern phone frauds. 10th IEEE International Conference on Computer and Information Technology, (pp. 824-831).

Marzuoli, A., Kingravi, H., Dewey, D., & Pindrop, R. (2016). Uncovering the landscap of fraud and spam in the thelephony channel. 15th IEEE international Conference on Machine Learning and Applications, (pp. 853-858).

Mba, G., Onaolapo, J., Stringhini, G., & Cavallaro, L. (2017). Flipping 419 cybercrime scams: targeting the weak and the vulnerable. International World Wide Web Conference, (pp. 1301-1310). Perth.

Mears, D., Reisig, M., Scaggs, S., & Holtfreter, K. (2016). Efforts to reduce consumer fraud victimization among the elderly: the effect of information access on program awareness and contact. Crime & Delinquency, 62(9), 1235-1259.

Moreno-Fernández, M., Blanco, F., Garaizar, P., & Matute, H. (2017). Fishing for phsihers. Improving internet users' sensitivity to visual deception cues to prevent electronic fraud. Computers in Human Behavior, 69, 421-436.

Murphy, D. R., & Murphy, R. H. (2007). Phishing, Pharming, and Vishing: Fraud in the Internet Age. In T. Fowler, & J. Leigh, The Telecommunications Review (pp. 37-45). VA: Noblis.

Ollmann, G. (2007). The vishing guide. IBM Global Technology Services.

Petty, R., & Cacioppo, J. (1986). The elaboration likelihood model of persuasion. Communication and persuasion, 1-24.

Petty, R., & Cacioppo, J. (2012). Communication and persuasion: Central and peripheral routes to attitude change. Springer Science & Business Media.

Rauti, S., & Leppänen, V. (2017). "You have a potential hacker's infection": a study on technical support scams. IEEE International Conference on Computer and Information Technology, (pp. 197-203).

Ross, M., Grossmann, I., & Schryer, E. (2014). Contrary to psychological opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud. Perspectives on psychological science, 9(4), 427-442.

Rusch, J. (1999). The "social engineering" of internet fraud. Internet Society Annual Conference. Retrieved from http://www. isoc. org/isoc/conferences/inet/99/proceedings/3g/3g_2. htm.

Sheng, S., Holbrook, M., Kumaragur, P., Cranor, L., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. Privacy Behaviors, 373-382.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti,

A., Cranor, L., Hong, J., & Nunge, E. (2007). Anti-Phishing Phil: The Design and Evaluation of a Game that teaches people not to fall for phish. Proceedings of the 3rd symposium on Usable privacy and security (pp. 88-99). ACM.

Singh, L., & Imphal, N. (2018). A survey on phishing and anti-phishing techniques. International Journal of Computer Science Trends and Technology, 6(2), 62-68.

Stajano, F., & Wilson, P. (2011). Understanding scam victims: seven principles for systems security. Communications of the ACM, 54(3), 70-75.

Tabron, J. (2016). Linguistic features of phone scams: a qualitative survey. 11th Annual symposium on information assurance, (pp. 52-58).

Titus, R., & Gover, A. (2001). Personal Fraud: The Victims and the Scams. In F. G., & K. Pease, Repeat Victimization (pp. 133-152). New York: Criminal Justice Press.

van de Weijer, S., Leukfeldt, R., & Bernasco, W. (2018). Determinants of reporting cybercrime: a comparison between identity theft, consumer fraud, and hacking. European Journal of Criminology, 1-23.

Whitty, M. (2013). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. British Journal of Criminology, 53(4), 665-684.

Whitty, M. (2015). Anatomy of the online dating romance scam. Security Journal, 28(4), 443-455.

Whitty, M. (2018). Do you love me? Psychological characteristics of romance scam victims. Cyberpsychology, behavior, and social networking, 21(2), 105-109.

Wood, S., Liu, P., Hanoch, Y., Xi, P., & Klapatch, L. (2018). Call to claim your prize: perceived benefits and risk drive intention to comply in a mass marketing scam. Journal of Experimental Psychology: applied, 24(2), 196-206.

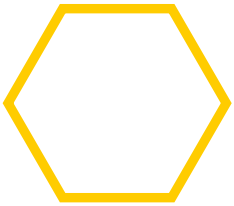
Wood, S., Liu, P., Hanoch, Y., Xi, P., & Klapatch, L. (2018). Call to claim your prize: perceived benefits and risk drive intention to comply in a mass masketing scam. Journal of Experimental Psychology: Aplied, 24(2), 196-206.

Workman, M. (2008). Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security. Journal of the american society for information science and technology, 59(4), 1-12.

Yeboah-Boateng, E., & Amanor, P. (2014). Phishing, SMishing & Vishing: an assessment of threats against mobile devices. Journal of Emerging Trends in Computing and Information Sciences, 5(4), 297-307.

Секретариат на ЕМПП

Waterloolaan / Bd. De Waterloo
76, 1000 Брюксел, Белгия
Телефон: +32 2 557 33 30
eucpn@ibz.eu
www.eucpn.org



TWITTER.COM/EUCPN
FACEBOOK.COM/EUCPN
LINKEDIN.COM/COMPANY/EUCPN