# МОДУЛ 2 – Банкови операции и цифрови умения

## 2.2: Безопасност онлайн: практики за сигурност за цифрово банкиране

| | |
|---|---|
| **Въведение** | В този раздел представяме критичната тема за онлайн сигурността на цифровото банкиране. Ние подчертаваме важността на разбирането на мерките за сигурност за защита на личната и финансова информация при извършване на транзакции онлайн. Това знание гарантира по-безопасни и по-уверени взаимодействия с платформите за цифрово банкиране. |
| **ПРОВЕРКА НА ПРЕДИШНИ ЗАДАЧИ** | N/A |
| **ВЪВЕДЕНИЕ В ТЕМАТА** | Раздел 4.2 се фокусира върху това да ви предостави основни умения, за да сте в безопасност, докато банкирате онлайн. Тъй като все повече финансови услуги преминават към цифрови платформи, от решаващо значение е да знаете как да разпознавате и избягвате потенциални рискове като фишинг измами. Това устройство ще ви даде възможност да навигирате в онлайн банкирането сигурно и уверено. |
| **ОБЩА ТЕОРИЯ** | Разбирането и прилагането на мерки за онлайн сигурност е от решаващо значение за безопасното цифрово банкиране и цялостното използване на интернет. По този начин хората могат значително да подобрят своята киберсигурност и да се защитят от онлайн заплахи. Тези практики насърчават сигурно и уверено онлайн изживяване, което е от решаващо значение за поддържане на контрол върху личните финанси и дигиталните взаимодействия. |

Co-funded by the European Union

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

| | |
|---|---|
| | Значението на силните пароли и двуфакторното удостоверяване<br><br>Силни пароли:<br><br>Определение: Силните пароли са сложни и трудни за отгатване от другите. Те обикновено включват комбинация от главни и малки букви, цифри и специални знаци.<br><br>Важно: Силните пароли са първата линия на защита срещу неоторизиран достъп до вашите акаунти. Те правят по-трудно за хакерите да разбият или отгатнат паролата ви с помощта на автоматизирани инструменти.<br><br>Двуфакторно удостоверяване (2FA):<br><br>Определение: 2FA добавя допълнителен слой сигурност, като изисква не само парола, но и втора част от информацията, обикновено код, изпратен на вашия телефон или генериран от приложение.<br><br>Важност: Дори ако някой успее да получи вашата парола, той пак ще се нуждае от втория фактор (напр. вашия телефон), за да получи достъп до вашия акаунт. Това значително повишава сигурността и намалява риска от неоторизиран достъп.<br><br>Разпознаване на опити за фишинг и други често срещани измами<br><br>Опити за фишинг:<br><br>Определение: Фишингът е измамен опит за получаване на чувствителна информация (като пароли, потребителски имена, данни за кредитни карти), като се представяте за надежден субект в електронна комуникация.<br><br>Разпознаване на знаци: Фишинг имейлите често изискват чувствителна информация, използват общи поздрави, съдържат правописни или граматически грешки или имат подозрителни връзки или прикачени файлове.<br><br>Важност: Способността да разпознавате опити за фишинг помага да не станете жертва на кражба на самоличност, финансови измами и други киберпрестъпления.<br><br>Защита на личната информация онлайн |

Co-funded by the European Union



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

| | |
|---|---|
| | Лична информация: Това включва подробности като вашето пълно име, адрес, дата на раждане, социалноосигурителен номер и всяка финансова информация.<br><br>Най-добри практики:<br><br>Предоставяйте лична информация само на защитени уебсайтове (потърсете HTTPS в URL адреса).<br><br>Бъдете внимателни при споделянето на лични данни в социалните медии и други онлайн платформи.<br><br>Избягвайте да отговаряте на непоискани искания за лична информация.<br><br>Важно: Защитата на личната информация намалява риска от кражба на самоличност, измама и злоупотреба с вашите данни от злонамерени лица.<br><br>Разбиране на ролята на софтуера за сигурност и актуализациите<br><br>Софтуер за сигурност:<br><br>Определение: Софтуерът за сигурност включва антивирусни програми, защитни стени и инструменти против зловреден софтуер, предназначени да предпазват вашите устройства от злонамерен софтуер и кибер заплахи.<br><br>Роля: Софтуерът за сигурност сканира и премахва вируси, злонамерен софтуер и други заплахи, осигурявайки ниво на защита срещу кибератаки.<br><br>Актуализации:<br><br>Определение: Софтуерните актуализации (включително операционни системи, браузъри и приложения) често включват корекции за сигурност, които поправят уязвимостите и укрепват защитата срещу новооткрити заплахи.<br><br>Важност: Редовното актуализиране на софтуера гарантира, че известните слабости в сигурността се отстраняват своевременно, намалявайки риска от експлоатация от киберпрестъпници. |
| **РЕГИОНАЛНА ТЕОРИЯ** | 1. Значението на силните пароли и двуфакторното удостоверяване |

Co-funded by the European Union

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

| | |
|---|---|
| | В Гърция, както и в много страни, използването на силни пароли и двуфакторно удостоверяване (2FA) се набляга на банки и експерти по киберсигурност. Гръцките банки често препоръчват на клиентите да създават пароли, които включват комбинация от букви (както главни, така и малки), цифри и специални знаци. Те също така насърчават използването на 2FA, където е налично, за добавяне на допълнителен слой на сигурност освен парола. Това е особено важно в Гърция поради нарастващото приемане на цифрови банкови услуги, което налага стабилни мерки за сигурност за защита срещу кибер заплахи.<br><br>2. Разпознаване на опити за фишинг и други често срещани измами<br><br>Гърците се съветват да бъдат бдителни срещу опитите за фишинг, които са широко разпространени в различни онлайн платформи, включително имейли, социални медии и приложения за съобщения. Често срещаните измами в Гърция може да включват измамни имейли или съобщения, които се преструват, че са от банки или държавни агенции, изискващи лична информация или подканващи потребителите да кликнат върху злонамерени връзки. Образователните кампании на банки и правителствени агенции подчертават важността на проверката на автентичността на съобщенията, преди да отговорите или да предоставите лична информация.<br><br>3. Защита на личната информация онлайн<br><br>Защитата на личната информация е сериозна загриженост в Гърция, особено с прилагането на GDPR (Общ регламент за защита на данните) в целия ЕС. Гръцките потребители се насърчават да внимават при споделянето на лични данни онлайн, като гарантират, че уебсайтовете са защитени (HTTPS протокол), преди да въведат чувствителна информация. Банките и финансовите институции в Гърция също са въвели строги мерки за защита на данните, за да се съобразят с изискванията на GDPR, като гарантират, че клиентските данни се обработват сигурно и прозрачно.<br><br>4. Разбиране на ролята на софтуера за сигурност и актуализациите<br><br>В Гърция, както и навсякъде другаде, се подчертава ролята на софтуера за сигурност (като антивирусни програми и защитни стени) за защита срещу зловреден софтуер и други кибер заплахи. Гръцките потребители се съветват да инсталират реномиран софтуер за сигурност на своите устройства и да го актуализират редовно. Актуализациите на операционни |

Co-funded by the European Union



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

| | |
|---|---|
| | системи, браузъри и приложения често включват корекции за сигурност, които помагат за смекчаване на уязвимостите и подобряване на цялостната киберсигурност.<br><br>5. Регулаторна рамка и съответствие<br><br>Гръцките финансови институции работят в рамките на регулаторната рамка на Централната банка на Гърция и Европейската централна банка (ЕЦБ), която определя насоки за киберсигурност и защита на данните в банковите операции. Спазването на тези разпоредби гарантира, че гръцките банки се придържат към високи стандарти за сигурност и поверителност, когато предлагат цифрови банкови услуги. Потребителите се насърчават да се запознаят с правата си съгласно тези разпоредби и да докладват незабавно за всяка подозрителна дейност на своята банка или съответните органи. |
| **ПРИМЕРИ (КАКТО РЕГИОНАЛНИ, ТАКА И НЕСПЕЦИФИЧНИ)** | Разпознаване на опит за фишинг<br><br>Контекст: Получавате имейл във входящата си кутия, който изглежда е от вашата банка, с молба да предоставите паролата си, за да „потвърдите акаунта си от съображения за сигурност“. В имейла се твърди, че неспазването може да доведе до временно спиране на вашия акаунт.<br><br>Стъпки за разпознаване и реагиране:<br><br>Проверете имейл адреса на подателя:<br><br>Контекст: Имейлът твърди, че е от вашата банка (напр. „YourBankName@gmail.com“).<br><br>Анализ: Легитимните банки обикновено използват своите официални имена на домейни за комуникация (напр. „@yourbankname.com“). Gmail или друг общ домейн може да бъде червен флаг.<br><br>Проверете за общи поздравления и спешност:<br><br>Контекст: Имейлът започва с общ поздрав като „Уважаеми клиенте“ и подчертава спешността.<br><br>Анализ: Легитимните комуникации често използват вашето име и поддържат професионален тон. Неотложността и заплахите от последствия при неспазване са често срещани тактики, използвани от фишърите, за да принудят жертвите да предоставят чувствителна информация. |

Co-funded by the European Union

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

| | |
|---|---|
| | Потърсете правописни и граматически грешки:<br><br>Контекст: Имейлът съдържа множество правописни грешки и неудобна граматика.<br><br>Анализ: Легитимните съобщения от банките обикновено са добре написани и професионални. Грешките в граматиката и правописа са индикатори за опит за фишинг.<br><br>Задръжте курсора на мишката върху връзки, без да щраквате:<br><br>Контекст: Имейлът включва връзка, която уж ви насочва към уебсайт, за да въведете паролата си.<br><br>Анализ: Задръжте курсора на мишката върху връзката (без да щраквате). Ако показаният URL адрес не съответства на официалния уебсайт на вашата банка или пренасочва към подозрителен домейн, това вероятно е връзка за фишинг.<br><br>Свържете се директно с вашата банка:<br><br>Контекст: Подозирате, че имейлът е опит за фишинг, след като разгледате горните точки.<br><br>Анализ: Вместо да отговаряте директно на имейла, използвайте номер за контакт или URL адрес на официалния уебсайт, който вече имате, за да се свържете с отдела за обслужване на клиенти на вашата банка. Подайте сигнал за подозрителния имейл и проверете дали са необходими някакви действия по вашия акаунт.<br><br>Докладвайте за опит за фишинг:<br><br>Контекст: Вие потвърждавате с вашата банка, че имейлът наистина е бил опит за фишинг.<br><br>Анализ: Докладвайте имейла на официалния имейл адрес за отчитане на фишинг на вашата банка или се свържете с отдела за обслужване на клиенти. Това им помага да предприемат действия за защита на други клиенти от подобни измами. |
| **ПРАКТИЧЕН ОПИТ** | Тест: Разпознаване на опити за фишинг<br><br>1.Кое от следните е често срещан признак за фишинг имейл?<br><br>А) Персонализиран поздрав с вашето име<br><br>Б) Спешно спиране на акаунт, заплашващ език |

Co-funded by the European Union



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

| | |
|---|---|
| | В) Професионален имейл формат от официалния домейн на банката<br><br>Г) Ясни инструкции как да защитите акаунта си<br><br>2.Какво трябва да направите, ако получите имейл с искане за парола, за да потвърдите акаунта си?<br><br>А) Отговорете с вашата парола, за да потвърдите самоличността си<br><br>Б) Кликнете върху връзката, предоставена в имейла, и въведете паролата си<br><br>В) Игнорирайте имейла и го изтрийте незабавно<br><br>Г) Обадете се на вашата банка, като използвате доверен телефонен номер и потвърдете заявката<br><br>3.Защо е важно да проверявате имейл адреса на подателя при подозрителни имейли?<br><br>А) За да проверите дали имейлът съдържа граматически грешки<br><br>Б) За да се гарантира, че имейлът не е маркиран като спам<br><br>В) За да потвърдите дали имейлът е от легитимен източник<br><br>Г) За да докладвате имейла на вашия доставчик на имейл<br><br>4.Какво трябва да направите, ако подозирате, че даден имейл е опит за фишинг?<br><br>А) Препратете имейла до всички ваши контакти, за да ги предупредите<br><br>Б) Кликнете върху всяка връзка в имейла, за да проверите автентичността му<br><br>В) Обадете се директно на вашата банка или финансова институция, за да потвърдите заявката<br><br>Г) Отговорете на имейла с вашата лична информация за проверка<br><br>5.Кое от следните е червен флаг за фишинг имейл? |

Co-funded by the European Union



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

| | |
|---|---|
| | А) Имейл адресът съвпада с официалния домейн на вашата банка<br><br>Б) Имейлът съдържа граматически и правописни грешки<br><br>В) Имейлът предоставя ясни инструкции как да защитите акаунта си<br><br>Г) Имейлът включва връзка към официалния уебсайт на банката за повече информация<br><br>Отговори:<br><br>1.Б) Спешно спиране на акаунт, заплашващ език<br><br>2.Г) Обадете се на вашата банка, като използвате доверен телефонен номер и потвърдете заявката<br><br>3.В) За да потвърдите дали имейлът е от легитимен източник<br><br>4.В) Обадете се директно на вашата банка или финансова институция, за да потвърдите заявката<br><br>5.Б) Имейлът съдържа граматически и правописни грешки |
| **Дискукия** | Въпрос за размисъл 1<br>Трябва ли банките да носят единствената отговорност за възстановяването на разходите на жертвите на онлайн измами или клиентите трябва да носят известна отговорност за гарантиране на собствената си онлайн сигурност?<br><br>Въпрос за размисъл 2<br>Как хората могат да балансират удобството на системите за цифрово плащане с необходимостта от стабилни мерки за сигурност? |
| **ОБРАТНА ВРЪЗКА И ДРУГИ** | |

Co-funded by the European Union

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