ПРОЕКТ
ДИГИТАЛЕН ДОСТЪП
(*DIGITAL ACCESS PROJECT*)

УЧЕБЕН МОДУЛ
Напреднали онлайн знания за безопасност

Изготвено от: CIC

Септември 2018

Този проект е финансиран с подкрепата на Европейската комисия. Тази публикация и цялото ѝ съдържание отразяват само възгледите на автора и Комисията не носи отговорност за каквото и да е използване на съдържащата се в нея информация.

СЪДЪРЖАНИЕ

УЧЕБНИ ЧАСОВЕ: [ВСИЧКИ УЧЕБНИ ЧАСОВЕ]
УЧЕБНО НАТОВАРВАНЕ: [УЧЕБНИТЕ ЧАСОВЕ НА ВСИЧКИ МОДУЛИ + ВРЕМЕТО ЗА УПРАЖНЕНИЯТА]

РЕЗЮМЕ

Този модул е предназначен да разшири знанията на потребителя за онлайн престъпни дейности в интернет пространството. Основните цели на раздела е да се даде възможност на потребителя да се предпази от киберпрестъпници и да запази личната информация в безопасност, гарантираща, че онлайн данните са защитени

КЛЮЧОВИ ДУМИ

Фишинг, измама, интернет измами, киберпрестъпления, кибертормоз, измамници.

ЦЕЛИ НА МОДУЛА

Дейности / Постижения		
Разбиране за интернет базирани престъпни дейности, насочени към финансова злоупотреба и умения за идентифициране и избягване на тези дейности.		
Знания	**Умения**	**Компетентности**
Фишинг/Измама	Разбиране на фишинга идентифициране на истински имейли от злонамерени идентифициране на истински SMS-и от злонамерени	Доверие в оценката на цифровата комуникация, която изглежда официална и взема информирано сигурно действие
Интернет измами	Разбиране на измами в интернет Разпознаване на някои общи измами Действия, които трябва да се предприемат, за да защитите себе си	Идентифициране на общи измами и практики и разбиране на основната защита.

Киберпреследване	Идентифициране на киберпреследването Стратегии за справяне Защита от киберпреслед ване	Identifying and dealing with cyberstalking and the avenues to report it.
Кибертормоз	Идентифициране на кибертормоза Стратегии за справяне Защита от киберпреслед ване	Идентифициране и справяне с кибертормоза и пътищата за докладване.

РАЗДЕЛ 1: Фишинг

Резултат

Разбирането на фишинга и възможността за идентифициране на реална електронна поща/SMS комуникация от злонамерени такива

Фишинг измами

Фишинг измамите се основават на комуникацията, направена чрез имейл или в социалните мрежи. В много от случаите кибер престъпниците изпращат на потребителите съобщения/ имейли, като се опитват да ги мамят, като им предоставят ценни и чувствителни данни (идентификационни данни за влизане от банкова сметка, социална мрежа, служебен акаунт, облачна услуга и т.н.), които могат да се окажат ценни за тях.

Освен това тези имейли изглеждат за получателя, че са пристигнали от официални източници (като банкови институции или други финансови органи, законни компании или представители на социалните мрежи).

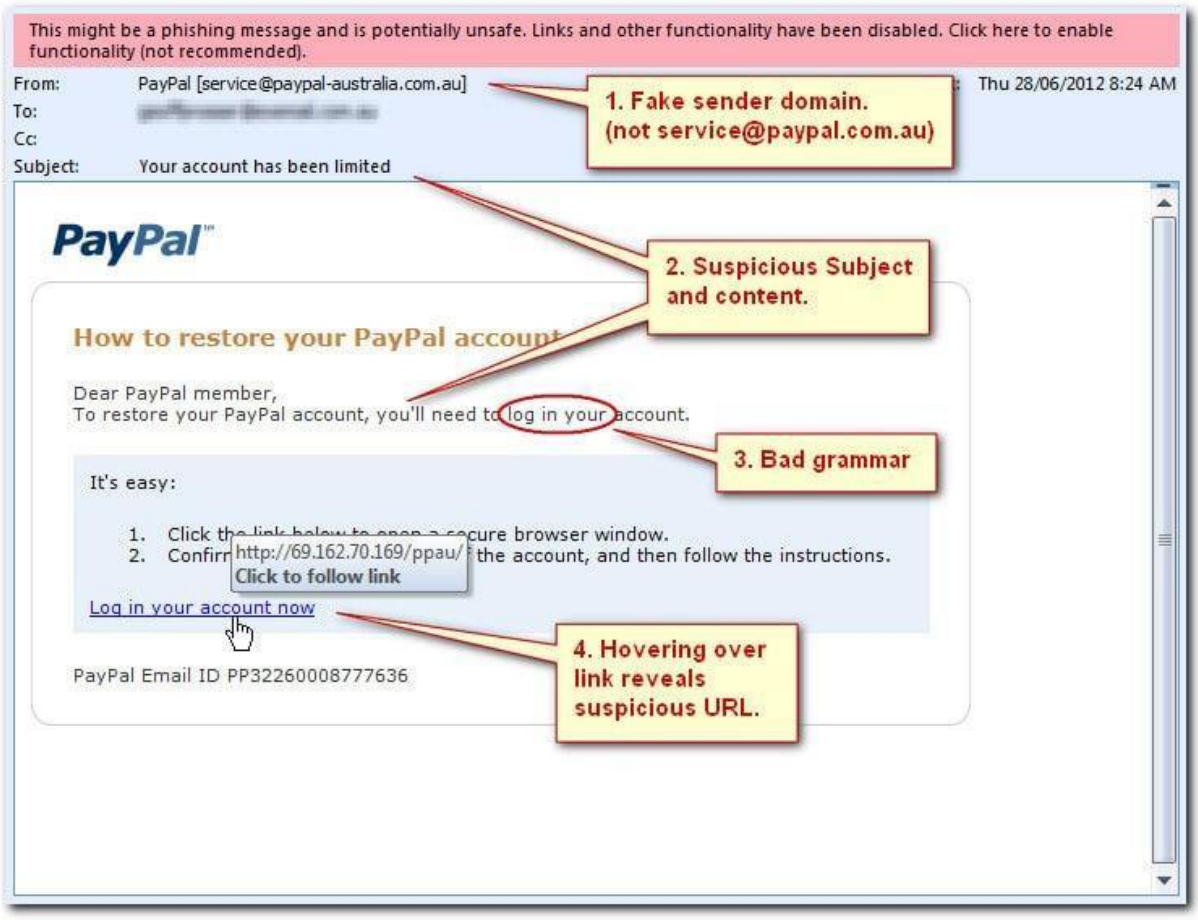
По този начин те ще използват техники за социално инженерство, като ви убедят да кликнете върху съответната злонамерена връзка и да получите достъп до уебсайт, който изглежда легитимен, но всъщност е контролиран от тях. Вие ще бъдете пренасочен към фалшива страница за достъп до интернет, който прилича на реалния сайт. Ако не внимавате, може да дадете идентификационните си данни за влизане и друга лична информация.

Виждали сме много спам кампании за електронна поща, в които фишинга е основния вектор на атаки за злонамерени престъпни действия от страна на хора, използвани за разпространение на финансови данни за кражба на зловреден софтуер.

За да растат успехите им, измамниците създават чувство за неотложност. Ще ви разкажат страшна история за заплахата на банковата ви сметка и как най-бързо трябва да получите достъп до сайт, на който трябва да въведете идентификационните си данни, за да потвърдите самоличността си или профила си.

След като попълните данните си за онлайн банкиране, киберпрестъпниците ги използват, за да получат достъп до реалната ви банкова сметка или да търгуват с данните ви с други заинтересовани страни

По-долу е даден пример за фишинг имейл



Идентифициране на фишинг измами

Не се доверявайте на показваното име

Любима тактика за фишинг сред киберпрестъпниците е да се подлъгва името на имейла. Ето как работи: Ако измамник иска да измисли хипотетичната марка „Моята банка“, имейлът може да изглежда по следния начин:

Този измамен имейл изглежда легитимен, тъй като потребителите обръщат предимно внимание на изписаното име. Не се доверявайте лесно, проверявайте имейл адреса – цялото му име и ако ви изглежда подозрителен, не го отваряйте.

Гледайте, но не кликвайте.

Задръжте курсора на мишката върху всички връзки, вградени в тялото на имейла. Ако

адресът на връзката изглежда странно, не кликвайте върху него. Ако искате да тествате връзката, отворете нов прозорец и въведете адреса на уебсайта директно, вместо да щраквате върху линка от нежелани имейли.

Проверете за правописни грешки.
Легитимните имейли обикновено нямат сериозни правописни грешки или лоша граматика. Четете имейлите си внимателно.

Анализирайте поздрава, който насочен към вас. Имейл, адресиран до неперсонализиран „Редовен клиент“може да е опасен, затова внимавайте. Истинските компании често използват личен поздрав с вашето име и фамилия.

Не предоставяйте лични данни.
Легитимните банки и повечето компании никога не биха ви поискали личните ви данни по имейл. Не пренебрегвайте тяхната политика за сигурност.

Бъдете предпазливи, ако попаднете на заплашителен тон в полето „относно“ на вашата поща.
Позоваването на чувство за спешност или страх е често срещана фишинг тактика. Пазете се също от такива, които твърдят, че вашият акаунт е бил спрян или е имало опит за влизане в профилът ви, който е бил неуспешен.

Прегледайте подписа.
Липсата на подробности за подателя или как можете да се свържете със съответната компания силно предполага, че е фишинг. Законните бизнеси винаги предоставят координати за обратна връзка.

Не отваряйте прикачени файлове.
Злонамерени прикачени файлове, които съдържат вируси и злонамерен софтуер е обща фишинг тактика. Те могат да повредят файловете на вашия компютър, да откраднат паролите ви и да ви шпионират без ваше знание. Не отваряйте прикачени файлове и имейли, които не очаквате.
Не се доверявайте на името на имейл адреса.
Измамниците използват автентични имена на имейла, които да ви накарат да се доверите и да го отворите.

Не вярвайте на всичко, което виждате.
Фишерите са много добри в измамите. Само защото имейла изглежда достоверен и убедителен, не означава, че е легитимен. Бъдете мнителни, когато получавате имейл, и ако имате дори най-малкото подозрение, не го отваряйте.

Фишинг измами – SMS измами и как да ги идентифицирате.

Това са съобщения, изпратени от хора, известни като „скамери“, които мамят хората, за това, че съобщенията които изпращат са действителни. Тези съобщения обикновено започват с „Поздравления“ и продължават с това, че сте спечелили 150 000 от позната компания, за да ви грабне вниманието и да ви подтикне бързо да им отговорите.

Какви са характерните им черти?

- Съобщението започва с поздравление,
- Съобщението може също да включва следното, напр. *"Вие сте избран за печелившия номер 3 ..."*
- Споменава се и име на някоя фирма
- Ще бъдете помолен да се свържете с някой

Какво да правите като получите такъв СМС

- Прочетете внимателно съобщението без много да се вълнувате;
- Никога не се обаждайте на тези мобилни номера;
- Никога не разкривайте банковите си данни на тез измамници;
- Ако получите обаждане в което ви препоръчват да предоставите банковите си сметки на тези хора, не давайте тази информация и прекратете обаждането.
- Незабавно се свържете с вашата банка и ги информирайте!

Пример на фалшив SMS

Неща, които една компания никога няма да поиска

Изброени са осем неща, които измамниците биха ви помолили да направите по имейл, SMS или директно обаждане и което никога не би поискала една законна институция, банка или компания.

- Да ви изпратят имейл или да ви се обадят, за да поискат вашия ПИН код или банкови данни
- Да изпрати човек до вашият дом, за да събере пари, банкови карти или друго
- Да ви помоли да оторизирате прехвърляне на средства към друга сметка
- Да поиска от вас да направите „тестова“ онлайн транзакция
- Да изпрати имейл с линк към уебсайт, който да ви подкани да въведете данните си за онлайн банкиране
- Да ви поискат лична банкова информация
- Да ви предоставят банкови услуги чрез някое мобилно приложение, по-различно официалното приложение на банката
- Да ви предлагат по телефона различни скъпоструващи стоки (диаманти, земя и т.н.)

Като обобщение, което може да се направи- изрийте съобщенията, които са опити за фишинг.

РАЗДЕЛ 2: Интернет измами

Резултат

Какво представляват измамите по имейл

Идентифициране на често срещани измами и практики с разбиране на основната защита.

В онлайн пространството терминът, който се използва за такава измама се нарича скам (scam). По дефиниция скам е бързо-профилна схема в която човек мами друг индивид или група, за да изкара пари, като предоставя фалшива информация по време на предлагане на сделка или оферта.

Има много различни видове скамове, които разчитат на нищо не подозиращите жертви. Скамерите атакуват жертвите си по имейл, със SMS- и дори и с телефонни обаждания.

Често срещани скамове

Неочаквани награди

Скамовете с неочаквани награди включват лотарийни печалби или почивки и ваканции. Тези скамове могат да бъдат получени онлайн, по телефон или по имейл. Те ви информират за това, че сте спечелили награда (голяма сума пари, ваучери за пазаруване, безплатна ваканция или туристически продукт) и изисква от вас да изпратите пари или лична информация.

Неочаквани пари

Това включва и измамите с наследство , „Нигерийски“ скам, възстановяване на пари и авансови плащания и други усъвършенствани измами с финансови средства.
Такива скамове искат от вас следното:

- Предварително да изпратите пари за продукт или награда
- Да предоставите лични данни за разплащане, такси за адвокати, за да предявите иск за наследство или голяма сума пари от далечен роднина в чужбина
- Прехвърляне на пари от нечие име с обещанието да получите пари

Пример за Нигерийки скам

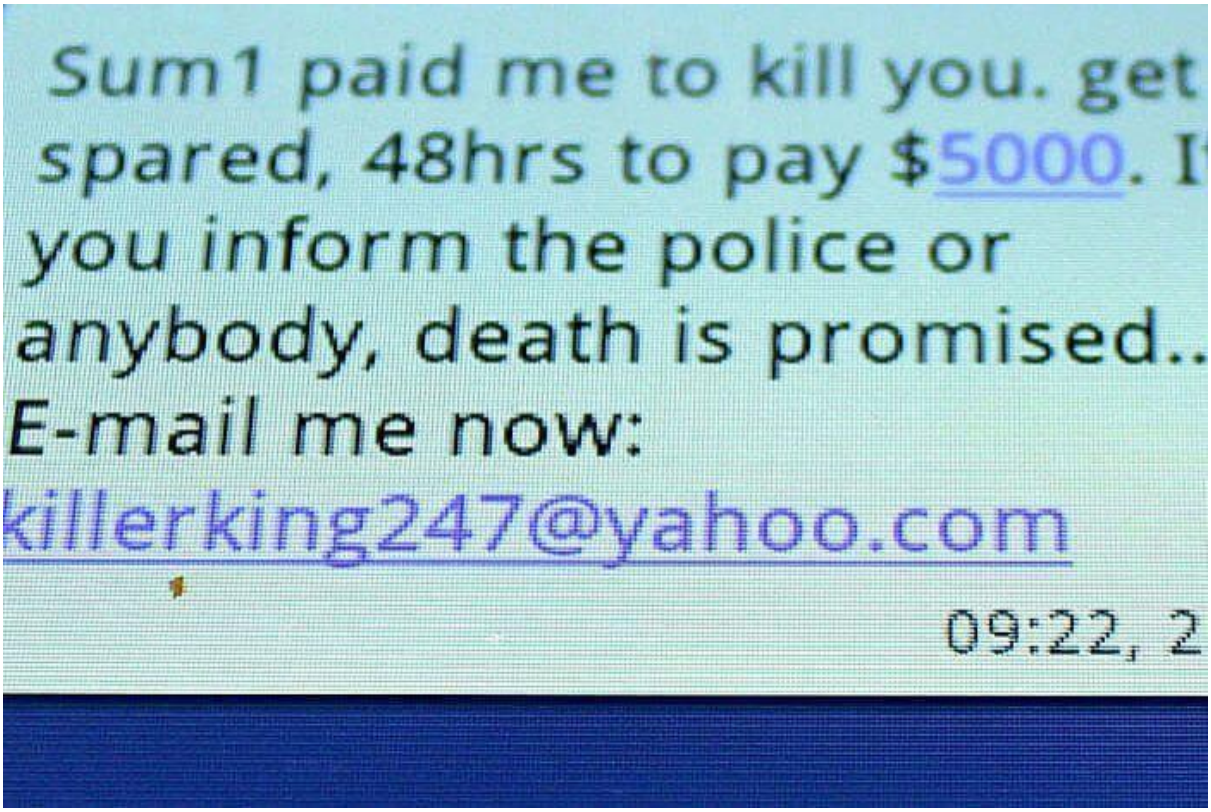
Запознанства и романтични скамове

Този вид измами са убедителни, тъй като на прицел са романтичната, състрадателна и наивна страна. Те действат на емоционално ниво, за да ви накарат да предоставите пари, подаръци или лични данни.

Заплашителни и изнудващи скамове

Този вид включва различни измами със злонамерен софтуер наречени „ransomware" "malware". Те могат сериозно да навредят на вашия компютър, като достигнат до него. Това означава трети лица да получат достъп до вашата лична информация, което може да доведе до загуба на данни, както и да попречи на достъпа ви до вашите програми и файлове. След това измамниците могат да наредят плащане без вие да имате изобщо достъп до вашия компютър.

„Наемни убийци" са скамове, които изпращат смъртоносни заплахи на случаен принцип чрез SMS или имейл от „наемен убиец". Съобщението съдържа заплаха за убийство, ако не му се изпратят пари.



Измами свързани с предлагане на работа и инвестиции

Тези скамове са насочени към хора, които си търсят работа или искат да работят от вкъщи. Често те обещават големи доходи за малко работа, но искат предварително плащане преди да започнете работа.

Инвестиционните скамве включват скамер измамници, които се свързват с вас чрез нежелани телефонни обаждания или имейли с предложения за инвестиции в доходоносни схеми, които ще осигурят атрактивна възвръщаемост. В много случаи измамниците използват усъвършенствани и оригинални уебсайтове, за да убедят потребителите, че техните оферти са легитимни.

Фалшиви антивирусни програми

Всички сте виждали поне веднъж такова съобщение на екраните си:"Вие сте били заразени! Изтеглете антивирусната програма X още сега, за да защитите вашия компютър. Няма по-невинна измама от нежеланите изкачващи прозорци на екрана докато сърфирате в интернет. В този случай, за да се отървете от досадните прозорци, ви препоръчваме да сканирате вашата система с помощта на добър антивирусен продукт.

Фалшива антивирусна програма за Windows

За да проверите сигурността си, ако прозорецът на секцията за антивирус свети зелено и пише "ON" програмата е легитимна. Но ако свети в червено и пише "OFF," възможно е софтуерът да е фалшив.

Както се вижда на картинката, те могат да изглеждат автентично и убедително.

Ако имате нужда от антивирусни програми, може да се доверите на следните сайтове.

Avira Antivirus

Avast Free Antivirus

AVG Free Antivirus

Биткойн измами

Дигиталните портфейли могат да бъдат отворени за хакерски атаки и измами, с цел да се възползват от тази нова технология, за да крадат чувствителни данни.

Най-честите онлайн измами, за които да внимавате:

- Фалшиви Биткойн борси
- Понци схеми
- Всекидневни опити за скам
- Злонамерен софтуер

Измами с биткойни

Ето как да залавяте Bitcoin скам и да останете в безопасност онлайн.

Фалшиви новини

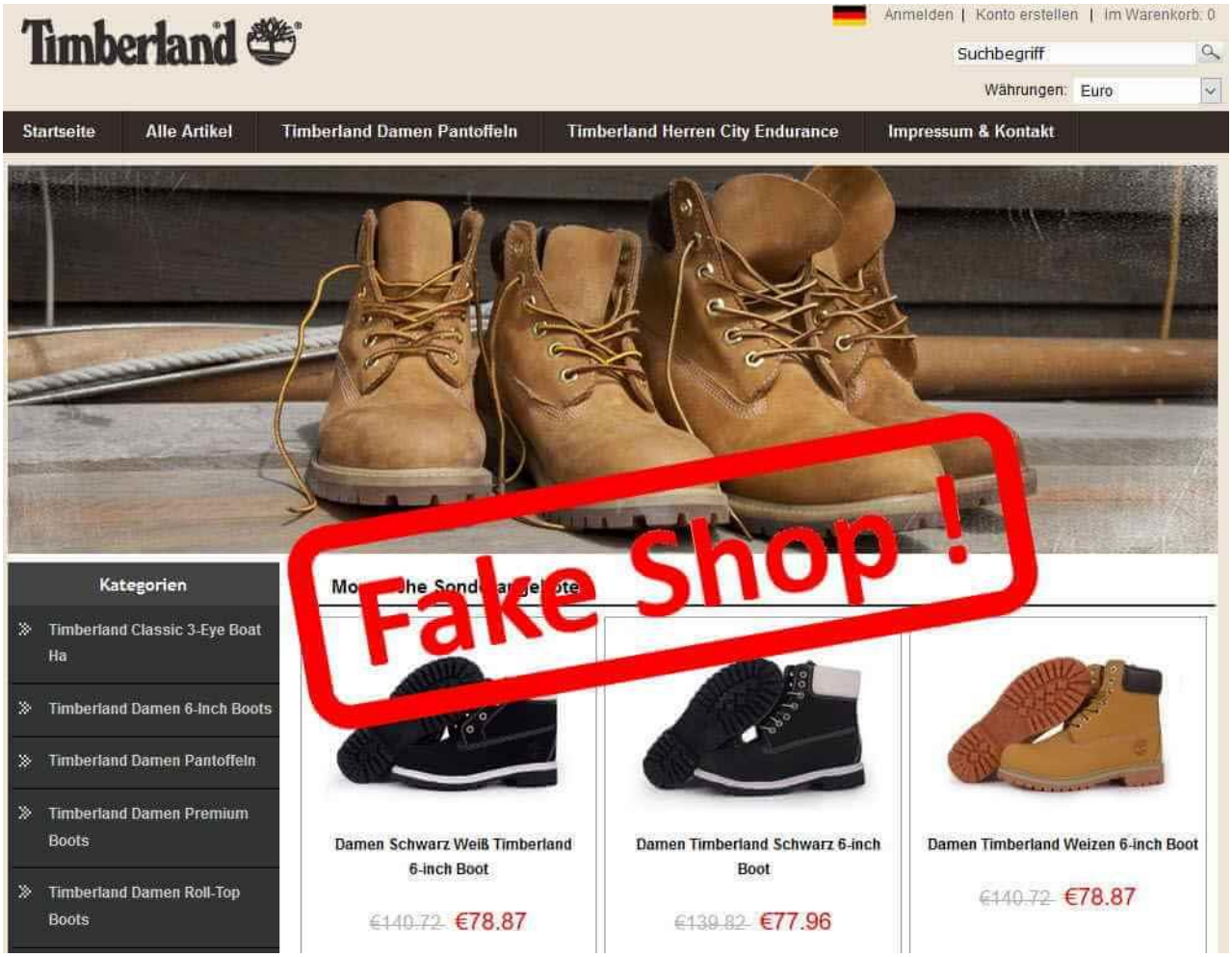
Разпространението на фалшивите новини по Интернет е опасно за всички нас, тъй като има сериозно въздействие у хората и на начина по който филтрираме тази информация, на която сме попаднали в социалните медии. Това е сериозен проблем, който трябва да засяга нашето общество, най-вече заради заблуждаващите ресурси и съдържание, намерени онлайн, което прави невъзможно хората да правят разлика между това, което е реално и кое не.

Препоръчваме ви достъп / четене само на надеждни източници на информация, идващи от приятели или хора, които знаете, че четат редовни емисии от надеждни източници: блогъри, експерти, за да се избегнат фалшиви новини.

Фалшиви онлайн магазини

Ние всички обичаме пазаруването и е по-лесно и по-удобно да го правите в интернет с няколко кликвания. Но за вашата онлайн безопасност бъдете предпазливи относно посещаваните от вас сайтове. Има хиляди уебсайтове, които предоставят невярна информация и могат да ви пренасочат към злонамерени връзки, което дава на хакерите достъп до най-ценните ви данни.

Ако забележите чудесна онлайн оферта, която е „прекалено добра, за да е истина“, може да се изкушите да пазарувате, но трябва да научите как да откриете фалшивите сайтове за пазаруване, така че да не бъдете измамени. Сайтове, като този, който е показан по-долу могат да бъдат много убедителни.

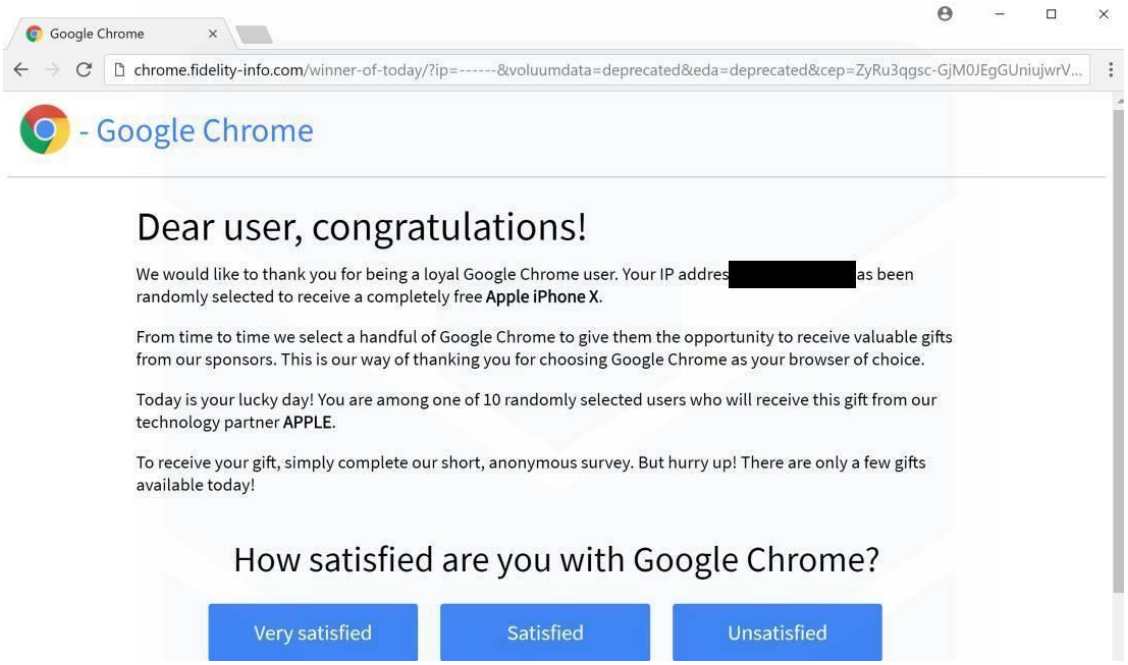


Фишинг измама с лоялни клиенти

Много уебсайтове имат програми за лоялни клиенти, за да се отблагодаряват на клиентите си за направените покупки, като им предлагат точки или купони. Това е предпоставка за друг вид измама от която хакери могат да откраднат чувствителна информация, свързана с вас. Ако смятате, че никой не би имал нужда от тази информация, помислете отново.

Това е много често срещана измама, която изглежда като истински имейл, идващ от програма за лоялни клиенти, но не е така. Злонамерените хакери са навсякъде и е достатъчно едно кликване, за да бъдат инсталирани злонамерен софтуер на вашия компютър и хакерите да получат достъп до вашите лични данни.
Ако ви е трудно да ги засечете тези скамове, ще ви бъде полезен този пример на текуща фишинг кампания насочена към притежателите на карти за разплащане, както и до някои полезни съвети и трикове.

Пример на подобна измама:



Основна защита

Точни копия. Измамниците често се преструват на някой, на когото вярвате, като правителство длъжностно лице, член на семейството, благотворителност или компания, с която правите бизнес. Не изпращайте пари или лична информация в отговор на неочаквано писмо или обаждане – независимо дали става дума за текст, телефонно обаждане или имейл.

Правете справка онлайн. Напишете името на продукта в търсачката, която използвате и добавете „мнения“, „оплакване“ или „измама“. Или потърсете фраза, която описва вашата ситуация. Дори може да потърсите телефонния номер, за да видите дали и други хора са докладвали такъв скам.

Не вярвайте на самоличността на този, който ви звъни или пише. Технологията позволява да се фалшифицира информация, така че името и номерът, които виждате, не винаги са реални. Ако някой се обади да поиска пари или лична информация, затворете. Ако мислите, че този човек може да казва истината, обадете се на номер, който знаете, че е истински.

Не плащайте предварително, заради дадено обещание. Ако някой ви поиска пари за каквото и да било, дори и за да си получите наградата която сте спечелили, най-вероятно става въпрос за измама, на която искат да ви вземат парите след което да изчезнат.

Обмислете начина на плащане. Кредитните карти имат значителна защита, но други методи на плащане нямат. Ако парите ви преминават през Уестърн Юниън или МъниГрам е рисковано, тъй като е почти невъзможно да си получите обратно парите. Това също важи за презареждащите се карти (като Мънипак или Рилоудит) и карти подарък (като iTunes или Google Play). Правителствените офиси и частните компании няма да изискват от вас да използвате тези начини на плащане.

Разговаряйте с някого. Преди да предоставите парите си или личната си информация, говорете с някого на когото може да се доверите. Измамниците обикновено искат от вас бързо да вземете решение. Дори може да ви заплашат. Не бързайте, направете си справка онлайн, обмислете хубаво ситуацията, консултирайте се с някой експерт или просто споделете с приятел.

Затваряйте телефона. Ако вдигнете и насреща чуете запис, който иска нещо да ви продаде или предложи, просто затворете. Тези обаждания са нелегални, а продуктите са фалшиви. Не натискайте 1, за да говорите с човек или да бъдете изключени от списъка. Това може да доведе до още повече обаждания.

Бъдете подозрителни към предлаганите безплатни оферти. Някои компании примамват с безплатни неща, за да ви накарат да се абонирате за продукти и да ви фактурират всеки месец, докато не анулирате. Преди да се съгласите с безплатния пробен период, проучете компанията и прочетете правилата за анулиране. И винаги преглеждайте месечните си извлечения за да видите дали не са ви таксували нещо допълнително.

Не депозирайте чекове, тъй като ако се окажете обект на измама, банката ще изисква сумата си от вас, след като насрещният е нелегален.

Раздел 3: Преследване в киберпространството

Резултат

Идентифициране и справяне с киберпрестъпленията и възможностите за докладване.

Преследване

Кибер преследването е престъпление, при което преследвачът тормози жертва чрез електронна комуникация, като електронна поща или съобщения публикувани на уеб сайт или дискусионна група. Един кибер преследвач разчита на анонимността, предоставена от Интернет, за да им позволи да преследват жертвата си, без да бъдат открити. Съобщенията за кибер преследването се различава от обикновения спам в това, че кибер съобщението е насочено към конкретна жертва с често заплашващи съобщения, докато спамърът насочва множество получатели с досадни съобщения.

Някои примери:

- Изпращане на манипулативни, заплашителни, неприлични или тормозещи имейли от различни имейл акаунти.
- Хакване на онлайн сметките на жертвата (като например банкови или електронни съобщения) и промяна на настройките и паролите на жертвата.
- Създаване на фалшиви онлайн профили в социални мрежи и сайтове за запознанства, представяне на жертвата или опит за установяване на контакт с жертвата чрез използване на фалшиво лице.
- Публикуване на съобщения в онлайн бюлетини и дискусионни групи с личната информация на жертвата, като домашен адрес, телефонен номер или номер за социално осигуряване. Публикациите също могат да бъдат неприлични или противоречиви - и жертвата получава многобройни имейли, обаждания или посещения от хора, които четат публикацията онлайн.
- Регистриране на множество пощи и услуги, като се използва името и имейл адреса на жертвата.

Киберпрестъпленията са трудни за хващане, тъй като преследвачът може да бъде в друга държава или далече от жертвата. В анонимния свят на интернет е трудно да се провери самоличността на преследвача, да се съберат необходимите доказателства за арест или да се стигне физически до него.

Ако сте жертва на киберпрестъпления, опитайте се да съберете възможно най-много физически доказателства и да документирате всеки контакт.
Има редица прости начини да се предпазите от кибер престъпленията. Една от най-полезните предпазни мерки е да останете анонимни. Използвайте основния си имейл адрес само за комуникация с хора, на които имате доверие, и създайте анонимен имейл за

всички други комуникации. Задайте опциите за филтриране на програмата за електронна поща, за да предотвратите нежелана комуникация. Когато избирате онлайн име, направете го различно от вашето име и неутрално по пол. Не поставяйте идентификационни данни в онлайн профилите.

Ако станете жертва на киберпреследвач, най-ефективният начин на действие е да съобщите за нарушителя на техния интернет доставчик. Ако това е невъзможно или неефективно, най-добре е да промените собствения си доставчик и всичките си онлайн имена.
Според статистиката 80% от случаите са били решени с тези методи.

РАЗДЕЛ 4: Кибер тормоз

Резултат

Подпомагане на потребителя да идентифицира, да се справи и да докладва в случай на кибертормоз.

Какво е кибер тормоз

Кибертормозът е тормоз, който се извършва чрез цифрови устройства като мобилни телефони, компютри и таблети. Кибертормоза може да възникне чрез SMS, текст и приложения или онлайн в социални медии, форуми или игри, където хората могат да преглеждат, участват или споделят съдържание. Кибертормоза включва изпращане, публикуване или споделяне на отрицателно, вредно или фалшиво съдържание за някой друг. Това може да включва и споделяне на лична информация с цел да го унижи. Някои видове кибертормоз престъпват линията на закона.

Най-често срещаните места, където се извършва кибертормоз, са:

- Социалната медия, като Facebook, Instagram, Snapchat, и Twitter
- Съобщения
- Незабавни съобщения
- Имейли

Как да се справим с кибер тормоза

Никога не отговаряйте

Не отговаряйте на нищо от казаното с цел отмъщение. Да кажете нещо лошо или да публикувате нещо унизително, за да си отмъстите, може да влоши нещата или дори да ви създаде неприятности.

Скрийншот

Ако можете направете скрийншот на това, което смятате, че може да е киберторзмоз и запазете копие на компютъра си.

Блокирайте и докладвайте

Повечето онлайн платформи имат тази функция, уверете се, че блокирате и съобщавате за нарушителите на подходящата социална медийна платформа.

Говорете за това.

Може към момента да не ви засяга особено, но кибертормозът ви засяга по най-различни начини. Не сте сам. Говорете с някого за това. Това не само ще ви помогне много, но и ще ви успокои.

Колко е сериозно?

Оценете сериозността на ситуацията. Ако ви търсят или искат да ви добавят хора, които не познавате, най-добре за вас е да ги изтриете или блокирате.

Докладвайте.

Ако сте жертва на кибертормоз от някого, с когото посещавате училище или колеж, съобщите го на учителя. Ако някой ви заплашва, дава ви лична информация или ви кара да се страхувате за вашата безопасност, свържете се с полицията или с възрастен, веднага щом можете.

Поверителност.

Препоръчваме ви да пазите вашата поверителност на високо ниво и да не се свързвате с някого, когото не познавате или не сте виждали никога в реалния живот. След като няма да разговаряте с непознати хора на улицата, защо да го правите онлайн? Хората не винаги са това, което казват, че са и може да изложите себе си и близките си на риск.

Съчувствайте им.

Помнете винаги, че щастливият човек не би преследвал и тормозил останалите. Тези които го правят преминават през труден момент или са объркани и често се нуждаят от помощ.

Кибертормозът не е особено характерен за възрастните, но може да се използва за изнудване за пари, лични данни и други криминални престъпления.

УПРАЖНЕНИЯ

Упражнение 1: PayPal – Реално идентифициране на кибер измами

Ако получите такова съобщение на пощата си, какво ще предприемете като действие?

Упражнение 2: Измама с банкови данни

1. Какво не трябва да правите, ако получите такъв имейл?
2. Как да проверите автентичността на пощата?

Упражнение 3: СМС фишинг за банкови измами

1. Защо този СМС изглежда съмнително?

Упражнение 4: Онлайн викторина – открийте скам

Направете този тест, за да си видите

резултатите.

https://www.protectseniorsonline.com/quiz/

ДОПЪЛНИТЕЛНА ЛИТЕРАТУРА И РЕСУРСИ

Условия, които трябва да знаете

https://www.lifewire.com/top-internet-terms-for-beginners-2483381

Планиране на интернет безопасността за възрастни (PDF)

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=18&cad=rja&uact=8&ved=2ahUKEwiz8LGAjNjdAhVSGsAKHbISB8QQFjAReqQIBxAC&url=https%3A%2F%2Fvictimserviceslanark.ca%2Fphotos%2Fcustom%2FVSLG%2FResources%2FSafetyPlanningForSeniors_English.pdf&usg=AOvVaw3WNu9papw-5PbHbhKSxVFi

Топ съвети за безопасност в интернет (PDF)

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=12&ved=2ahUKEwiz8LGAjNjdAhVSGsAKHbISB8QQFjALegQIBRAC&url=https%3A%2F%2Fquery.prod.cms.rt.microsoft.com%2Fcms%2Fapi%2Fam%2Fbinary%2FRE1ImTu&usg=AOvVaw0QyXRMv5RLg-kAS0tIaUvz

Обяснението за фишинг – Youtube видео

https://www.youtube.com/watch?v=9TRR6lHviQc

Чудесен сайт с повече информация за фишинга

http://www.phishing.org/

Актуализиран списък на всички основни онлайн измами

https://www.thebalancecareers.com/top-internet-scams-a-z-list-2062169

Защита на вашите данни

https://youtu.be/BL7WJM342Uc

Повече информация за скам измамите

https://www.scamwatch.gov.au/get-help/protect-yourself-from-scams

Онлайн безопасност за възрастни хора

https://www.connectsafely.org/seniors/

Повече информация за онлайн

безопасността

https://www.protectseniorsonline.com/resources/

БИБЛИОГРАФИЯ

Съвети за това как да идентифицирате фишинг или фалшив имейл

https://blog.returnpath.com/10-tips-on-how-to-identify-a-phishing-or-spoofing-email-v2

Топ онлайн измами трябва, които да избягвате

https://heimdalsecurity.com

СМС измами и как да ги идентифицираме

https://support-pg.digicelgroup.com

Осем неща, които банката ви никога няма да ви поиска, за разлика от измамника

https://www.telegraph.co.u

Онлайн скам измами

https://www.acorn.gov.au/learn-about-cybercrime

10 неща, които да направите, за да избегнете измама

https://www.consumer.ftc.gov

Киберпреследване

https://searchsecurity.techtarget.com

Онлайн тормоз и киберпрестъпления

https://www.privacyrights.org/consumer-guides/online-harassment-cyberstalking

РЕШАВАНЕ НА
УПРАЖНЕНИЯТА

Упражнение 1

Първоначалната ви реакция може би ще си помислите, че това не сте го купували и ще кликнете, за да видите продукта. По този начин ще активирате вирус или връзка към фалшив сайт.
Погледнете името и ако не го разпознавате, трябва да ви светне червена лампичка.

Задръжте курсора върху връзката на продуктите, за да видите дали правилно е изписан URL адреса на Ebay.

Задръжте курсора над линка PayPal, за да видите дали сочи към правилния URL адрес.
Ако не отговаря на тези изисквания, изтрийте имейла.

Ако случайно сте закупили продукт и използвате Paypal отидете на сайта на PayPal от вашия собствен браузър и проверете историята на транзакциите си. Не използвайте линкове в имейла.

If you still have concerns, contact Paypal and talk to them directly.

Упражнение 2: Барклис

Погледнете имейл адреса, първото име изписано в полето е правилно, но второто буди подозрение.

Задръжте курсора на мишката върху връзката за възстановяване, без да кликвате на нея. Проверката на URL адреса води към неразпознат сайт.

Ако имате притеснения уведомете банката и изтрийте имейла.

Упражнение 2: СМС скам

Банка никога не би изпратила СМС с линкове.

Линковете изглеждат подозрително, не ги отваряйте. Помнете, че телефонът ви е като компътър и изпълнява същите действия.

Обадете се на банката и говорете с тях.

Изтрийте СМСа и говорете с приятел.