Участвайте безопасно и отговорно онлайн

26 минути

В тази пътека за обучение ще ви запознаят с рисковете за безопасността, които можете да направите, докато използвате интернет. Вие ще научите за онлайн измами и как да ги избегнете. Ще научите и за най-добрите практики за споделяне на информация онлайн. В допълнение, ще бъдат въведени в кибертормоз.

# Онлайн безопасност и поверителност

17 минути | 8 единици

В този модул ще научите за някои от рисковете за безопасността, които могат да ви повлияят, когато използвате интернет, и съвети за безопасна работа и поддържане на информацията ви онлайн.

## Защитете се от фишинг

3 минути

### Защитете се от фишинг

Въпреки че има много положителни неща, които можем да направим онлайн, винаги трябва да сме наясно с рисковете за безопасността. Има много измами, които онлайн хищници използват за достъп до информация на хората онлайн.

Трябва да сте наясно с тези измами, за да можете да направите всичко възможно, за да ги избегнете. **Фишинг**  е обща онлайн измама, която трябва да знаете.

**Гледайте следното видео, за да научите повече за фишинг и как да се предпазите от тази онлайн измама.**

### Видео: Защитете се от фишинг

Интернет ни предоставя множество възможности. Можем да говорим с други хора, да правим покупки онлайн и да вършим лични дела от едно място. Но тези онлайн взаимодействия невинаги са безопасни. Нека поговорим за популярна онлайн измама, за която трябва да знаете. Често срещан начин за ловене на риба е да се сложи храна на кука, така че рибата да иска да я изяде. Захапе ли храната, ще бъде закачена. Фишинг измамите в интернет работят по същия начин. Хората, които искат да откраднат информацията ви, са като рибари. Изпращат ви имейл или незабавно съобщение чрез сайт на социална мрежа или онлайн игра. Те често се представят за някой друг и искат от вас лична информация или ви казват да щракнете върху хипервръзка, за да можете да завършите важна задача. Ако им дадете информацията или щракнете върху хипервръзката, ще бъдете „закачени“. Но не се притеснявайте. Тези четири практики могат да ви предпазят от фишинг измами. Практика номер едно: внимавайте за съмнителни съобщения. Измамниците се опитват да направят съобщенията им да изглеждат официални и познати, за да им се доверите. Помислете добре, когато получите подозрително съобщение, и избягвайте да споделяте лична информация чрез съобщение или имейл. Това включва домашния ви адрес, банкова информация, пароли и други. Не щраквайте върху връзка и не изтегляйте файл, ако не познавате или не се доверявате на подателя. Практика номер две: потърсете знаци, че дадена уеб страница е безопасна и сигурна. Преди да предоставите информация за кредитна карта, да въведете парола или да предоставите друга лична информация, уверете се, че се намирате в надежден и защитен уеб сайт. Повечето защитени уеб сайтове имат префикс https в началото на URL адреса в адресната лента на браузъра. Също така се уверете, че се намирате в правилната уеб страница. Измамниците често се опитват да ви препратят към уеб страници, които изглеждат официални и използват правописни грешки в имената на компаниите, за да ви измамят. www.microsoft.net не е същото като официалния уеб сайт на Microsoft на www.microsoft.com. Винаги проверявайте URL адреса, за да се уверите, че се намирате в правилната уеб страница. Практика номер три: поддържайте уеб браузъра си и операционната си система актуални. Можете да включите автоматичните актуализации, за да се уверите, че най-новите софтуерни версии се инсталират автоматично на компютъра ви. Поддържането на софтуера на устройството ви актуален означава, че ще получавате най-новите актуализации на защитата, които ще ви помогнат да предпазите компютъра си. Практика номер четири: инсталирайте потвърден софтуер за защита от злонамерен софтуер на устройствата си. Това е специален софтуер, създаден да предпази компютъра ви от вреден софтуер и хакери. Не бъдете следващата риба, хваната на кукичката. Когато използвате интернет, не забравяйте да мислите, преди да щракнете, изтегляте или споделяте, за да се предпазите от фишинг измами онлайн.

## Комуникирайте безопасно онлайн

2 минути

### Комуникирайте безопасно онлайн

Интернет ни позволява да общуваме с други хора по нови начини. Въпреки това, не винаги е безопасно да общуват с други хора онлайн. Не винаги знаете със сигурност на кого говорите, когато сте в интернет, така че трябва да внимавате да бъдете в безопасност.

**Гледайте следното видео, за да научите как да общувате безопасно онлайн.**

### Видео: комуникация безопасно онлайн

Използвайки интернет, можем да общуваме с други хора по света по нови начини. Това има множество предимства, но крие и някои опасности. Има онлайн хищници, които използват интернет всеки ден. Тези хищници често се преструват за други хора. Така че може да е трудно да узнаете с кого говорите онлайн. Ето три съвета, които можете да използвате, за да се предпазите от онлайн хищници, когато общувате онлайн. Съвет номер едно: използвайте инстинктите си. Ако някой ви изнервя или ви кара да се чувствате неловко, спрете да общувате с него и незабавно кажете на някого, на когото имате доверие. Повечето уеб сайтове и сайтове на социални мрежи имат инструменти, които можете да използвате, за да докладвате подозрителна дейност. Съвет номер две: ограничете нещата, които споделяте. Онлайн хищниците често се опитват да ви накарат да споделите личната си информация чрез имейли и съобщения. Избягвайте да споделяте лична информация с непознати онлайн. Съвет номер три: поддържайте дистанция. Обмислете внимателно дали да се срещнете с някого на живо, с когото сте говорили само онлайн. Онлайн хищниците често използват социални мрежи, за да се представят за някой друг, като създават фалшиви профили и използват снимките на други хора. Дори и някой да изглежда дружелюбен, може да е трудно да се уверите със сигурност с кого говорите онлайн. Винаги казвайте на родител или на някого, на когото имате доверие, когато онлайн непознат поиска да се видите на живо, за да не се окажете в опасна ситуация. Много онлайн хищници използват интелигентни тактики, за да ви примамят в опасни ситуации, но вие можете да сте по-умни. Имайте предвид тези рискове и съвети, за да сте в безопасност, когато говорите с други хора онлайн.

## Създаване на силни пароли

2 минути

### Създаване на силни пароли

Голяма част от безопасното съхранение и съхраняването на информацията ви онлайн е защитата на вашата информация, профилите и компютъра ви чрез силни пароли.

**Гледайте следното видео, за да научите как да създавате силни, ефективни пароли, които могат да защитят вашата информация.**

### Видео: създаване на силни пароли

Паролите защитават личната ви информация и акаунтите ви от други хора. Паролата е също толкова важна, колкото е ключалката на вратата. Искате силна ключалка, която трудно се чупи и ще пази опасните хора да не влязат в дома ви. Също така не искате никой да намери ключовете за ключалката ви. Силната парола е като силна ключалка за акаунта ви, искате да бъде трудна за отгатване за останалите, искате да бъде и безопасна и защитена, за да може другите да не я открият. Следвайте тези съвети, за да създадете силни пароли, и ги пазете. Съвет номер едно: използвайте комбинация от букви, цифри и символи в паролата си. Използването на комбинация от главни и малки букви и символи и добавянето на цифри може да подобри силата на паролата ви. Съвет номер две: избягвайте използването на често срещани думи в паролата си. Това включва често срещани думи и фрази като „парола“ или „уеб сайт“, както и лични ключови думи като рождения ви ден, името ви или родния ви град. Хакерите лесно могат да отгатнат тези фрази в паролата ви. Уникалната комбинация от символи и цифри създава по-силна парола. Съвет номер три: използвайте различни пароли за различните акаунти. Ако някой отгатне паролата за имейла ви, безопасността и поверителността ви може да са застрашени, ако използвате същата парола за банковата си сметка. Вместо това използвайте различни пароли за всеки онлайн акаунт, който имате. Съвет номер четири: вашата парола е само и единствено за вас. Когато я споделяте с други хора, дори приятели и роднини, е по-вероятно някой друг да я използва или да не остане в безопасност. Пазете паролите си за себе си. Когато влизате в акаунти, не забравяйте да излезете, когато сте готови, и не записвайте данните си за вход на обществени компютри. Освен това избягвайте вършенето на лични дела на обществени компютри и обществени мрежи, това улеснява хакерите в осъществяването на достъп до информацията ви. Не забравяйте, че използването на силни пароли и поддържането им защитени е важно за онлайн безопасността ви и поверителността ви. Не забравяйте тези съвети, когато създавате нова парола.

## Опишете най-добрите практики за споделяне на информация онлайн

2 минути

### Бъдете умни, когато споделяте

Когато отидем онлайн, често можем да направим много неща, които заплашват нашата безопасност, без да мислим много за него. Важно е да помислите два пъти за това, което споделяте онлайн и да поддържате вашата безопасност в ума.

**Гледайте следното видео, за да научите повече за рисковете от прекомерното споделяне онлайн.**

### Видео: Свръхсподеляне онлайн

Интернет и мрежата ни дават възможност да бъдем свързани с приятели и роднини по целия свят. Можем да използваме социалните мрежи и други платформи, за да видим какво се случва в живота на приятелите ни, да споделяме лични новини и да поддържаме връзка с други хора, но споделянето на неща онлайн невинаги е безопасно. Помислете за следния сценарий: Харолд си взема нова кола и иска приятелите му да я видят. Така че публикува нейна снимка в социална мрежа. Това може да изглежда нормално, но снимката включва множество лична информация за Харолд. Всеки може да види регистрационния му номер, каква кола кара и къде живее само от една снимка. Може да няма проблем приятелите му да видят това, но може да е опасно, ако грешният човек разбере тази информация и иска да я използва по лош начин. Важно е да мислим за безопасността и поверителността, когато споделяме неща онлайн. Когато създавате профили в уеб сайтове на социални мрежи, не забравяйте да преглеждате настройките за поверителност на акаунта си. Ако профилът ви е публичен, всеки може да види информацията ви и какво споделяте. Вместо това използвайте настройката за поверителен акаунт, за да може само личните ви връзки да виждат какво споделяте. Също така подбирайте внимателно, когато приемате покани за свързване с някого чрез социални мрежи. Повечето платформи на социални мрежи имат начин да приемате и да отхвърляте заявки някой да бъде ваш приятел или последовател в сайта. След като приемете някого, този човек има директен достъп до профила ви и нещата, които споделяте. Имайте това предвид, когато получавате заявки и се уверете, че взаимодействате само с хора, които познавате и на които се доверявате. Дори когато контролирате кой има достъп до вашите профили и акаунти, не можете да контролирате какво правят другите хора с информацията ви. Когато споделяте нещо онлайн, не можете да го изтриете. Никога не споделяйте нещо онлайн, което не бихте искали да бъде видяно публично и от непознати. Винаги мислете, преди да споделите. Не забравяйте за безопасността си и правете интелигентни избори, когато споделяте неща онлайн.

### Опитайте го сами

Какво научихте от това видео? Записвайте 1-3 неща, които ще имате предвид, когато споделяте лична информация онлайн.

## Опишете важността на управлението на вашия цифров отпечатък

3 минути

### Цифровият ви отпечатък

Има много неща, които можем да направим онлайн, от сърфиране в интернет, за споделяне на актуализации в социалните медии, за извършване на онлайн покупки. Трябва да имате предвид, че всичко, което правите онлайн, става част от вашата онлайн история или **цифровия ви отпечатък**.

Трябва да помислите за цифровия си отпечатък, когато споделяте информация или правите неща онлайн, защото нещата, които се случват онлайн, са трудни за изтриване.

**Гледайте следното видео, за да научите повече за цифровия си отпечатък и как да го управлявате.**

### Видео: Управлявайте цифровия си отпечатък

Ако използвате интернет, трябва да сте наясно с цифровия отпечатък, който оставяте. Точно както физическите следи от стъпки, които показват нечии стъпки по черен път, вашият цифров отпечатък е хронология на цялата ви дейност онлайн. Всички публикации в социалните мрежи, които създавате, всички уеб сайтове, които посещавате и всяка информация, която споделяте онлайн, допринасят за цифровия ви отпечатък. След като публикувате нещо онлайн, то не може да бъде изтрито. Така че вашият цифров отпечатък може да се запази вечно. Това може да е нещо хубаво, ако цифровият ви отпечатък включва неща, които ви дават положителна репутация онлайн. Това може да ви помогне да изградите личната си марка. Вашата онлайн хронология може също така да помогне на приложенията, които използвате, да научат повече за вас. Те могат да използват тази информация, за да ви служат по-добре, като се адаптират към нещата, които харесвате и към ежедневните ви навици. Но те могат да използват тази информация и по грешния начин и да я споделят с други хора. Имайте предвид следните съвети, когато влизате онлайн, за да управлявате цифровия си отпечатък. Съвет номер едно: разберете какво казва отпечатъкът ви за вас. Други хора използват вашия цифров отпечатък, за да ви преценяват онлайн. Това може да включва работодатели, когато кандидатствате за работа, или лица, набиращи персонал, когато кандидатствате за академични програми. Важно е да знаете какво казва вашият цифров отпечатък за вас и как се използва информацията ви. За да видите личната си марка онлайн, можете да я потърсите сами. Потърсете името си в търсачката на Bing и вижте какви резултати се показват. Ако тези резултати не покажат каквото искате, помислете какво споделяте онлайн и каква информация позволявате другите хора да виждат. Съвет номер две: управлявайте настройките си за поверителност. Можете да промените настройките за поверителност в повечето сайтове на социални мрежи и онлайн приложения, които използвате. Това може да ви помогне да контролирате кой вижда какво споделяте и каква информация се показва, когато някой ви потърси онлайн. Съвет номер три: управлявайте бисквитките си. Бисквитките са бележки, давани на уеб браузъра ви, докато сърфирате в мрежата. Тези бисквитки помагат на приложенията да следят информацията, която им е необходима, докато използвате приложението. Това може да помогне на приложението да работи по-добре за вас. Но тези данни допринасят и за вашия цифров отпечатък. Можете да използвате настройките в браузъра си, за да ограничите или блокирате използването на бисквитки в определени уеб сайтове. Съвет номер четири: помислете, преди да споделите. След като споделите нещо онлайн, не можете да го върнете. Уверете се, че нямате против нещо да бъде част от публичния ви цифров отпечатък, преди да го споделите. Вашият цифров отпечатък може да живее вечно. Имайте предвид тези съвети, за да се уверите, че сте доволни от цифровия си отпечатък и от начина, по който се използва.

Проверка на знанията

3 минути

1. Кои от следните компоненти трябва да търсите в URL адреса на уеб страница, за да се уверите, че сте на защитен сайт?

* http
* Сигурен
* **HTTPS-правилно! "https" означава, че уеб страницата е защитена.**
* Ssh

1. Коя от тези пароли е най-силна?

* **John@453-правилно! Тази парола съдържа главни, малки, специални знаци и числа.**
* john500
* JoHn300
* 125893

1. Цифровият ви отпечатък е:

* Размерът на информацията в онлайн профилите ви.
* Броят на хората, с които сте свързани онлайн.
* **Рекорд за всичко, което правиш и казваш онлайн. Правилното! Цифровият ви отпечатък улеснява проследяването на действията ви онлайн.**
* Вашето онлайн потребителско име.
* r използване на силни пароли.

## Резюме

3 минути

Поздравления!

Вие сте завършили онлайн модула за безопасност и поверителност и сега можете да отговорите на следните въпроси сами:

1. Какви са някои от опасностите от използването на интернет и мрежата?
2. Кои са някои от признаците на рисковете за безопасността и измамите онлайн?
3. Какви стъпки можете да предприемете, за да бъдете в безопасност, докато използвате интернет?
4. Как можете да управлявате цифровия си отпечатък?

**следния видеоклип, за да научите как да създавате силни, ефективни пароли ,**

# Онлайн учтивост

9 минути | 5 единици

В този модул ще научите повече за правата и най-добрите практики за използване на информация онлайн. Ще научите и за кибертормоза.

Въвеждането

3 минути

Можем да използваме интернет за достъп до много информация и да общуваме с други хора, но трябва да сме сигурни, че се държите като отговорни цифрови граждани.

В този урок ще научите как отговорно да използвате интернет и уеб.

**До края на този урок ще можете да:**

1. Опишете правата, които хората имат за информация и съдържание, споделени в интернет.
2. Опишете най-добрите практики за използване на информацията, намерена в мрежата.
3. Описание на последствията от недобре лечение на другите в интернет.
4. **защитите информацията си.**

## Опишете най-добрите практики за използване на информацията, намерена в мрежата

2 минути

### Отговорно използване на информацията

Въпреки че достъпът до информация е лесен в цифровия свят, има някои правила, които трябва да имате предвид, когато искате да използвате информацията, която намирате онлайн.

**Гледайте следното видео, за да научите някои от указанията за използване на информация, която намирате онлайн.**

### Видео: отговорно използване на информацията

Интернет ни предоставя неограничена информация и възможности. Можем да намерим всичко от смешни видеоклипове до любимите ни песни или информация за това как да решим проблем с домашна работа, но трябва да се отнасяме отговорно към информацията, която намираме онлайн. Помислете за един сценарий. Харолд иска да напише готварска книга и да я продаде онлайн. Не е добър в правенето на снимки, така че търси снимки онлайн. Изтегля снимки на различни храни и ги включва в книгата си. Това може да изглежда нормално, защото е лесно да се направи, но не е честен или отговорен начин за използване на информация, намерена онлайн. Когато някой качи оригиналната си работа онлайн, включително текстове, снимки, видеоклипове, музика и други, той става собственик на съдържанието. Като собственик той има определени права, които обикновено се считат за авторски права, да реши как това съдържание може да се използва. Ако използвате текстовете или работата на някой друг като свои, това се счита за плагиатство. Не е честно спрямо оригиналния автор и може да ви вкара в беда. Ако искате да използвате съдържанието на някой друг в работата си, не забравяйте да го споменете, за да покажете заслугите му за работата му. Когато използвате нечия работа в продукт, който продавате, първо трябва да получите разрешение от автора. Също така може да се наложи да платите за лиценз за използване на нечия работа. Понякога авторите на съдържание правят работата си достъпна за свободно ползване. Можете да използвате търсачки като Bing, за да намирате снимки, мултимедия и други видове съдържание, което е достъпно за използване. Докато използвате интернет и намирате информация онлайн, не забравяйте да я използвате справедливо и отговорно.

## Опишете последствията от недобре лечение на другите в интернет

3 минути

### Кибертормоз

Интернет ни позволява да се свързваме с други хора онлайн от всички страни по света. За съжаление, хората невинаги се третират добре онлайн.

**Кибертормоза** е вид тормоз, който се извършва по интернет. Тя може да бъде лесно да изпращате средни съобщения или да разпространявате отрицателни слухове за други хора, но това може да бъде опасно за лицето, което е насочено.

**Гледайте следното видео, за да научите съвети за предотвратяване на кибертормоза и цифровото гражданство.**

### Видео: лечение на други почтително онлайн

Интернет и платформите на социалните мрежи ни свързват с нашите приятели, роднини и връстници по нови начини. Понякога хората се възползват от тези платформи и ги използват, за да разпространяват негативни съобщения за други хора. Кибертормозът – или тормоз, който се осъществява в интернет – може да е точно толкова лош, колкото и тормоза на живо. Хората могат да използват интернет, за да изпращат злобни съобщения на някого, да разпространяват фалшиви слухове или да споделят нечия лична информация без разрешение.

Когато някой е обект на кибертормоз, неговите чувства могат да бъдат наранени и репутацията му да бъде накърнена. Невинаги можете да предотвратите кибертормоза, но можете да изиграете роля в превръщането на интернет в по-дружелюбно и безопасно място за всички. Ето някои насоки, които можете да следвате, за да популяризирате цифровата учтивост онлайн:

* Живейте спрямо „златното правило“. Отнасяйте се с другите по начина, по който искате да се отнасят с вас, независимо дали на живо, или онлайн.
* Избягвайте изпращането на негативни съобщения и участието в поведение, което може да нарани някого.
* Уважавайте различията. Всички сме различни по много начини. Когато общувате с хора онлайн, уважавайте различията в мнението, опита и културата им. Дори и да не сте съгласни с нещо, което друг човек споделя онлайн, все пак трябва да се отнасяте с уважение и да спомагате за това интернет да бъде дружелюбно пространство за комуникация. Направете пауза, преди да отговорите.
* Преди да споделите нещо онлайн, винаги направете пауза и помислете за последствията. Съобщението ви ще нарани ли някого? Ще навреди ли на репутацията ви или на безопасността или репутацията на други хора? Помислете добре, преди да споделите онлайн. Отстоявайте себе си и другите.
* Ако не се чувствате в безопасност онлайн, трябва да се измъкнете от тази ситуация и да я докладвате на някого, на когото имате доверие.
* Когато видите жестока или опасна дейност онлайн, предложете подкрепа на въвлечените в нея хора и докладвайте инцидента на някого, на когото имате доверие. Всички можем да изиграем роля в превръщането на интернет в безопасно и дружелюбно място за всички.
* Изиграйте своята роля и бъдете отговорен цифров гражданин онлайн.

## Проверка на знанията

2 минути

1. Кой от тези действия не нарушава авторските права?

* Използване на нечии изображения в книга, която публикувате без тяхно разрешение.
* **Цитиране на абзац от нечия книга и препращането към тях-правилно! Съблюдавайте авторските права, когато цитирате собственика.**
* Продаваш нечие видео под името си.
* Да продадеш нечия книга без книжка.

1. Кибертормоз може да се осъществи:

* Само в социалните медийни платформи.
* Само чрез имейли.
* Само на SMS.
* **На платформите за социални медии и SMS и чрез имейли. Правилното! Кибертормоза може да се осъществи във всеки вид онлайн комуникация.**

## Резюме

3 минути

Поздравления!

Вие сте завършили онлайн учтивост модул и сега можете да отговорите на следните въпроси сами по себе си:

1. Какво трябва да направите, когато искате да използвате информацията, която намирате онлайн?
2. Какво можете да направите, за да предотвратите или прекратите кибертормоза?

# Отпечатване на сертификата ви

2 минути | 2 единици

Трябва да попълните всички модули в този курс, за да получите вашия сертификат.

## Получаване на кредит

3 минути

### Пълна

Честито попълване на участието безопасно и отговорно онлайн. Изберете **получаване на кредит** , за да завършите курса и да получите вашия сертификат.

### Получени кредити

Честито попълване на участието безопасно и отговорно онлайн.

В полето по-долу въведете името си, както искате да се показва на вашия сертификат, след което изберете **Преглед на сертификата**.