МОДУЛ 6 – ОНЛАЙН ПЛАЩАНИЯ

6.2 Най-добри практики и безопасност на онлайн плащанията

Въведение	С нарастването на онлайн пазаруването и дигиталните транзакции е жизненоважно да запазите онлайн плащанията си в безопасност, за да защитите финансовата си информация. Безопасността на онлайн плащанията включва стъпки за защита на вашите лични и финансови данни, когато правите покупки или транзакции онлайн. Като разберете рисковете и вземете предпазни мерки, можете да намалите шансовете за измама или кражба на самоличност. Безопасността на онлайн плащанията включва мерки за защита на вашите лични и финансови данни от попадане в неподходящи ръце. Един съществен аспект е да сте наясно с фишинг. В този урок ще научите как да сте в безопасност, когато извършвате онлайн плащания, благодарение на списък с най-добри практики и съвети относно онлайн безопасността, когато има финансови аспекти.
ПРОВЕРКА НА ПРЕДИШНИ ЗАДАЧИ	По време на ролевата игра зрелостниците ще поемат различни роли, според проучването, което са провели при изпълнение на заданието. Оставете място за свободно изразяване и богато взаимодействие между обучаемите, намесвайте се само когато е необходимо. Този подход им позволява

Key Action 2 – Small-scale Partnerships in Adult Education
Project Number: 2022-2-EL01-KA210-ADU-000093393

	да изследват ситуации от реалния живот и да развият практически умения за безопасно навигиране при онлайн плащания.
ВЪВЕДЕНИЕ В ТЕМАТА	Най-добрият метод за безопасност на онлайн плащанията е редовно да актуализирате софтуера си. Това включва вашата операционна система, уеб браузър и всеки софтуер за сигурност, който използвате. Актуализациите често включват корекции за известни проблеми със сигурността, което помага да защитите вашата лична и финансова информация от кибер заплахи. Активирайте автоматичните актуализации, когато е възможно, за да сте сигурни, че използвате най-сигурните версии на софтуера. Използването на защитени уебсайтове е от решаващо значение при извършване на онлайн транзакции. Потърсете „https“ в URL адреса, което показва защитена връзка, която криптира вашите данни. Избягвайте да въвеждате чувствителна информация на уебсайтове без тази защитена връзка и внимавайте със сайтове, които искат ненужни лични данни. По-добре е да бъдете предпазливи, когато се съмнявате в легитимността на даден уебсайт. Наблюдението на активността в акаунта ви е от съществено значение за безопасността на онлайн плащанията. Редовно проверявайте извлеченията по сметката си и историята на транзакциите, за да забележите всякаква неразрешена или подозрителна дейност. Преглеждайте акаунта си поне веднъж седмично и настройте сигнали за големи или необичайни транзакции, за да сте информирани в реално време. Ако забележите неразрешени или подозрителни транзакции, незабавно

Key Action 2 – Small-scale Partnerships in Adult Education
Project Number: 2022-2-EL01-KA210-ADU-000093393

	докладвайте за тях на вашата финансова институция. Повечето банки и компании за кредитни карти имат отдели за измами, които да разследват и разрешават подобни проблеми. Препоръчително е да поддържате записи на вашите комуникации с вашата финансова институция относно подозрителни транзакции за бъдещи справки. Освен това предприемете проактивни стъпки, за да защитите информацията си за онлайн плащане. Използвайте сигурни и уникални пароли за вашите акаунти, активирайте двуфакторно удостоверяване и избягвайте използването на обществени Wi-Fi мрежи за онлайн плащания.
ОБЩА ТЕОРИЯ	Що се отнася до сигурността, системите за онлайн плащане имат усъвършенствани мерки за защита на чувствителна информация. Технологията за криптиране осигурява предаването на данни, а двуфакторното удостоверяване проверява самоличността на потребителите, минимизирайки рисковете от измами. Въпреки тези предпазни мерки, потребителите все пак трябва да вземат предпазни мерки като използване на силни пароли, избягване на обществен Wi-Fi за транзакции и редовно наблюдение на акаунти, за да предотвратят кибер заплахи. Онлайн плащанията предлагат няколко предимства за потребителите, включително удобство, гъвкавост и сигурност. Извършването на плащания онлайн е удобно, тъй като клиентите могат да го правят по всяко време и навсякъде с интернет връзка, елиминирайки необходимостта да посещават физически магазин или

Key Action 2 – Small-scale Partnerships in Adult Education
Project Number: 2022-2-EL01-KA210-ADU-000093393

	банка. Освен това онлайн плащанията осигуряват гъвкавост, като предлагат различни опции за плащане като кредитни карти, дебитни карти и цифрови портфейли. Измамите с фишинг често включват измамни имейли или съобщения, които се представят за доверени лица, за да ви подмамят да разкриете чувствителна информация. За да не станете жертва, внимавайте с нежелани имейли и никога не кликвайте върху подозрителни връзки и не предоставяйте лична информация. Най-добрите практики за безопасност на онлайн плащанията могат да бъдат: 1. Използвайте виртуална частна мрежа (VPN): Помислете за използване на VPN, когато извършвате онлайн плащания, особено когато използвате обществени Wi-Fi мрежи. VPN криптира вашата интернет връзка, осигурявайки допълнителен слой на сигурност и поверителност. 2. Редовно преглеждайте настройките за поверителност: Отделете време, за да преглеждате и актуализирате редовно настройките за поверителност на своите акаунти и устройства. Ограничете количеството лична информация, споделена онлайн, за да минимизирате риска от кражба на самоличност и неоторизиран достъп до вашите акаунти. 3. Бъдете внимателни с имейли и телефонни измами: Бъдете внимателни с нежелани имейли или телефонни обаждания, изискващи лична или финансова информация, дори ако изглежда,

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only for the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Key Action 2 – Small-scale Partnerships in Adult Education
Project Number: 2022-2-EL01-KA210-ADU-000093393

	че са от законни източници. Избягвайте да кликвате върху връзки или да изтегляте прикачени файлове от неизвестни или подозрителни източници. 4. Активиране на многофакторно удостоверяване: Когато е възможно, активирайте многофакторно удостоверяване (MFA) за вашите онлайн акаунти. MFA добавя допълнителен слой сигурност, като изисква допълнителна проверка освен парола, като например еднократен код, изпратен на вашия телефон. 5. Съхранявайте резервни копия на важни данни: Редовно архивирайте важни документи и данни, съхранени на вашите устройства, като например финансови записи и разписки за транзакции. В случай на пробив в сигурността или загуба на данни, наличието на резервни копия гарантира, че все още имате достъп до важна информация.
РЕГИОНАЛНА ТЕОРИЯ	Обобщихме и преведохме скорошно проучване от „Il Sole 24 Ore“ (https://www.ilsole24ore.com/art/la-sicurezza-informatica-passa-nuovi-modelli-relazione-i-cittadini-clienti-AF3AldXC) предоставя някои много интересни данни за най-новото развитие на италианско ниво по темата за онлайн плащанията: В Европа и Италия има спешна нужда от бързо и ефективно преодоляване на празнината в защитата на киберсигурността както за системата на страната, така и за отделните стратегически активи, като се започне от малки и големи предприятия. Както централната публична администрация (CPA), така и местната публична

Key Action 2 – Small-scale Partnerships in Adult Education
Project Number: 2022-2-EL01-KA210-ADU-000093393

	администрация (LPA) обработват чувствителна информация ежедневно и предоставят критични и често незаменими услуги. Тази промяна към укрепване на киберсигурността е подкрепена от последните разпоредби, както на европейско (Регламент на ЕС от 7 януари 2023/2841), така и на национално ниво (Проект на закон за киберсигурността, одобрен от Съвета на министрите на 25 януари). Тези разпоредби имат за цел да ускорят и насърчат приемането на конкретни мерки за смекчаване на киберриска, пред който са изправени както публичните, така и частните субекти. През последните години броят и ефективността на кибератаките нарастват, оказвайки влияние върху дейността на компании и публични администрации, които предоставят стратегически услуги и управляват чувствителни данни. Икономическите последици и повишените прекъсвания на услугите засягат общностите, гражданите-потребители и клиентите. Ключовите институции не могат да бъдат оставени изложени на подобни рискове, особено като се има предвид политическата, икономическа и социална нестабилност, произтичаща от сценарии на международни конфликти. Издаването на новия европейски регламент има за цел да ускори адаптирането и реакцията на страната към кибер рисковете чрез установяване на мерки за повишаване нивата на киберсигурност в институциите и органите на ЕС. Регламентът определя мерки за създаване на вътрешна рамка за управление на риска, управление и контрол за всеки субект и създава нов Междуинституционален комитет за киберсигурност (IICB), който има за

Key Action 2 – Small-scale Partnerships in Adult Education
Project Number: 2022-2-EL01-KA210-ADU-000093393

	задача да наблюдава и подкрепя правилното прилагане на новите правила. На национално ниво законопроектът за киберсигурността разширява обхвата на субектите, които трябва да докладват за съответен инцидент. Той упълномощава субектите да разработят вътрешна структура, отговорна за определяне на стратегии за управление на рисковете за киберсигурността и прилагане на планове за действие и мониторинг на риска. Законопроектът въвежда и нова хипотеза за отговорност на държавата и административни санкции при неизпълнение на установените задължения. Несъмнено има повишена чувствителност към тези проблеми в рамките на пазара на киберсигурност. Публичните и частните организации започват да подхождат към дигиталната трансформация с фокус върху „сигурни цифрови иновации“, наблягайки на вниманието върху аспектите на киберсигурността чрез усъвършенствани инструменти за откриване на пробиви, дефиниране на по-ефективни стратегии за реагиране и предоставяне на иновативни защитни услуги за стратегически активи. Ползите са обективно значими, тъй като разходите за репутация, прекъсванията на услугите и загубата на информация са реални и никой разумен държавен служител не може да ги игнорира или да се въздържи от предприемане на действия за противодействие. Тази трансформация включва цялостно преосмисляне на оперативните процеси в перспектива на дълбоки иновации, активирани от нови модели на отношения с потребителите и

Key Action 2 – Small-scale Partnerships in Adult Education
Project Number: 2022-2-EL01-KA210-ADU-000093393

	предоставяне на услуги. Иновациите водят до положителна трансформация не само за самата институция, но и за гражданите и частните лица, които се възползват от услугите. Отговорност на индустриалните оператори е да направят достъпа до модерни услуги за киберсигурност по-„демократичен“. Предизвикателството е да направим тези услуги все по-опростени, лесни за конфигуриране и управление и достъпни за малки и средни организации, без да се жертва ефективността.
ПРИМЕРИ (КАКТО РЕГИОНАЛНИ, ТАКА И НЕСПЕЦИФИЧНИ)	1. Мария, възрастен гражданин, редовно пазарува онлайн хранителни стоки. Преди да направи каквито и да било покупки, тя винаги проверява за символа на катинар в адресната лента на браузъра и гарантира, че URL адресът на уебсайта започва с „https://“, за да потвърди, че уебсайтът е защитен. Като следва тази практика, Мери защитава своята лична и финансова информация от потенциални кибер заплахи. 2.Джовани, друг старши, често проверява извлеченията по банковата си сметка и транзакциите с кредитни карти онлайн. Наскоро той забеляза подозрителна транзакция в извлечението по кредитната си карта. Без забавяне Джон съобщи за неразрешеното таксуване на банката си, която незабавно проучи проблема и възстанови сумата. Бдителността на Джон при наблюдение на активността в акаунта му му помогна бързо да открие и адресира потенциална измамна дейност. 3. Сара, пенсиониран професионалист, обича да използва различни онлайн услуги за комуникация и забавление. За

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only for the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Key Action 2 – Small-scale Partnerships in Adult Education
Project Number: 2022-2-EL01-KA210-ADU-000093393

	да гарантира сигурността на своите акаунти, Сара следва съвета за създаване на силни и уникални пароли за всеки от своите онлайн акаунти. Тя използва комбинация от букви, цифри и специални знаци и избягва използването на лесно отгатваема информация като нейното име или рождена дата. Като поддържа силни пароли, Сара намалява риска от неоторизиран достъп до нейните онлайн акаунти.
ПРАКТИЧЕН ОПИТ	Коя е една от най-добрите практики за гарантиране на безопасността на онлайн плащанията? а. Споделяне на пароли с приятели б. Използване на обществен Wi-Fi за транзакции в. Проверка за символа на катинар в адресната лента на браузъра г. Щракване върху подозрителни връзки в имейли Кое от следните е сигурен метод на плащане за онлайн транзакции? а. Изпращане на пари в брой в плик б. Използване на кредитна карта с технология за криптиране в. Предоставяне на вашия социалноосигурителен номер на неизвестни уебсайтове г. Споделяне на вашия ПИН номер с онлайн търговци на дребно Колко често трябва да наблюдавате вашите финансови отчети и кредитни отчети за подозрителна дейност? а. Никога б. Веднъж годишно в. Поне веднъж месечно г. Само когато получите известие от вашата банка

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only for the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Key Action 2 – Small-scale Partnerships in Adult Education
Project Number: 2022-2-EL01-KA210-ADU-000093393

	Какво трябва да направите, ако забележите неоторизирани транзакции по сметката си? а. Игнорирайте ги, тъй като вероятно ще се разрешат сами б. Съобщете ги незабавно на вашата финансова институция в. Изчакайте следващото изявление, за да видите дали ще се повторят г. Споделете информацията в социалните медии, за да предупредите другите Кое от следните НЕ е препоръчителна практика за безопасност на онлайн плащанията? а. Използване на силни и уникални пароли за всеки онлайн акаунт б. Избягване на обществени Wi-Fi мрежи за транзакции в. Щракване върху връзки в имейли от неизвестни податели г. Проверка за сигурни връзки на уебсайтове, преди да въведете чувствителна информация *Верни отговори* *1 – в* *2 – б* *3 – в* *4 – б* *5 - в*
Дискукия	В епохата на нарастваща дигитализация вярвате ли, че традиционните методи на плащане, като пари в брой или чекове, все още са уместни или стават остарели в полза на онлайн плащанията? Защо? „Как можем да постигнем баланс между възприемането на удобството на онлайн плащанията, като същевременно гарантираме сигурността на нашата финансова информация? Какви мерки

Key Action 2 – Small-scale Partnerships in Adult Education
Project Number: 2022-2-EL01-KA210-ADU-000093393

	смятате, че са необходими за постигане на този баланс?
ОБРАТНА ВРЪЗКА И ДРУГИ	Целта на това задание е да даде възможност на възрастните хора със знанията и уменията за подобряване на сигурността на онлайн плащанията чрез разработване и прилагане на персонализиран контролен списък за сигурност на онлайн плащанията. В това задание възрастните ще разработят изчерпателен контролен списък за сигурност на онлайн плащанията, като се фокусират върху основните мерки за сигурност за онлайн транзакции, като сигурност на уебсайтове, управление на пароли и безопасни методи на плащане. След това те ще прегледат текущите си практики за онлайн плащане, включително уебсайтовете, които използват, използваните методи на плащане и стратегии за управление на пароли. След като сравнят своите практики с елементите от контролния списък, те ще идентифицират всички пропуски или области за подобряване на сигурността на онлайн плащанията. Въз основа на тази оценка възрастните хора ще направят необходимите корекции в своите практики, прилагайки допълнителни мерки за сигурност или променяйки съществуващите, за да подобрят сигурността. Накрая те ще напишат кратък размисъл, в който ще обсъдят всички предизвикателства, възникнали по време на фазата на оценка и коригиране, и ще размишляват върху значението на сигурността на онлайн плащанията за личната финансова безопасност.

Key Action 2 – Small-scale Partnerships in Adult Education
Project Number: 2022-2-EL01-KA210-ADU-000093393