



information
matters

Тренировъчна програма за онлайн курсове

Модул 9

Медийна грамотност и поверителност



Финансирано от Европейския съюз. Изразените възгледи и мнения обаче принадлежат изцяло на техния(ите) автор(и) и не отразяват непременно възгледите и мненията на Европейския съюз или на Европейската изпълнителна агенция за образование и култура (EACEA). За тях не носи отговорност нито Европейският съюз, нито EACEA.

Номер на споразумението: 2022-1-BG01-KA220-ADU-000085514



Съфинансирано от
Европейския съюз

Съдържание

Въведение.....	4
Цел.....	11
Резултати от обучението.....	12
Ключови думи.....	12
Предмет и теми.....	13
Основни дефиниции.....	13
Полезни връзки.....	15
Валидиране на модула.....	16
Оценка на модула.....	18
ПРАКТИКА.....	18
Дейност 1: Как да пазим и използваме безопасно паролите?20	
Цели на практиката:.....	20
Материали/продължителност.....	21
Изпълнение на дейността:.....	21
Препоръки за изпълнение.....	25
Въпроси за отразяване.....	26

Дейност 2: Пазете личната информация в безопасност – истории за поверителността	27
Цели на практиката:	27
Материали/продължителност:	28
Изпълнение на дейността:	28
Препоръки за изпълнение	30
Въпроси за отразяване:	30
Приложение към Дейност 2	31
Дейност 3: Онлайн банкиране без страх	35
Цели на практиката:	35
Материали/продължителност:	36
Изпълнение на дейността:	36
Препоръки за изпълнение:	40
Въпроси за отразяване:	41
Поздравления за завършването на Модул 9 – Медийна грамотност и поверителност!	42
ПРИЛОЖЕНИЕ към Модул 9	43
ОТГОВОРИ НА ТЕСТОВЕТЕ:	47

Въведение

Добре дошли в модула за медийна грамотност и поверителност. В този урок ще проучим значението на защитата на личните данни и поддържането на поверителността онлайн, особено за възрастни хора. До края на този урок ще имате по-задълбочено разбиране на проблемите с поверителността в дигиталната ера и ще имате практически стратегии за защита на вашата лична информация.



Нека се запознаем с някои основни определения и примери

- » **Личните данни** са всяка информация, която може да се използва за идентифициране на физическо лице, следователно се отнася до всяка информация, която пряко или косвено се отнася до физическо лице. Те включват подробности като вашето име, адрес, телефонен номер, имейл, рождена дата и дори по-чувствителна информация като вашите финансови отчети или медицинска история. Личните данни са ценни и трябва да се пазят в тайна, за да се предпазят от потенциална злоупотреба или експлоатация.
- » От съществено значение е да защитите поверителността на тези данни от споделяне или достъп от неупълномощени страни, тъй като това може да доведе до кражба на самоличност или други форми на киберпрестъпления. За да предотвратим изтичане на лични данни, трябва да разберем как да използваме настройките за поверителност в социалните медии и други онлайн платформи, да избягваме споделянето на чувствителна информация през незащитени мрежи и да използваме силни пароли и други мерки за сигурност, за да защитим своите акаунти.



- » **Онлайн поверителността** се отнася до способността да контролирате и защитавате вашата лична информация, докато използвате интернет. Това включва защита на вашите лични данни, ограничаване на количеството информация, която споделяте онлайн, и информироване кой има достъп до вашите онлайн дейности. Като разбирате и практикувате онлайн поверителността, можете да поддържате по-голям контрол върху своята дигитална самоличност и да се предпазите от онлайн заплахи като кражба на самоличност, измами или неразрешено наблюдение.
- » Вашият **дигитален отпечатък** е следата от информация, която оставяте след себе си, докато използвате дигитални устройства и интернет. Той обхваща вашите онлайн дейности, включително уебсайтовете, които

посещавате, публикациите в социалните медии, които правите, коментарите, които оставяте, и изображенията или видеоклиповете, които споделяте. Вашият дигитален отпечатък може да има дългосрочни последици и може да бъде използван от други за проследяване на вашето онлайн поведение, влияние върху решенията или дори определяне на доверието ви. Разбирането на вашия дигитален отпечатък е от съществено значение за поддържане на положителна онлайн репутация и защита на поверителността ви.

Като цяло е важно възрастните хора да бъдат проактивни в защитата на поверителността си в дигиталната среда. Като сме информирани, използваме сигурни практики и внимаваме за нашите онлайн дейности, можем да минимизираме потенциалните рискове и да постигнем по-безопасно онлайн изживяване.

Какво означава онлайн безопасността за възрастните хора?

Онлайн поверителността и прилагането на набор от инициативи за безопасност по отношение на защитата на личните данни и личната информация означава:

- Да познавате и прилагате основни правила и принципи за безопасност, защита на неприкосновеността на личния живот и личната информация;
- Да прилагате настройки за поверителност и разрешения като бисквитки, да сте запознати с инструментите за проследяване, да сте наясно с вашия дигитален отпечатък;
- Да бъдете осведомени относно стратегиите и инструментите, използвани в момента за проследяване, шпиониране и навлизане в личната сфера.



Как можете да обучите вашите възрастни участници на медийна грамотност и поверителност?

- Можете да намерите полезно съдържание и допълнителни връзки, свързани с медийната грамотност и поверителността в програмата за обучение.
- Прилагайте дейности, планирани за възрастни учащи, за да подпомогнете тяхната осведоменост относно поверителността. Като работите и изпълнявате тези обучителни дейности, можете да мотивирате и подкрепите вашите участници да съберат и развият желаните умения и компетенции в областта на медийната грамотност и поверителността. Упражненията предлагат възможности за разширяване на знанията в следните 3 области:
 - Как да пазим и използваме безопасно паролите?
 - Пазете личната информация в безопасност – истории за поверителността
 - Онлайн банкиране без страх

- Възможно е вашите участници преди това да са използвали различни, не толкова подходящи правила за работа с пароли. Те се нуждаят от повече търпение и време, за да разберат, че може би трябва да променят практиката си.
- Отделете достатъчно време за практикуване на метод, който вашите участници могат да използват с увереност.
- Възрастните хора често се страхуват от онлайн банкирането, тъй като този подход изглежда твърде опасен за тях. Така че нашата цел е в първата стъпка да потвърдим и да се доближим до техните страхове, за да разберем при какви обстоятелства трябва да работим.
- Ако знаете обстоятелствата на вашите участници, можете да адаптирате историите и по-нататъшните дейности според тях.
- Мотивирайте обучаемите си да направят резюме на правилата за безопасност като напомняне за бъдещите си онлайн дейности. Изложете това правило по привлекателен начин и го разпространете сред вашите участници.



Цел

Лични данни са всяка информация, която може да се използва за идентифициране на физическо лице. От съществено значение е да защитите поверителността на тези данни от споделяне или достъп от неупълномощени страни, тъй като това може да доведе до кражба на самоличност или други форми на киберпрестъпления. За да предотвратят изтичането на лични данни, възрастните трябва да разберат как да използват настройките за поверителност в социалните медии и други онлайн платформи, да избягват споделянето на чувствителна информация през незащитени мрежи и да използват силни пароли и други мерки за сигурност, за да защитят своите акаунти.

Важно е възрастните хора да бъдат проактивни в защитата на личния си живот в дигиталната среда. Като са информирани, използват сигурни практики и внимават за своите онлайн дейности, те могат да сведат до минимум потенциалните рискове и да постигнат по-безопасно онлайн изживяване.

Използвайте предоставените ресурси, за да подкрепите вашите участници, за да подобрят знанията си и да продължат пътуването си към придобиване на медийна грамотност и съзнание за поверителността. Бъдете бдителни, пазете се и се наслаждавайте на дигиталния свят отговорно.

Резултати от обучението

Участниците ще могат да разберат значението на поверителността и да обсъдят възможните уязвимости при използването на интернет и дигитални устройства. Те също така ще научат как да защитават и споделят лична информация отговорно. На обществено ниво те ще развият повишена осведоменост за въздействието на дезинформацията в обществената сфера.

Ключови думи

Лични данни, онлайн поверителност, дигитален отпечатък, интернет хигиена, предпазни мерки.

Предмет и теми

Онлайн поверителност и прилагане на набор от инициативи за безопасност по отношение на защитата на личните данни и личната информация:

- Основни правила и принципи за безопасност, защита на личния живот и личната информация;
- Настройки за поверителност и разрешения като бисквитки, информираност за инструментите за проследяване, дигитален отпечатък;
- Познаване на стратегиите и инструментите, използвани в момента за проследяване, шпиониране и навлизане в личната сфера.

Основни дефиниции

- **Лични данни:** Личните данни се отнасят до всяка информация, която пряко или косвено се отнася до физическо лице. Те включват подробности като вашето име, адрес, телефонен номер, имейл, рождена дата и дори почувствителна информация като вашите финансови отчети или медицинска история. Личните данни са ценни и трябва да се пазят в тайна, за да се предпазят от потенциална злоупотреба или експлоатация.

- **Онлайн поверителност:** Онлайн поверителност се отнася до възможността да контролирате и защитавате вашата лична информация, докато използвате интернет. Това включва защита на вашите лични данни, ограничаване на количеството информация, която споделяте онлайн, и информиране кой има достъп до вашите онлайн дейности. Като разбирате и практикувате онлайн поверителността, можете да поддържате по-голям контрол върху своята дигитална самоличност и да се предпазите от онлайн заплахи като кражба на самоличност, измами или неразрешено наблюдение.
- **Дигитален отпечатък:** Вашият дигитален отпечатък е следата от информация, която оставяте след себе си, докато използвате дигитални устройства и интернет. Той обхваща вашите онлайн дейности, включително уебсайтовете, които посещавате, публикациите в социалните медии, които правите, коментарите, които оставяте, и изображенията или видеоклиповете, които споделяте. Вашият дигитален отпечатък може да има дългосрочни последици и може да бъде използван от други за проследяване на поведението ви онлайн, влияние върху решения или дори определяне на доверието ви. Разбирането на вашия дигитален отпечатък е от съществено значение за поддържане на положителна онлайн репутация и защита на поверителността ви.



Полезни връзки

 <https://www.digitaleseniorinnen.at/leistungen/know-how>

 <https://erwachsenenbildung.at/digiprof/mediathek/17725-studie-zu-bildung-und-digitalen-kompetenzen-im-alter.php>

 <https://cyberclever.eu/resources>

Кратка анимация за онлайн навигация и поверителност:

 https://www.youtube.com/watch?v=zsboDBMq6vo&list=PL3cj0_EtKN4joc4Gt2IFzBMoZp4h5ty7o&t=51s



Валидиране на модула

В края на модула обучаемите ще са придобили

Знания:

Обучаемите са в състояние да

- Разбират значението на личните данни и поверителността
- Идентифицират различните форми на киберпрестъпност
- Съзнателно управляват индивидуалните си настройки в различни платформи
- Знаят точно какви минимални условия са необходими, за да оценят даден уебсайт като защитен
- Прилагат солидни познания при управление на пароли и приложения за онлайн банкиране

Умения:

Обучаемите са в състояние да

- Използват съзнателно силни пароли
- Разпознават случаите, когато нечие лично пространство е нарушено
- Докладват на съответните организации, ако забележат, че техните пароли или данни са били неправилно обработени
- Контролират собствените си онлайн дейности по самоотговорен начин

Компетенции:

Обучаемите са в състояние да

- Боравят със собствените си пароли и лични данни със самоотговорност в онлайн света
- Подкрепят и защитават личното си пространство
- Уважават поверителността на другите потребители
- Използват предимствата на онлайн приложенията и уебсайтовете без страх, но внимателно и съзнателно

Оценка на модула

В приложението към модула ще откриете тестове за измерване на входно и изходно ниво, с които ще можете да проследите напредъка в рамките на обучението.

ПРАКТИКА

Задачите по проекта могат да се решават в малки групи или индивидуално.

Някои предложения за конкретните задачи, съобразени с нуждите и началното ниво на знания на целевата група и целите, които трябва да бъдат постигнати.

- Направете кратки демонстрационни видеоклипове за проблеми с поверителността (подобно на подробните описания в курса) в споделени общностни пространства. Мненията на участниците също могат да бъдат добавени в края на филмите. Тези видеоклипове могат да се използват и по-късно като учебни материали.
- Организирайте с участниците някои общностни практически събития в общността на възрастните хора. С вашата подкрепа, обучаемите могат да изнесат кратки презентации

на колегите си за управление на пароли или онлайн банкиране и да споделят някои практически уроци, които вече са придобили.

- Страница/група в социалните медии за възрастни хора - подкрепете създаването на страница/група в социалните медии - насочена към възрастни потребители, в която редовно да се споделят кратки публикации за най-важните въпроси, свързани с поверителността. Участниците могат първо да направят списък с теми: колкото по-конкретни, толкова по-добре. Подкрепете ги да подберат на база опита от темите и дейностите, засегнати в урока.





Деятност 1: Как да пазим и използваме безопасно паролите?

Цели на практиката:

- Изяснете/повторете целта на паролата
- Научете как да намирате сигурни пароли за себе си, без да ги записвате
- Правилата за „как можете да защитите паролата си?“

Материали/продължителност

- Листове, химикалки и маркери за участниците
- Онлайн шаблони за бяла дъска/плакат (напр. <https://canva.com> и/или по-голяма хартия за плакати за участниците)
- 2 часа

Изпълнение на дейността:

Стъпка 1 – Въведение:

Като въведение в тази дейност, помолете вашите участници да направят списък на областите от ежедневиия живот/уебсайтовете, където използват пароли. Може да се напише на онлайн повърхност (напр. споделен документ/бяла дъска/работен лист/чат).

След това можете да обсъдите в дискусия как участниците са разбрали за паролите и дали са имали затруднения да ги запомнят или да зададете това в онлайн платформа като въпрос за размисъл.

Стъпка 2:

Помолете участниците да проучат препоръките в интернет във връзка с добри пароли.

Те могат да напишат правилата в споделен документ или на работен лист (в този случай ги помолете да ви го изпратят), а вие като обучител можете да предоставите по-късно плакат с най-важните правила, които могат да бъдат споделени в резултат на работата на участниците. Участниците могат да отпечатаат тези правила и да ги запазят за насоки в бъдеще.

Подкрепете работата с постоянната си обратна връзка за най-важните елементи за научаване (вижте приложението).

Полезни връзки относно безопасност на паролата:

-  <https://edu.gcfglobal.org/en/internetsafety/creating-strong-passwords/1/>
-  <https://www.webroot.com/us/en/resources/tips-articles/how-do-i-create-a-strong-password>
-  <https://terravasecurity.com/how-to-create-a-strong-password-in-7-easy-steps/>
-  <https://www.rhsb.com/your-passwords-hackable/>

Стъпка 3:

Дайте на участниците прости методи (вижте по-долу) как да генерират и забелязват силни пароли. Представете примерите със собствени данни от фиктивно лице (напр.: Мария, 76-годишна жена, живееща в дом за възрастни във Виена, в къща номер 42, 4 внука, котка, любимата храна е виенски шницел, любим цвят - светло синьо).

Пример 1: MSchnitzelH42

- Помислете за любимата си храна или зеленчук (или специална дума).
- Разменете първата буква от него с първата буква от собственото си име.
- Променете последната буква на първата буква от вашето фамилно име. Добавете вашата възраст или номер на къща в началото или в края.
- Пример: „Мария Хубер“, чиято любима храна е „Шницел“ и живее на номер „42“.

Пример 2: 3!SaeK@60

- Опитайте с дума, която вашето дете/вашият внук не е можел да каже правилно като малко дете, напр. „сак“ вместо „заек“.
- Добавете числото на колко години е бил той/тя, например 3 и удивителен знак '!' --> 3!saek
- Направете първото „s“ главно „S“, а последното „k“ главно „K“ --> 3!SaeK
- След това добавете @60 в края, защото тогава сте били на 60. --> 3!SaeK@60

Пример 3: Ptdbpnmwn2M

- Методът на първата буква: Паролата **т**рябва **д**а **б**ъде **п**роменяна **н**ай-**м**алко **в**еднъж **н**а **2 М**есеца. --> Ptdbpnmwn2M
- За този пример можете да използвате фраза/цитат/ред от стихотворение и т.н., които вероятно никога няма да забравите в живота си.

Стъпка 4

Обсъдете с участниците в онлайн сесия какво трябва да направят, ако паролата им бъде използвана от някой друг или открадната. Основно злоупотребата с парола трябва да бъде докладвана незабавно на координатора на уебсайта, от който паролата е била открадната.

Проучете с участниците или ги насърчете да направят проучване как се разглеждат тези случаи в тяхната страна. Има държави, които имат Център за интернет сигурност, например, където тези проблеми могат да бъдат докладвани.

Препоръки за изпълнение

- » Възможно е вашите участници преди това да са използвали различни правила за работа с пароли (например те съхраняват пароли в мобилния си телефон/записват ги в бележник и ги държат на бюрото си или в Google Drive в документ, наречен „пароли и потребителски имена“). Те се нуждаят от повече търпение и време, за да разберат, че може би трябва да променят практиките си.

- » Насърчете отделянето на достатъчно време за практикуване на метод, който вашите участници могат да използват с увереност. Можете да ги попитате един по един дали могат да намерят добър работещ метод.
- » Можете да зададете напомняне в мобилните телефони или в календара заедно на всеки 2 месеца за смяна на най-важните пароли.

Въпроси за отразяване

- Намерихте ли метод, който ви помага да създавате силни пароли?
- Кой е най-добрият начин да запомните паролите си?
- Ще управлявате ли паролите си по различен начин в бъдеще? Как?



Деятност 2: Пазете личната информация в безопасност – истории за поверителността

Цели на практиката:

- Познаване на различните форми на киберпрестъпления
- Разпознаване на най-важните правила в контекста на сигурността на поверителността.
- Познаване разликата между защитени и незащитени мрежи
- Да знаете как да защитите поверителността си на открити пространства
- Да бъдете осъзнати относно онлайн дейностите и да постигнете по-безопасно онлайн изживяване

Материали/продължителност:

- Листи и химикалки за участниците
- Онлайн бяла дъска
- 1.5 - 2 часа

Изпълнение на дейността:

Стъпка 1 – Въведение

Тази дейност е предназначена или за начинаещи, които нямат много информация относно поверителността, или за по-възрастни хора, които може вече да са имали проблеми с тези ситуации. Дейността е подходяща и за идентифициране на общи правила за общност от възрастни хора.

Стъпка 2

В случай на сесия със самостоятелно темпо, помолете участниците да прочетат 3-те истории.

В случай на онлайн групова сесия, организирайте участниците в 3 групи. Дайте на отделните групи 1-1 описания на случаите (вижте приложението). Групите трябва да обсъдят обстойно историите, да отговорят на въпросите, свързани с тях. При индивидуална работа въпросите са същите.

Особено важно е как жертвите да избегнат нежелания инцидент следващия път.

Стъпка 3

Накарайте участниците да представят сценариите и своите подробни отговори в онлайн дискусия или на онлайн платформа. Ако работите с група, дайте възможност на участниците в другите групи да добавят към отговорите, ако намерят това за полезно. В случай на самостоятелно обучение, осигурете обратна връзка за вашите участници.

Стъпка 4

Помолете участниците да обобщят най-важните правила за поведение в поне 5 точки въз основа на сценариите, които могат да помогнат за избягване на подобни нежелани истории. Може да се споделя както обикновено в този модул.

Препоръки за изпълнение

- Ако знаете обстоятелствата на вашите участници, можете да пренапишете историите съответно.
- Ако вашите участници/група живеят заедно или се срещат редовно и имат социален работник, например в дом/клуб за възрастни хора, опитайте се да се консултирате с колеги, за да пренапишете сценариите според техните нужди.

Въпроси за отразяване:

- Научихте ли нещо полезно от тези истории? Бихте ли го обобщили накратко?
- Има ли правила, които бихте споделили на приятелите или познатите си?
- Кое правило е най-важно за вас?

Приложение към Дейност 2

Сценарий 1:

Борис се среща със старите си приятели и колеги в кафене два пъти седмично. Междувременно иска да обсъди нещо с други хора в социалните медии. Той влиза с простата си парола и междувременно произнася няколко букви на глас, за да се увери, че прави всичко добре. Приятелите му също гледат мобилния му телефон. По-късно отива до тоалетната и оставя мобилния си телефон на масата, защото не иска да го носи със себе си, за да не се намокри. Когато се връща приятелите му са заети да чатят по мобилния му телефон. Какво може да се случи след това?

Възможни отговори:

- Ако приятелите в чата не са споменали, че не са идентични със собственика на мобилния телефон, това може да доведе до неприятни недоразумения.
- Могат да се изпращат и подли съобщения.
- Важни връзки могат да бъдат изтрити или могат да бъдат направени нежелани такива.
- На отключен мобилен телефон може да се съхраняват важни данни, които могат да бъдат използвани от злонамерени злоупотребяващи за нежелани цели.

Препоръки:

- Никога не оставяйте мобилния си телефон без надзор.
- Използвайте силна парола.
- Никога не изговаряйте данните си на глас на обществени места.

Сценарий 2:

Силвия използва споделен лаптоп в общностно помещение. Георги е в същото пространство и има посетители, които тя не познава. Силвия влиза в лаптопа си, защото говори с приятелите си онлайн и иска да сподели снимки от почивката с внуците си. Даниеле и Михаил, посетителите я гледат през цялото време. След час Силвия иска да изпие чаша вода и отива в кухнята. Тя оставя лаптопа си на масата. Тя си казва няколко думи с останалите в кухнята и се връща след 10 минути. Вечерта тя вече е получила 6 съобщения от приятелите си, питащи какво ѝ е и защо им е изпратила такива неприятни съобщения след приятния следобеден разговор. Какво може да се е случило?

Възможни отговори:

- Посетителите не знаят или не одобряват правилата на общността, така че вероятно са изпратили съобщения на приятелите на Силвия.
- Силвия най-вероятно не се е отписала от чата.
- Тя вероятно няма парола за отключване на лаптопа си или паролата е твърде слаба.

Препоръки:

- Никога не оставяйте личните си устройства без надзор.
- Използвайте силна парола.
- Обявявайте правилата на общността в открити пространства.

Сценарий 3

Доротея отива с приятелката си в приятен ресторант с градина за обяд. Има само няколко места, така че двама мъже ги канят да седнат в другия край на дългата маса. Те искат да се пошегуват с Доротея и приятелката ѝ, но искат само да си говорят. След 15 минути те имат възможност да седнат на друга малка маса и да оставят мъжете. Но малко по-късно Доротея забеляза, че е оставила чантата с мобилния си телефон на

другата маса. Тя няма сложен код (1234) и онлайн приложението на нейната банка е отворено, защото тя е проверявала дали има достатъчно пари в сметката си точно преди обяд. Какво може да се случи след това?

Възможни отговори:

- За съжаление в този случай всички данни за вход могат да бъдат откраднати, а в най-лошия случай банковите данни на Доротея могат да бъдат използвани за прехвърляне на парите и сметката ѝ изцяло в друга сметка или за редовно плащане на малки или големи суми оттук. Тя трябва незабавно да промени всички данни за вход, евентуално да забрани използването на акаунта за кратко време.

Препоръки:

- Никога не оставяйте личните си устройства без надзор!
- Използвайте силна парола!
- Ако не сте сигурни, че винаги можете да контролирате устройствата си, не използвайте чувствителни приложения на открито (напр. онлайн банкиране и други важни онлайн услуги) и излизайте от профила си когато приключите с използването им. В този случай никога не съхранявайте пароли на личното си устройство.



Дейност 3: Онлайн банкиране без страх

Цели на практиката:

- Да се осъзнаят предимствата на онлайн банкирането.
- Да разпознаят възможностите на онлайн банкирането.
- Да се разбере важността на основните правила на онлайн банкирането, за да бъдем информирани потребители.

Материали/продължителност:

- Компютри или персонални устройства (смартфони, таблети, лаптопи и др.) с достъп до интернет
- Маркер, листи, химикалки за участниците
- Мин. 2 часа

Изпълнение на дейността:

Стъпка 1 – Въведение

Възрастните хора често се страхуват от онлайн банкирането, тъй като този подход изглежда твърде опасен за тях. Така че нашата цел е в първата стъпка да потвърдим и да се доближим до техните страхове, за да разберем при какви обстоятелства трябва да работим.

Обяснете целта и учебните цели на тази дейност и обърнете внимание на препоръките.

Стъпка 2

Помолете участниците да формират малки групи. Тези малки групи трябва да обсъдят и съберат какви предимства и недостатъци/рискове на онлайн банкирането знаят. Може да

бъде написано от участниците, на онлайн бяла дъска/маса/шаблон, или можете да ги помолите да отговорят на този въпрос индивидуално.

Ако имате възможност, можете да обсъдите всеки от тези коментари с групата в дискусиата.

Стъпка 3

Помолете всички участници да проучат видеоклипове в интернет за онлайн банкиране. Събраната информация може да бъде добавена към списъка, създаден в стъпка 2.

Стъпка 4

Насърчете участниците да изберат няколко банкови институции, с чиято онлайн система биха искали да се запознаят. Разбира се, можете да изберете опцията за онлайн банкиране на тяхната индивидуална банка, която те познават добре от дълго време. Препоръчва се проучване на онлайн уроци. Според нивото на знания те могат да го направят сами или вие можете да им ги предоставите.

Стъпка 5

Направете резюме на правилото за безопасност.

Подчертайте какво може и какво не може да се изисква от банковите институции или, в случай на онлайн пазаруване, от потребителите.

Изложете това правило по привлекателен начин и го разпространете в групата (напр. редактирайте общ плакат и го предоставете като обучител и споделете с участниците онлайн).

Пример: Онлайн банкиране без страх

Какво мога да направя, за да запазя парите и самоличността си в безопасност?

Като цяло онлайн банкирането е безопасно, но има стъпки, които можете да предприемете, за да се грижите за парите и самоличността си:

- » **Използвайте силна парола**, която избягва общи думи, цифри или модели на клавиатурата (като „парола“ или „123456“). Не включвайте лична информация, като вашето име, дата на раждане или подробности за член на семейството във вашата парола. Щракнете тук, за да научите повече за това как да изберете силна парола.

- » **Не използвайте повторно пароли** за различни акаунти.
- » **Никога не споделяйте пълната си парола** или ПИН код.
Банките никога няма да поискат пълния ви ПИН или парола – вместо това те ще поискат конкретни цифри или букви, например първия и третия знак.
- » **Винаги излизайте от сесията си за онлайн банкиране**, особено ако използвате споделено устройство. Ако използвате обществен компютър, като компютър в библиотека, бъдете особено внимателни – може да няма достатъчно ниво на сигурност. Ако имате нужда, попитайте персонала на библиотеката за повече информация.
- » **Използвайте само защитени Wi-Fi мрежи** за достъп до вашето онлайн банкиране. Ако използвате обществена мрежа, като например в кафенета или гари, може да е възможно хората в същата мрежа да получат достъп до вашите данни.
- » **Проверявайте редовно баланса и транзакциите си**. Ако има транзакция, която не разпознавате, докладвайте незабавно на банката си.

- » **Редовно проверявайте дали вашите лични данни са правилни и актуални.**

Полезна връзка:

 [Онлайн банкиране за възрастни хора | Възраст Великобритания](#)

Стъпка 6

Обсъдете въпроси за размисъл с участниците.

Препоръки за изпълнение:

- » Целта на тази дейност е преди всичко не да убеди участниците да изберат онлайн банкиране, а да даде информация за преодоляване на страховете им от тази техника, да покаже нова перспектива и да даде възможност на отворените хора да използват онлайн банкирането, след като са се подготвили задълбочено.
- » Ако имате възможност, можете да проведете последващи семинари, на които участниците, изпробвали онлайн банкирането, да споделят своите първи впечатления.

Въпроси за отразяване:

- Чувствате ли се по-сигурни, когато мислите за онлайн банкиране сега?
- По-ясно ли ви е онлайн банкирането?
- Какво мислите, бихте ли могли да банкирате онлайн сега с повече увереност?
- Ако бихте искали да пробвате онлайн банкиране, кого можете да помолите за помощ/подкрепа?



Поздравления за завършването на Модул 9 – Медийна грамотност и поверителност!

Не забравяйте, че като сте информирани, използвате сигурни практики и внимавате за вашите онлайн дейности, можете да минимизирате потенциалните рискове и да постигнете безопасно онлайн изживяване.

Съветваме ви да продължите с урок 10. Успех!





ПРИЛОЖЕНИЕ към Модул 9

Медийна грамотност и поверителност

Тест за входно ниво

Въпрос 1: Безопасно е да използвате една и съща парола за няколко онлайн акаунта.

- a. Вярно
- b. Невярно

Въпрос 2 - Кое от следните е препоръчителна практика за защита на личната информация онлайн?

- a. Споделяне на лична информация в социални медийни платформи.
- b. Съхраняване на лична информация, запазена на обществени компютри.
- c. Редовно актуализиране на настройките за поверителност на акаунтите в социалните медии.
- d. Щракване върху неизвестни прикачени файлове към имейл.

Въпрос 3: Онлайн банкирането не е безопасно за възрастни хора.

- a. Вярно
- b. Невярно

Въпрос 4: Настройките за поверителност позволяват на хората да контролират кой има достъп до тяхната лична информация в социалните медийни платформи.

- a. Вярно
- b. Невярно

Тест за изходно ниво

Въпрос 1: Настройките за поверителност и разрешенията, като бисквитки, нямат влияние върху защитата на личната информация онлайн.

- a. Вярно
- b. Невярно

Въпрос 2: Кое от следните НЕ е основно правило за гарантиране на онлайн поверителност и защита на личната информация?

- a. Избягване споделянето на лична информация в социалните медийни платформи
- b. Използване на силни и уникални пароли за различни онлайн акаунти
- c. Кликване върху подозрителни връзки или изтегляне на файлове от неизвестни източници
- d. Поддържане на актуализиран софтуер и антивирусни програми

Въпрос 3: Онлайн банкирането е безопасна и сигурна опция за възрастните хора и те трябва да се чувстват уверени да го използват.

- a. Вярно
- b. Невярно

Въпрос 4: Кое от следните действия може да помогне за защитата на личните данни?

- a. Използване на една и съща парола за множество онлайн акаунти.
- b. Споделяне на лична информация в социални медийни платформи.
- c. Отваряне на прикачени файлове към имейл или щракване върху подозрителни връзки.
- d. Редовно актуализиране на пароли и използване на силни, уникални пароли за всеки онлайн акаунт.



ОТГОВОРИ НА ТЕСТОВЕТЕ:

ТЕСТ ВХОДНО НИВО

Верни отговори:

Въпрос 1: а) Невярно

Въпрос 2: с) Редовно актуализиране на настройките за поверителност на акаунтите в социалните медии .

Въпрос 3: b) Невярно

Въпрос 4: а) Вярно

ТЕСТ ИЗХОДНО НИВО

Верни отговори:

Въпрос 1: b) Невярно

Въпрос 2: с) Кликване върху подозрителни връзки или изтегляне на файлове от неизвестни източници

Въпрос 3: а) Вярно

Въпрос 4: d) Редовно актуализиране на пароли и използване на силни, уникални пароли за всеки онлайн акаунт.



information matters

contact@informationmatters.eu

Финансирано от Европейския съюз. Изразените възгледи и мнения обаче принадлежат изцяло на техния(ите) автор(и) и не отразяват непременно възгледите и мненията на Европейския съюз или на Европейската изпълнителна агенция за образование и култура (EACEA). За тях не носи отговорност нито Европейският съюз, нито EACEA.

Номер на споразумението: 2022-1-BG01-KA220-ADU-000085514



**Съфинансирано от
Европейския съюз**