



**information
matters**

Тренировъчна програма **за онлайн курсове**

Модул 6

Медийна грамотност и дигитални услуги



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	3
Цел	8
Ключови думи	9
Предмет	9
Основни дефиниции	10
Полезни връзки	12
Валидиране на модула	13
Оценка на модула	14
Дейност 1: „Обучение за дигитален детектив“	15
Цели на обучението:	15
Обстановка/материал/продължителност:	16
Изпълнение на дейността:	16
Въпроси за отразяване	20
Поздравления за завършването на Модул 6!	21
ПРИЛОЖЕНИЕ към Модул 6	22
ОТГОВОРИ НА ТЕСТОВЕТЕ	25



Въведение

Добре дошли в Модул 6 от нашия курс. В този урок ще разгледаме темата как да бъдем по-безопасни онлайн, как да запазим поверителността си, как да извършваме сигурни онлайн плащания и някои основни понятия, свързани с темата. Нека видим някои основни определения.



Безопасността се отнася до състоянието на сигурност от потенциална вреда, опасност или риск. Той включва мерки и практики, прилагани за предотвратяване на злополуки, наранявания или каквато и да е форма на увреждане на лица, имущество или информация. Безопасността може

да бъде физическа, емоционална или дигитална и включва идентифициране и смекчаване на потенциални опасности. В контекста на технологиите безопасността може да включва мерки за защита на потребителите от киберзаплахи, гарантиране на надеждността на дигиталните системи и осигуряване на сигурна онлайн среда.



Поверителността е състояние на свобода от неоторизирано проникване или намеса в личния живот, дейности или информация. То включва правото на лицата да контролират достъпа и използването на своите лични данни. Поверителността може да бъде физическа, като правото да бъдеш свободен от наблюдение, или дигитална, по отношение на защитата на личната информация онлайн.

В дигиталната ера опасенията за поверителността често се въртят около събирането, съхранението и споделянето на лични данни от организации, уебсайтове и онлайн платформи. Мерките за поверителност имат за цел да защитят автономността на индивида и да предотвратят неоторизиран достъп до чувствителна информация.



Сигурните методи за онлайн плащане

се отнасят до електронни транзакции, извършвани чрез интернет, които дават приоритет на защитата на чувствителна финансова информация, като гарантират поверителността, целостта и автентичността на процеса на плащане. Тези методи използват усъвършенствани технологии за криптиране и протоколи за сигурност за защита на финансовите данни на потребителите, предотвратявайки неоторизиран достъп и измамни дейности.

Основните характеристики на сигурните онлайн методи за плащане включват:

- **Шифроване:** Използването на алгоритми за криптиране за кодиране на финансова информация по време на предаване, което я прави нечетима за неоторизирани страни. Secure Sockets Layer (SSL) и Transport Layer Security (TLS) са общи протоколи за криптиране.
- **Токенизация:** Замяната на чувствителни данни с уникален идентификатор или токен. Това помага за защитата на действителните финансови подробности, тъй като дори и да бъде прихванат, токенът няма значима информация.
- **Двуфакторно удостоверяване (2FA):** Допълнителен слой на сигурност, изискващ от потребителите да предоставят две форми на идентификация, преди да извършат транзакция. Това често включва парола и временен код, изпратен до мобилното устройство на потребителя.
- **Шлюзове за защитени плащания:** Шлюзовете за плащане действат като посредници между уебсайта на търговеца и финансовата институция, като сигурно обработват транзакциите. Уважаваните и сигурни шлюзове за плащане се придържат към индустриалните стандарти за защита на данните.

- **Откриване и предотвратяване на измами:** Внедряване на инструменти и алгоритми за откриване и предотвратяване на измамни дейности, като необичайни модели на покупка или множество неуспешни опити за влизане.
- **Съответствие със стандартите:** Придържане към индустриалните стандарти и разпоредби, като стандарта за сигурност на данните в сектора на разплащателните карти (PCI DSS), който установява изисквания за обработка на информация за кредитни карти.
- **Образование на клиентите:** Предоставяне на информация и най-добри практики на потребителите за поддържане на сигурни онлайн практики, включително важността на силните пароли, избягване на обществен Wi-Fi за чувствителни транзакции и редовно наблюдение на финансовите извлечения.



Цел

Пазаруване, медицински консултации, искане за общински услуги - с нарастващата дигитализация много ежедневни дейности станаха по-сложни за по-малко дигитално грамотните. Възрастните хора често имат затруднения при използването на онлайн банкиране, резервиране, пазаруване и гледане на филми в онлайн стрийминг, играене на игри и достъп до здравни онлайн услуги.

Необходимо е да се развият нови умения за участие в обществения живот (избори, политически дебати онлайн), икономически дейности (като покупка/продажба на стоки и услуги) и социално включване (личен обмен, дистанционно обучение по физически упражнения или други подобни).

Резултати от обучението

След завършване на този модул участниците трябва да демонстрират повишена увереност в онлайн пазаруването, достъпа до медицински консултации и безопасното използване на банкови услуги. Те също така трябва да могат да навигират в услугите за резервации, развлечения и достъп до игри. Те ще могат да разберат как да участват с по-голяма лекота в онлайн общностите и обществения живот.

Ключови думи

Дигитални услуги, онлайн общности, банкиране, резервации, пазаруване, търсене, стрийминг, игра, онлайн медицински консултации.

Предмет

Достъп до свързани устройства и дигитални платформи. Покритите теми включват пазаруване, онлайн забавления, активно участие в общността, проучване на онлайн здравни ресурси и т.н. Разбиране на безопасността и поверителността, включително сигурни методи на плащане, разпознаване на измами и финансови измами.

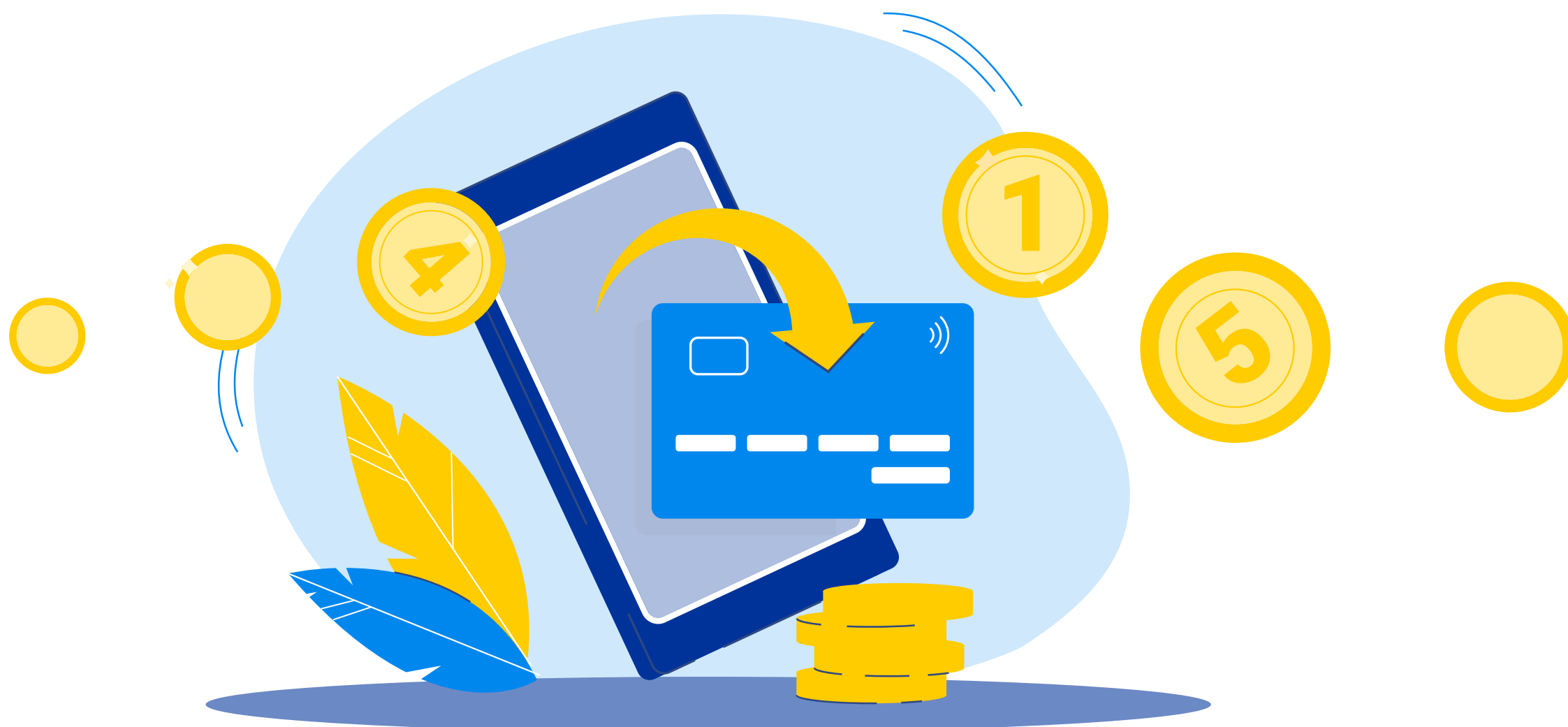


Основни дефиниции

- 1. Безопасността** се отнася до състоянието на сигурност от потенциална вреда, опасност или риск. Тя включва мерки и практики, прилагани за предотвратяване на злополуки, наранявания или каквато и да е форма на увреждане на лица, имущество или информация. Безопасността може да бъде физическа, емоционална или дигитална и включва идентифициране и смекчаване на потенциални опасности. В контекста на технологиите безопасността може да включва мерки за защита на потребителите от киберзаплахи, гарантиране на надеждността на дигиталните системи и насърчаване на сигурна онлайн среда.
- 2. Поверителността** е състояние на свобода от неоторизирано проникване или намеса в личния живот, дейности или информация. То включва правото на лицата да контролират достъпа и използването на своите лични данни. Поверителността може да бъде физическа, като правото да бъдеш свободен от наблюдение, или дигитална, по отношение на защитата на личната информация онлайн. В дигиталната ера опасенията за поверителността често се въртят около събирането, съхранението и споделянето на лични данни от организации, уебсайтове и онлайн

платформи. Мерките за поверителност имат за цел да защитят автономността на индивида и да предотвратят неоторизиран достъп до чувствителна информация.

3. Сигурните онлайн методи за плащане се отнасят до електронни транзакции, извършвани чрез интернет, които дават приоритет на защитата на чувствителна финансова информация, като гарантират поверителността, целостта и автентичността на процеса на плащане. Тези методи използват усъвършенствани технологии за криптиране и протоколи за сигурност за защита на финансовите данни на потребителите, предотвратявайки неоторизиран достъп и измамни дейности.



Полезни връзки

Дигитализация на услугите: осигуряване на равен достъп за всички, включително възрастните хора днес и утре

 <https://www.age-platform.eu/special-briefing/digitalisation-services-ensuring-equal-access-all-including-older-people-today-and>

Как можем да осигурим дигитално включване на възрастните хора?

 <https://www.weforum.org/agenda/2021/10/how-can-we-ensure-digital-inclusion-for-older-adults>

Senior Planet и AARP предлагат безплатни онлайн класове за приложения:

 <https://www.digitallearn.org>

 www.aarp.org/home-family/personal-technology/info-2021/senior-planet-and-aarp-online-classes.html

Making It Click: Подкрепа за хора с ниско потребление на интернет:

 <http://www.goodthingsfoundation.org/insights/making-it-click-supporting-people-with-low-internet-use>

Валидиране на модула

В края на модула обучаемите ще са научили как да проверяват безопасността на уебсайт и как да разбират кои сайтове не са безопасни.

Знания:

Обучаемите ще са в състояние да

- Проверяват безопасността на уебсайт
- Разбират кои сайтове са безопасни и кои не
- Имат представа за безопасни уебсайтове и тяхното използване

Умения:

Обучаемите са в състояние да

- Идентифицират основните аспекти на безопасността на уебсайта
- Проверяват безопасността на уебсайтовете, които посещават
- Правят разликата между безопасни и опасни уебсайтове

Компетенции:

Обучаемите са в състояние да

- Разбират онлайн безопасността
- Идентифицират основните точки на онлайн безопасността, свързани с уебсайт

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



Дейност 1: „Обучение за дигитален детектив“

Цели на обучението:

- Подобрете уменията на участниците за идентифициране и борба с мисинформацията онлайн чрез практическа, интерактивна дейност.



Обстановка/материал/продължителност:

- Устройства, свързани с интернет (лаптопи, таблети или настолни компютри)
- Достъп до уеб браузър
- Списък с избрани уебсайтове (някои надеждни и някои съдържащи мисинформация)

Изпълнение на дейността:

Стъпка 1 – Въведение:

(15 минути)

- Започнете с кратка презентация за разпространението на дезинформацията онлайн и нейното въздействие.
- Подчертайте значението на проверката на фактите и критичната оценка в дигиталната ера.

Стъпка 2 – Разбиране на надеждните източници

(20 минути)

- Предоставете списък с надеждни уебсайтове, които са известни с точна и достоверна информация (напр. уебсайтове за проверка на факти, реномирани новинарски издания).
- Обсъдете критериите, които правят тези източници надеждни (достоверност, прозрачност, стандарти за проверка на фактите).

Стъпка 3 – Идентифициране на дезинформация

(30 минути)

- Въведете списък с уебсайтове, които съдържат дезинформация или са известни с разпространението на невярна информация.
- Насърчете участниците да проучат тези уебсайтове, търсейки признаци на дезинформация (сензация, липса на достоверни източници, пристрастен език).
- Обсъдете често срещаните предупредителни знаци, свързани с мисинформацията.

Стъпка 4 – Интерактивна проверка на фактите

(40 минути)

- Предоставете на участниците конкретни твърдения или новинарски статии както от надеждни, така и от ненадеждни източници.
- Задайте на участниците проверка на фактите на твърденията, като използват уважавани уебсайтове за проверка на факти.
- Обсъдете резултатите като група, като наблегнете на важността на проверката на информация от много различни източници.

Стъпка 5 – Групова дискусия

(15 минути):

- Направете групова дискусия относно предизвикателствата и стратегиите, възникнали по време на процеса на проверка на фактите.
- Насърчете участниците да споделят съждения и съвети за разграничаване между надеждни и ненадеждни източници.

Стъпка 6 – Споделяне на ресурси

(20 минути):

- Накарайте участниците да съставят списък с полезни уебсайтове и инструменти за проверка на фактите и идентифициране на мисинформация.
- Споделете съставения списък с групата и обсъдете как тези ресурси могат да бъдат включени в техните ежедневни онлайн дейности.

Стъпка 7 – Размисъл и въпроси и отговори

(15 минути):

- Завършете сесията с размисли върху ключовите изводи и наученото.
- Отворете дискусията за въпроси и предоставете допълнителни ресурси за по-нататъшно обучение.

Последващи действия:

Насърчете участниците да продължат да упражняват уменията си за проверка на факти, като се ангажират редовно с надеждни уебсайтове за проверка на факти. Освен това споделете списък с подобни източници на новини и инструменти за проверка на факти, които те могат да интегрират в своята онлайн рутина.

Тази дейност не само подобрява способността на участниците да идентифицират дезинформация, но също така ги оборудва с практически умения за отговорно навигиране в дигиталния пейзаж.

Въпроси за отразяване

- Всички уебсайтове безопасни ли са?
- Как можем да идентифицираме уебсайт като небезопасен?
- Какво да правим, когато видим, че даден уебсайт не е безопасен?

Поздравления за завършването на Модул 6!

Този урок предостави кратък преглед на безопасността, поверителността и финансите онлайн. Надяваме се, че сега се чувствате по-подготвени за дигиталния свят.

Съветваме ви да продължите с урок 7. Успех!





ПРИЛОЖЕНИЕ към Модул 6

Медийна грамотност и дигитални услуги

Тест за входно ниво

Въпрос 1: Онлайн пазаруването може да осигури удобство и достъп до широка гама от продукти за възрастни хора.

- a. Вярно
- b. Невярно

Въпрос 2: Кое от следните НЕ е пример за онлайн забавление за възрастни хора?

- a. Гледане на филми или сериали онлайн
- b. Играене на игри в платформи за социални медии
- c. Участие във виртуални обиколки на музеи и забележителности
- d. Посещение на онлайн курсове или вебинари

Въпрос 3: Активното участие в общността чрез онлайн платформи може да помогне на възрастните хора да поддържат връзка с другите и да се борят със самотата.

- a. Вярно
- b. Невярно

Въпрос 4: Кое от следните НЕ е препоръчително действие за разпознаване на измами и финансови престъпления при използване на дигитални услуги?

- a. Предоставяне на лична или финансова информация на неизвестни лица или уебсайтове
- b. Проверка за защитени връзки към уебсайтове (https://) при извършване на онлайн плащания
- c. Внимание при нежелани имейли или телефонни обаждания с искане за лична или финансова информация
- d. Четене на онлайн отзиви и обратна връзка, преди да направите покупки

Тест за изходно ниво

Въпрос 1: Пазаруването онлайн е по-безопасно от пазаруването във физически магазини.

- a. Вярно
- b. Невярно

Въпрос 2: Кое от следните НЕ е пример за онлайн забавление?

- a. Стрийминг на филми и телевизионни предавания
- b. Играене на онлайн игри
- c. Присъединяване към социални медийни платформи
- d. Четене на дигитални новинарски статии

Въпрос 3: Активното участие в общността може да бъде улеснено чрез онлайн платформи.

- a. Вярно
- b. Невярно

Въпрос 4: Кое е важно съображение, когато изследвате онлайн здравни ресурси?

- a. Проверка на достоверността на източниците
- b. Споделяне на лична медицинска информация онлайн
- c. Игнориране на потребителски отзиви и обратна връзка
- d. Избягване на достоверни уебсайтове за здравеопазване

ОТГОВОРИ НА ТЕСТОВЕТЕ

ТЕСТ ЗА ВХОДНО НИВО

Верни отговори:

Въпрос 1: а) Вярно

Въпрос 2: с) Посещение на онлайн курсове или уебинари

Въпрос 3: а) Вярно

Въпрос 4: г) Предоставяне на лична или финансова информация на неизвестни лица или уебсайтове

ТЕСТ ЗА ИЗХОДНО НИВО

Верни отговори:

Въпрос 1: б) Невярно. Въпреки че онлайн пазаруването може да бъде удобно, важно е да бъдете внимателни и да гарантирате легитимността и сигурността на използваните уебсайтове и платформи.

Въпрос 2: с) Четене на дигитални новинарски статии. Онлайн забавлението обикновено се отнася до дейности като стрийминг, игри и ангажираност в социалните медии.

Въпрос 3: Вярно. Онлайн платформите предоставят възможности на хората да се ангажират със своите общности, да участват в дискусии, да се присъединят към групи по интереси и да допринесат за различни каузи.

Въпрос 4: а) Проверка на достоверността на източниците. От решаващо значение е да проверите надеждността и репутацията на онлайн здравните ресурси, преди да разчитате на тях за точна информация.





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**