

Въведение

Живеем в свят, който е все по-свързан, където чатенето, пазаруването, продаването или срещата с нови хора е само на едно кликане разстояние. Но не всичко е розово: интернетът крие много рискове и измамници, готови да ни подведат. Това ръководство е предназначено за вас, млади хора, които ежедневно използвате телефони, социални мрежи или пазарувате онлайн. То ще ви помогне да разпознавате най-честите измами, като тези на фалшиви търговски сайтове, романтични капани, фалшиви банкови съобщения или криптовалути измами. Просто, директно и с реални примери, това ръководство ще ви научи как да се защитите, кога да бъдете подозрителни и какво да направите, ако се чувствате застрашени. Защото безопасното сърфиране е първата истинска защита. И помнете: дори едно кликане може да направи разлика.

Слайд 1 – Електронна търговия (E-Commerce)

Това е най-разпространената онлайн измама и засяга както купувачите, така и продавачите. Най-често срещаните форми са:

1. Фалшиви търговски сайтове

- Сайтове, които изглеждат реални, с продукти на много изгодни цени.
- След плащане по банков път или с карта, стоката не пристига.
- Продавачът изчезва, а контактите са фалшиви или не съществуват.
- Понякога получавате пратка с наложен платеж, плащате при доставка, но вътре има предмети с малка стойност.

2. Фалшиви обяви в портали като Subito, eBay, Facebook Marketplace или Instagram

- Измамникът публикува фалшива обява.
- Започва преговор чрез WhatsApp, понякога изпращайки (фалшиви) документи.
- Искането за плащане е чрез банков превод или презплатена карта.
- След като получи парите, измамникът изчезва.

3. Фалшиви купувачи

Ако вие продавате:

- Получавате съобщения от предполагаеми купувачи от чужбина, които измислят разходи, които трябва да бъдат платени предварително.
- Или ви молят да отидете на пощата, за да „получите“ парите, но всъщност трябва да заредите пари в тяхна полза (измама с пощенски терминал).

Слайд 2 – Как да се защитите от измами при онлайн покупко-продажба

Защитата от измами не е невъзможна... просто следвайте някои прости, но основни правила:

- Бъдете внимателни с прекалено ниските цени: те са първият знак за възможна измама.
- Винаги проверявайте отзивите за продавача, когато купувате от аукционни сайтове (като eBay).

Отрицателни отзиви = висок риск от измама.

- Търсете телефонния номер или прякора в Google: много пъти вече е бил докладван като измама.

- Не вярвайте на идентификационни документи, изпратени от продавачи или купувачи: Те могат да са фалшиви или откраднати от други жертви.

- Никога не изпращайте копия на своите документи на непознати: Те могат да ги използват за измами или да причинят щети от ваше име.

- Ако сте продавач, НИКОГА не изпращайте пари: вие трябва да получавате парите, а не обратното!
- Никога не отивайте на поща, за да получите плащане: НЕ МОЖЕТЕ да получите пари, като вкарате картата си. Всеки, който ви помоли да направите това, ви измамва.

Слайд

3

–

продължение

Винаги проверявайте на търговски сайтове:

- Дали има реални контакти (телефон, имейл, адрес).
Липсата на тези данни е голям алармен сигнал!
- Използвайте само добре познати и добре оценени сайтове: ако е клонинг сайт, обикновено няма отзиви или има само подозрителни такива.

Слайд 4 – Как да избегнем капаните при онлайн пазаруване и продажби

Когато пазарувате онлайн, златното правило е: ако нещо изглежда прекалено хубаво, за да е истина, вероятно е измама. Продукт, който струва значително по-малко от нормалната цена, например смартфон на половин цена, трябва веднага да ви алармира. Измамниците използват тези „супер отстъпки“, за да привлекат вниманието.

Ако купувате от аукционен сайт или портал като eBay или Subito.it, винаги проверявайте отзивите за продавача. Ако последователно получава отрицателни коментари или има нисък рейтинг, най-добре е да се откажете.

Полезен съвет е също да потърсите телефонния номер или потребителското име на продавача в Google. Измамниците често са били докладвани от други потребители, и може да намерите подобни преживявания.

А ако някой ви изпрати снимка на личната си карта, за да „докаже“, че е надежден... бъдете внимателни! Тази карта може да е фалшива или открадната от друга жертва. Не ѝ се доверявайте само защото има снимка: всичко онлайн може да бъде фалшифицирано.

Слайд

5

–

продължение

Обратно също е вярно: никога не изпращайте документите си на хора, които не познавате добре. Дори проста снимка на документа ви е достатъчна, за да позволи на измамник да го използва незаконно.

Когато продавате продукт, помнете, че вие сте този, който трябва да получава парите, а не да ги изпраща! Ако някой ви каже, че трябва да заредите акаунта си, за да ви плати, или ви помоли да отидете до банкомат и да вкарете картата си, за да получите плащане, никога не го правете: това е капан. Тази техника се нарича „измама с пощенски терминал (postamat scam)“ и работи само ако жертвата изпълни точно инструкциите на измамника.

Накрая, ако пазарувате на електронен търговски сайт, проверете внимателно дали има телефонен номер, валиден имейл адрес и физически адрес. Ако ги няма, сайтът е много вероятно да е измамен или поне ненадежден.

И не забравяйте: винаги проверявайте онлайн отзивите. Ако сайтът е фалшив, някой друг вече е попаднал в капана!

Слайд 6 – Внимавайте за примката! Какво е phishing и как ни крадат данните?

Phishing е като риболов... но вместо риба, ние сме „уловът“. Измамниците хвърлят примамка – обикновено съобщение, което изглежда спешно или важно – и се надяват някой да „хапне“ като кликне върху линка.

Тези съобщения често изглеждат като идващи от вашата банка, куриер или дори известна компания. Те казват неща като:

- „Внимание, вашата сметка е блокирана!“
- „Сега трябва да потвърдите тази операция!“
- „Има проблем с вашата пратка, кликнете тук!“

Слайд 7 – продължение

Всички тези съобщения ви карат да се чувствате притиснати и тревожни, точно защото искат да действате без да мислите два пъти. Така кликвате върху линка... и това е всичко. Сайтът, който изглежда като официалната банка, всъщност е перфектно копие, но фалшиво. Щом въведете данните си, те попадат директно в ръцете на измамника.

Но това не свършва дотук. Ако използвате приложението на банката си или имате система за двуфакторна автентикация (чрез SMS или пръстов отпечатък), измамниците понякога ви обаждат, преструвайки се на истински лица. Те имат учтив глас, знаят вашата информация и говорят за неща, които изглеждат реални. Всъщност вече работят по вашата сметка и им трябва само последната стъпка: OTP код, CVV на картата или потвърждение с пръст. И вие, без да знаете, разрешавате трансфер на стотици или дори хиляди евро.

Понякога дори казват: „За да сте сигурни, деинсталирайте банковото приложение и го инсталирайте отново утре.“ Но това е само, за да ви губят времето и да не видите какво правят със сметката ви.

Слайд 8 – Как да се защитим?

- Никога не кликайте върху линкове в подозрителни съобщения, дори ако изглеждат легитимни или идват от „Poste Italiane“ или „Вашата банка“.
- Ако получите заплашителен телефонен обаждаме, затворете и се обадете директно на банката от официалния ѝ номер.
- НИКОГА не давайте PIN, парола, OTP или CVV код на никого. Нито една банка няма да ги иска чрез съобщение или телефон.
- Ако съобщение ви кара да се обадите на номер, първо проверете дали е официалният на банката. Още по-добре – обадете се директно на обслужването на клиенти.
- Помнете: дори човекът да изглежда учтив, подготвен и убедителен... той може да е измамник с предварително запомнен сценарий.

Слайд 9 – Онлайн измами с търговия: рискът да загубите всичко

През последните години, особено след пандемията, се увеличиха онлайн реклами, обещаващи лесни печалби чрез инвестиции в криптовалути или акции на големи компании като Amazon или Tesla. Тези реклами често се появяват във Facebook или Instagram и са придружени от фалшиви свидетелства, преувеличени числа и твърдения като:

- „Започнете с едва 250 евро и забогатеете за седмица!“

Зад тези реклами стоят фалшиви финансови съветници, които ви се обаждат от чуждестранни номера (често с код +44, т.е. английски) и говорят убедително, почти като истински експерти. Те обясняват как работи търговията, карат ви да се чувствате специални и ви уверяват, че можете да спечелите много повече отколкото в обикновена банка.

Първоначално искат само малка инвестиция, например €250. След това ви дават достъп до фалшива платформа, където „виждате“ как парите ви растат. Всичко изглежда реално – за няколко дни първоначалната ви инвестиция сякаш се удвоява.

Слайд 10 – продължение

И точно тук е истинската капана: те се обаждат отново и ви убеждават да инвестирате още. Казват ви, че е правилното време и ще спечелите още повече. Ако се поддадете, започвате да превеждате все по-големи суми, дори хиляди или десетки хиляди евро.

За да ви „помогнат“, ще поискат да инсталирате програма като AnyDesk или подобна, която позволява на измамника да контролира дистанционно компютъра или телефона ви. Те казват, че е само за помощ, но всъщност използват програмата, за да прехвърлят парите ви в анонимни сметки и портфейли.

Накрая, когато поискате да изтеглите парите си, започват проблемите:

- казват, че има внезапна загуба и са нужни още пари, за да „възстановят“ сумата,
- или че трябва да платите данъци, преди да изтеглите парите.

И когато разбират, че вече няма да изпращате нищо... изчезват.

Слайд 11 – Но не свършва: идва втората измама

След като сте измамени, някой може да се свърже с вас отново, преструвайки се на:

- адвокат,
- банка,
- орган, който обещава да ви помогне да възстановите загубените пари... но само след още едно плащане.

Вие се надявате, вярвате и може би изпращате пари отново. Но това е втора измама, дори по-жестоката от първата.

Слайд 12 – Как да се предпазим?

- Никога не се доверявайте на никого, който ви предлага онлайн инвестиции, особено ако номерът е чуждестранен или непознат.
- Ако наистина искате да инвестирате, отидете в реална банка или при съветник, когото можете да срещнете лично.
- Винаги проверявайте сайта на CONSOB (www.consob.it), за да видите дали компанията, която се е свързала с вас, е разрешена да оперира в Италия.
- Никога не инсталирайте програми за дистанционно управление по молба на непознати.
- Не правете преводи към чужди IBAN, освен ако не сте абсолютно сигурни в получателя.
- И най-важното: не се поддавайте на илюзията за лесни пари. Безопасните инвестиции изискват време, търпение и експертиза.

Слайд 13 – Измамата с счупен или откраднат телефон

Представете си: получавате WhatsApp съобщение от някой, който твърди, че е вашият брат, братовчед или дори племенник, и ви казва, че телефонът му е счупен, сменил е SIM картата и не може да звъни. Звучи странно, нали? Но има още!

За да изглежда по-реално, изпраща супер странни гласови съобщения, съдържащи само досадни шумове като бззз или гргргр – сякаш наистина телефонът е повреден.

След това идва обратът: казва, че трябва спешно да направи плащане, може би за заем, данъци или кредит, но не може, защото телефонът му е счупен и не може да ползва онлайн банкиране. Така той ви пита: „Хей, можеш ли да ми направиш плащането? Ще ти дам данните на картата или IBAN.“ И вие, доверявайки се, му изпращате парите.

За съжаление, всъщност попадате директно в измамата.

Слайд 14 – продължение

Не се паникьосвайте: най-умното е да вземете телефона си (истинския!) и да се обадите на роднината си – „истинския“, а не този, който ви пише в WhatsApp. Ако отговори – браво! Хванали сте измамата.

Ако не отговори, не се паникьосвайте и не бързайте да изпълнявате каквото ви казват в съобщението. Вземете момент, обадете се на друг член на семейството, който може да знае нещо (като снаха, зет или друг роднина), но най-важното: НИКОГА не правете плащане само защото някой ви е писал в WhatsApp.

И ако искате допълнителна сигурност, можете също да се обадите на полицията и да попитате дали ситуацията изглежда като измама. По-добре безопасно, отколкото да съжалявате!

Слайд 15 – Измамата с фалшиви пратки

Тази измама се появява особено около Коледа, когато всички сме супер заети с онлайн пазаруване. Получавате съобщение, което изглежда, че е от куриера, например: „Хей, има проблем с вашата пратка!“

Съобщението ви кани да кликнете на линк, за да „решите проблема“ и да получите пратката си. Но внимавайте – това е пълна измама!

Класическите фрази, които може да видите:

- „Вашата пратка е задържана в нашия логистичен център. Следвайте инструкциите тук:“ (и има линк)
- „Здравейте, не успяхме да доставим пратката, проверете тук:“ (линк)
- „Вашата пратка може да се забави, потвърдете доставката тук:“ (линк)
- „Здравейте, пратката ви чака да настроите предпочитанията за доставка. Кликнете тук:“ (линк)
- „Имаме пратка за вас. За да насрочите доставка, кликнете тук:“ (линк)

Тези съобщения изглеждат сериозни, нали? Но щом кликнете на линка, отваряте страница, която изглежда като официалния сайт на куриера, но е капан!

Ще поискат да платите например 2 евро или малка такса, за да отключите доставката. Въвеждате данните на картата си и... бум! Вземат тези 2 евро, а междувременно активирате скъпи абонаменти за странни услуги с месечни такси до 50 евро!

Опитът да блокирате тези абонаменти? Мисия невъзможна. Единственият изход е да докладвате и блокирате картата, като поискате нова.

Слайд 16 – продължение
Трик за избягване на измамата: проверявайте линка внимателно – ако не започва с „https“ („s“ е решаващо!), т.е. няма SSL сертификат, бъдете много внимателни – това често е знак за измама.

Ако очаквате пратка и имате тракинг код, отидете директно на официалния сайт на куриера и проверете къде е пратката. Ако имате съмнения, обадете се на куриера преди да кликнете на каквото и да е.

Правило номер едно: никога, никога, никога не кликайте на подозрителни линкове!

Слайд 17 – Кражба на идентичност
Много неприятно нещо, което може да се случи онлайн, е някой да открадне дигиталната ни идентичност. Какво е това? Това е като да откраднат вашата „онлайн версия“ – цялата информация, която ви идентифицира в интернет, като име, снимка, телефон, имейл и дори по-сериозни данни като SPID, PEC или дигитален подпис.

Проблемът е, че профилите в социалните мрежи като WhatsApp, Instagram и Facebook са любими цели на измамниците. Често, още по-зле, някой използва нашата информация, за да създаде фалшив профил, който изглежда точно като нас!

Как работи кражбата на профил? Често получавате съобщение от контакт (който е бил хакнат), с покана да кликнете на линк. Може да пише „Участвайте в анкета“ или нещо подобно. Но линкът е капан – той е за потвърждение на смяна на парола, която някой се опитва да направи на вашия профил. Ако кликнете, всъщност казвате: „Да, смени паролата!“ и хакерът получава контрол над акаунта ви.

Веднъж вътре, хакерът променя всичко: пароли, имейли, настройва двуфакторна автентикация с техния номер, а вие оставате извън профила. Оттам те могат да използват профила ви за странни съобщения на приятели, разпространение на омраза, увеличаване на последователи на инфлуенсъри и дори, за съжаление, за незаконни действия.

Слайд 18 – продължение
Проблем са и фалшивите профили: ако не внимавате с поверителността, всеки може да вижда снимките, публикациите и видеата ви и да използва информацията, за да създаде профил, който изглежда като вашия. Понякога дори приятели или познати го правят, от завист или просто да създадат проблем, да ви обиждат или да клюкарстват.

Но има и по-лошо: получавате съобщения (дори SMS или имейли), които изглеждат от официални агенции като INPS. Те казват „Имате чек за получаване“ или „Актуализирайте пенсионния си статус“ и включват линк. Ако кликнете, ви искат лични документи като лична карта, данъчен код и селфи с картата в ръка. Но внимавайте, нито една публична администрация не иска това!

Тези документи се използват от измамници, за да отворят онлайн банкови акаунти на ваше име и да извършват незаконни действия. Ако се сблъскате с това, докладвайте веднага, за да може полицията да се намеси и да затвори фалшивите сайтове.

Слайд

19

–

продължение

Съвети за предпазване:

- Никога не кликайте на странни линкове, дори ако идват от приятели или роднини. Ако вече сте клиkali, опитайте да възстановите профила чрез официалните процедури, но това често е трудно.
- Не публикувайте снимки или публикации, които разкриват къде живеете, как живеете или твърде лични данни. Внимавайте и с геолокацията в снимките!
- Никога не качвайте лични документи на сайтове или портали, освен ако не сте 100% сигурни, че са действително необходими. Публичните администрации вече имат вашите данни; те няма да искат да качват нищо.
- Ако частно лице ви иска лични документи по време на преговор или продажба, откажете! Това е огромен риск.

С малко внимание и разум можете да се чувствате по-сигурни в интернет!

Слайд

20

–

Клевета

и

престъпления

от

омраза

Внимание,

приятели!

Клеветата е сериозно престъпление, което включва уронване на нечия репутация или приписване на неверни факти, които я увреждат. С появата на социалните мрежи този проблем нарасна драстично, защото публикациите често предизвикват бурни дискусии, а много хора губят самообладание и прибягват до обиди, нападки и злословие срещу тези, които не са съгласни с тях.

Когато това се случва в социалните мрежи, е още по-сериозно, защото обидите се виждат от много хора – понякога хиляди. Това, което често наричаме „мнение“, всъщност може да представлява клевета, а пострадалият има право да подаде жалба.

Към това се добавят и явленията с т.нар. „хейтъри“ – хора, които провокират конфликти и сипят обиди – и „hate speech“ (реч на омразата), тоест изказвания, които подбуждат към насилие или омраза срещу определени хора или групи.

Италианският закон (чл. 604 bis от Наказателния кодекс) строго наказва подбуждането към омраза и дискриминационната пропаганда, основана на раса, етническа принадлежност, религия или други лични фактори.

Съществува и препоръка на Комисията срещу расизма и нетолерантността към Съвета на Европа (ECRI) (Препоръка № 15/2015), която обяснява какво е реч на омразата: всички форми на комуникация, които насърчават или подбуждат към омаловажаване, омраза, стигматизация или заплахи срещу човек или група поради раса, цвят на кожата, произход, религия, пол, сексуална ориентация и други основания.

Слайд

21

–

продължение...

Когато участваме в онлайн дискусии, винаги трябва да помним да използваме добри маниери и здрав разум – така, както го правим и в реалния живот.

За съжаление, анонимността в интернет и чувството за дистанция от другите често изкарват наяве най-лошото у нас, карайки ни да се държим като „тролове“ или „хейтъри“, без дори да осъзнаваме. Това явление се нарича „**ефектът на Гигес**“ (от мита за Гигес, разказан от Платон), когато се чувстваме недосегаеми само защото сме онлайн.

Затова: нека винаги уважаваме другите, използваме интернет отговорно и не позволяваме анонимността да ни превърне в лоши хора.

Мрежата е сериозно нещо, и правилата на учтивостта и закона важат и там.

Слайд **22** – **Край**

Интернет е мощен инструмент: той може да информира, обединява, забавлява... Но може и да заблуди, да открадне данни, да разпространява омраза или да ви измами за секунди.

Да умееш да разпознаваш онлайн опасностите не е параноя – това е интелигентност. Не кликвайте на случаен принцип. Не се доверявайте само защото „изглежда истинско“. Никога не подценявайте последствията.

Както каза Ед Шийрън:
„Give a little time to me...“
...ето, преди да кликнете: дайте си миг.

Помислете. Проверете. Попитайте.
Защото онлайн – онзи, който спира (за да се замисли), е този, който остава в безопасност.