# Градење дигитална отпорност

# Прирачник и методологија

Градење дигитална отпорност со правење на дигиталната благосостојба и безбедност достапни за сите

2022-2-SK01-KA220-ADU-000096888

Co-funded by the European Union

Erasmus+ проект КА220 Партнерства за соработка во образованието на возрасни

# Градење дигитална отпорност со правење на дигиталната благосостојба и безбедност достапни за сите

2022-2-SK01-KA220-ADU-000096888

DigiWELL

# Градење дигитална отпорност
# Прирачник и методологија

септември, 2023

Co-funded by the European Union

Оваа публикација е подготвена како резултат на проектот “Градење дигитална отпорност со правење на дигиталната благосостојба и безбедност достапни за сите” (Проект бр: 2022-2-SK01-KA220-ADU-000096888), што се спроведува во рамките на Еразмус + КА220 партнерствата за соработка во образованието на возрасни.

## DigiWELL Конзорциум

Slovak University of Agriculture in Nitra, Slovakia

Muğla Sıtkı Koçman University, Turkey

Czech technical university in Prague, Czech

Innovation, Training, and Employment Association for Sustainable Development (AIFED), Spain

European Institute for Innovation – Technology (EIfI-Tech), Germany

Foundation Maker's Place Private Company (Found.ation), Greece

Syzigia Skopje Foundation (SYZYGY), Macedonia

Faculty of Economics and Management
Slovak University of Agriculture in Nitra |
Tr. Andreja Hlinku 2 | 949 76 Nitra | Slovakia | email: digiwell@uniag.sk

Website: www.digiwell.sk

## Одрекување:

*" Кофинансиран од Програмата Еразмус+ на Европската Унија. Оваа публикација ги одразува само гледиштата на соработниците, а Европската комисија и Словачката академска асоцијација за меѓународна соработка не можат да бидат одговорни за каква било употреба што може да се направи на информациите содржани во нив."*

Работен пакет 2: **Градење дигитална отпорност Прирачник и методологија**

*Список на соработници:*

*Murat Sümer, Czech Technical University,*

*David Vaneček, Czech Technical University,*

*Martina Hanová, Slovak University of Agriculture in Nitra, Slovakia*

*Marcela Hallová, Slovak University of Agriculture in Nitra, Slovakia*

*Eva Oláhová, Slovak University of Agriculture in Nitra, Slovakia*

*Eyüp Şen, Muğla Sıtkı Koçman University, Turkey*

*İlker Yorulmaz, Muğla Sıtkı Koçman University, Turkey*

*Maria Martinez, AIFED, Spain*

*Jesus de Haro Martinez, AIFED, Spain*

*Chris Ashe, ElfI-Tech, Germany*

*Mattia Ferrari, ElfI-Tech, Germany*

*Maria Kandilioti, Found.ation, Greece*

*Roula Mourmouri, Found.ation, Greece*

*Suzana Trajkovska, SYZYGY, Macedonia*

*Aleksandar Kochankovski, SYZYGY, Macedonia*

# Содржини

# Резиме

По пандемијата COVID-19, некои потреби станаа витални поради употребата на дигитални технологии и интернет, кои се многу во нашите животи. Најважно од нив е да може безбедно да се врши трансакција во дигиталниот свет без да се оштети. Особено на возрасните им се потребни дигитални безбедносни мерки и некои компетенции за да се заштитат од сајбер заканите. Исто така, интернетот и дигиталните технологии не само што го олеснуваат животот, туку создаваат и некои негативни психолошки проблеми. На пример, сајбер-малтретирањето стана тежок проблем за справување. Според тоа, обезбедувањето благосостојба во дигиталниот свет сега стана неопходност во сегашните услови. Повторно, во врска со ова прашање, зголемената употреба на дигиталната технологија и точката што ја достигна дигиталната трансформација донесоа некои прашања како што е дигиталниот замор на агендата на луѓето.

Во овој поглед, проектот DigiWELL има за цел да ги вклучи принципите за дигитална благосостојба во образованието за возрасни. Нејзините иницијативи се насочени кон придонес кон севкупните практики на организациите, мрежите и иницијативите за образование на возрасни. Проектот разбира колку е клучно да се реши како технологијата влијае на менталното здравје, продуктивноста и општата благосостојба на возрасните во дигиталната ера. Главната цел на DigiWELL е да им обезбеди на возрасните ученици информации, способности и ресурси неопходни за етичка и совесна навигација во дигиталниот свет. Проектот DigiWELL, исто така, вклучува создавање и извршување на дополнителни иницијативи за зајакнување на возрасните ученици. Целта на овие активности е да се обезбеди средина за поддршка каде што возрасните можат да ги споделат своите искуства, тешкотии и триумфи во промовирањето на дигиталната благосостојба. Имајќи го ова на ум, проектот DigiWELL претставува многу можности за поединци и организации за возрасни да станат свесни и просветлени за важноста на дигиталната благосостојба и за тоа како да се промовира дигиталната благосостојба на возрасни индивидуи и возрасни едукатори и обучувачи. Овозможувањето на дигиталната благосостојба со холистички пристап е многу по возможно доколку сите релевантни страни преземаат активности за поддршка на потребите за дигитална благосостојба на поединците. Следствено, информациите, советите и добрите практики презентирани во овој прирачник ги повикуваат луѓето и заинтересираните организации да преземат иницијативи за повеќе од нас да имаат подобра дигитална благосостојба, а исто така и посилен дигитален живот.

# 1 Вовед

## 1.1 Цел на методот и Мануел

- Да придонесе за овозможување дигитална благосостојба и дигитална безбедност достапни за сите преку охрабрување и информирање на возрасните за дигиталната благосостојба и дигиталната безбедност и потребните компетенции за нив.
- Да се воведе дигитална отпорност, дигитална благосостојба и дигитална безбедност, рамка на терминологија и најдобри практики за дигитална благосостојба и дигитална безбедност кај сите луѓе.
- За да се обезбеди мултикултуралност, приспособување на развиените резултати на релевантните организации во земјите партнери.

## 1.2 EU DigComp Framework

Во DigComp, дигиталната компетентност вклучува „сигурна, критичка и одговорна употреба и ангажирање со дигиталните технологии за учење, на работа и за учество во општеството. Таа е дефинирана како комбинација од знаења, вештини и ставови“. ( Препорака на Советот за клучните компетенции за доживотно учење , 2018).

Рамката DigComp ги идентификува клучните компоненти на дигиталната компетентност во 5 области. Областите се сумирани подолу:

**Информативна и податочна писменост** : да се артикулираат потребите за информации, да се лоцираат и да се преземат дигитални податоци, информации и содржина. Да се суди за релевантноста на изворот и неговата содржина. За складирање, управување и организирање на дигитални податоци, информации и содржина.

**Комуникација и соработка** : да комуницирате, да комуницирате и да соработувате преку дигитални технологии додека сте свесни за културната и генерациската разновидност. Да се учествува во општеството преку јавни и приватни дигитални услуги и партиципативно граѓанство. Да управуваат со сопственото дигитално присуство, идентитет и репутација.

**Создавање дигитална содржина** : креирање и уредување дигитална содржина Да се подобрат и интегрираат информациите и содржината во постоечкото тело на знаење додека се разбира како треба да се применуваат авторските права и лиценците. Да знае да дава разбирливи инструкции за компјутерски систем.

**Безбедност** : За заштита на уредите, содржината, личните податоци и приватноста во дигитални средини. Да се заштити физичкото и психолошкото здравје и да се биде свесен за дигиталните технологии за социјална благосостојба и социјална инклузија. Да се биде свесен за влијанието врз животната средина на дигиталните технологии и нивната употреба.

**Решавање проблеми** : Да се идентификуваат потребите и проблемите и да се решат концептуални проблеми и проблемски ситуации во дигитални средини. Да се користат дигитални алатки за да се иновираат процеси и производи. За да бидете во тек со дигиталната еволуција.

Една од клучните надлежности во областа на Безбедноста е заштитата на здравјето и благосостојбата. Заштита на здравјето и благосостојбата значи; (а) да може да избегне здравствени ризици и закани за физичката и психолошката благосостојба додека користи дигитални технологии, (б) да може да се заштити себеси и другите од можни опасности во дигитални средини (на пр. сајбер малтретирање) и (в ) да бидат свесни за дигиталните технологии за социјална благосостојба и социјална инклузија.

## 1. 3 Зошто M&M е добар ресурс за возрасни

Како што беше споменато погоре, по пандемијата COVID-19, некои потреби станаа витални поради употребата на дигитални технологии и интернет, кои се многу во нашите животи. Најважно од нив е да може безбедно да се врши трансакција во дигиталниот свет без да се оштети. Особено на возрасните им се потребни дигитални безбедносни мерки и некои компетенции за да се заштитат од сајбер заканите. Исто така, интернетот и дигиталните технологии не само што го олеснуваат животот, туку создаваат и некои негативни психолошки проблеми. На пример, сајбер-малтретирањето стана тежок проблем за справување. Според тоа, обезбедувањето благосостојба во

дигиталниот свет сега стана неопходност во сегашните услови. Повторно, во врска со ова прашање, зголемената употреба на дигиталната технологија и точката што ја достигна дигиталната трансформација донесоа некои прашања како што е дигиталниот замор на агендата на луѓето.

Овој прирачник користи што е можно повеќе примери од реалниот свет и им дозволува на возрасните ученици сами да сфатат некои концепти за да го поддржат учењето на возрасни врз основа на Ноулс (1968).

## 1.4 Зошто M&M треба да е добар ресурс за возрасни обучувачи

Обуката и образованието играат клучна улога во зајакнувањето на свеста за дигиталната безбедност преку зајакнување на поединците со знаење, вештини и најдобри практики потребни за да се заштитат себеси и нивните организации од сајбер закани. Дополнително, обуката и образованието за дигитална безбедност се суштински компоненти за градење силна култура на сајбер безбедноста. Со дизајнирање на програми за обука кои се приспособени на специфичните потреби и улоги, ги опремуваат возрасните со знаења и вештини потребни за да се идентификуваат и ефективно да одговорат на сајбер заканите.

Обуката им помага на поединците да ги разберат различните видови на сајбер закани, како што се фишинг, малициозен софтвер, социјален инженеринг и откуп. Со препознавање на овие закани, поединците можат да бидат повнимателни и повнимателни додека користат дигитални платформи. Образованието може да ги научи поединците како да идентификуваат е-пошта, пораки или веб-страници за фишинг. Тие учат да забележуваат сомнителни елементи и избегнуваат да кликнуваат на малициозни врски или да даваат чувствителни информации. Во исто време, обуката вклучува насоки за обезбедување на мобилни уреди, нивна заштита со шифри, користење шифрирање и претпазливост при преземањето апликации, додека се осигурува дека поединците се свесни за релевантните регулативи за сајбер безбедност и барањата за усогласеност, што помага во одржувањето на правните и етичките практики. Конечно, преку образованието, поединците разбираат дека сајбер-безбедноста е заедничка одговорност и дека активното вклучување на сите е неопходно за одржување на безбедна средина, додека всадува добри навики за сајбер-безбедност, охрабрувајќи ги поединците да спроведуваат безбедносни мерки и на работа и во нивниот личен живот.

Проектот DigiWELL има за цел да одговори на потребите за дигитална безбедност и благосостојба на возрасните кои не се родени во ерата на Интернет. Тоа ќе го постигне со создавање и развивање флексибилни можности за учење кои се грижат за специфичните барања за учење на возрасните. Проектот ќе се фокусира на подобрување на дигиталната отпорност преку комбиниран пристап за учење. Овој прирачник особено придонесува за горенаведената цел бидејќи создава култура свесна за безбедноста која активно се брани од сајбер закани и ги штити дигиталните средства и чувствителните информации.

Со други зборови, прирачникот со сесија посветена на дигиталната безбедност може да игра значајна улога во опремувањето на возрасните со потребните вештини и знаења за да се заштитат себеси во дигиталната ера, поттикнувајќи побезбедно и побезбедно онлајн искуство за поединци и заедници. DigiWELL е вреден ресурс за возрасни, бидејќи ги едуцира возрасните за потенцијалните ризици, помагајќи им да ја разберат важноста на сајбер безбедноста и како да се заштитат на интернет. Конечно, нуди практични упатства за спроведување дигитални безбедносни мерки и ги

овластува возрасните да се движат со самодоверба во дигиталниот свет и служи како референтен водич што возрасните можат повторно да го посетат секогаш кога ќе се сретнат со нови предизвици за дигиталната безбедност или кога им е потребно освежување на одредени теми.

## 1.5 Речник на проектот DigiWELL и како да се користи

Речник има за цел да ги запознае возрасните корисници на дигитални технологии со основните термини и дефиниции поврзани со дигиталната благосостојба, дигиталната безбедност и дигиталната отпорност.

### *Класификација на термините*

Содржински, речникот содржи 3 основни категории поими;

1. Термини и дефиниции од областа на информатичко-комуникациските технологии (дигитални технологии според проектот).
2. Термини и дефиниции од областа на информации, сајбер и дигитална безбедност (дигитална безбедност според проектот).
3. Термини и дефиниции дефинирани со целите на проектот: дигитална благосостојба и дигитална отпорност. Овие термини се релативно нови и тие се дел од деск истражувањето на проектните тимови. Треба да се нагласи дека не постои единствена дефиниција за овие поими. Оваа категорија вклучува и термини од областа на менталното и физичкото здравје, на пр. дигитална зависност, дигитален замор/прегорување, дигитална детоксикација итн.

***Забелешка:*** Во текстуалната база на речник, терминот може да има повеќе од една дефиниција поради многу причини: оригиналната дефиниција еволуирала со текот на времето, широката дефиниција е прилагодена на одредена област, дефинициите на поимите се слични, но со суптилни разлики итн.

### *Поими и дефиниции*

***Дигитална еластичност:*** 1. Дигитална еластичност значи да се има свесност, вештини, агилност и самодоверба за користење на новите технологии и прилагодување на променливите барања за дигитални вештини. Дигиталната еластичност го подобрува капацитетот за решавање проблеми и вештини, како и капацитетот за навигација со дигитални трансформации. 2. Дигиталната отпорност е способност на младите луѓе да развијат критички ментален сет при пристап до дигитални информации за да ја намалат нивната ранливост на потенцијално штетни информации. 3. Дигитална отпорност значи „процес на добро приспособување на дигиталните извори на стрес и развивање вештини за управување со влијанието на дигиталните средини и апликации кои постојано се менуваат“.

***Дигитална безбедност:*** Дигиталната безбедност е заштита на дигиталниот идентитет, бидејќи претставува физички идентитет на мрежата или интернет услугите. Дигиталната безбедност

е збир на најдобри практики и алатки кои се користат за заштита на личните податоци и онлајн идентитетот во онлајн светот. Примери на алатки се: веб-услуги, антивирусен софтвер, СИМ-картички за паметни телефони, биометриски и безбедни лични уреди, управувачи со лозинки, родителска контрола итн.

***Дигитална благосостојба:*** 1. Дигиталната благосостојба ја опишува способноста на една личност ефикасно да управува со негативните влијанија на технологијата врз нивниот професионален и личен живот. Целта на дигиталната благосостојба е да промовира здрава употреба на технолошки уреди и дигитални услуги. 2. Состојба на лична благосостојба доживеана преку здрава употреба на дигиталната технологија. 3. Дигиталната благосостојба ги опфаќа начините на кои информатичката технологија - вклучувајќи ги комуникациите и сензорите - може да им помогне на луѓето да живеат долг и здрав живот.

***Дигитална компетентност:*** Сигурна, критичка и одговорна употреба и ангажирање со дигиталните технологии за учење, на работа и за учество во општеството. Се дефинира како комбинација на знаења, вештини и ставови.

***Дигитална зависност:*** Дигиталната зависност е штетна зависност од дигиталните медиуми, уредите и интернетот која се карактеризира со нивна прекумерна употреба на начин што има негативно влијание врз животот на корисникот.

***Дигитални вештини:*** Дигиталните вештини се како опсег на способности за користење на дигитални уреди, комуникациски апликации и мрежи за пристап и управување со информации. Тие им овозможуваат на луѓето да креираат и споделуваат дигитална содржина, да комуницираат и да соработуваат и да решаваат проблеми за ефективно и креативно самоисполнување во животот, учењето, работата и социјалните активности.

***Сајбер закана:*** Секоја околност или настан со потенцијал да има негативно влијание врз организации/поединци преку неовластен пристап, уништување, откривање, измена на информации и/или одбивање на услугата. Целта е да се украдат/ оштетат податоци или да се наруши дигиталната благосостојба.

***Сајбер-малтретирање:*** Термин за различни форми на малтретирање во онлајн просторот во кој еден или повеќе поединци користат дигитална технологија за намерно и постојано да му наштетат на друго лице (на пр. испраќање е-пошта или инстант пораки, објавување коментари на социјалните мрежи или јавни форуми).

***Сајбер-безбедност:*** Сајбер-безбедноста е подгрупа на безбедноста на информациите, нејзината цел е да го заштити сајбер просторот (т.е. мрежи, интранет, сервери, информации и компјутерски системи и инфраструктура) од неовластен пристап, сајбер-напади или оштетувања.

Сајбер-безбедноста се фокусира на заштитата на информациите во електронска/дигитална форма лоцирани во компјутери, складишта и мрежи (во сајбер просторот).

***Дигитална приватност:*** Дигиталната приватност е способност на поединецот да го контролира и заштити пристапот и употребата на нивните лични информации како и кога пристапува на интернет. Дигиталната приватност им помага на поединците да останат анонимни на интернет со заштита на личните информации како што се имиња, адреси, социјален идентификациски број, детали за кредитна картичка итн.

***Дигитална безбедност наспроти сајбер безбедност наспроти безбедност на информации:*** Безбедност на информации: ги заштитува информациите (во кој било формат и форма) и информациските системи од неовластен пристап и употреба за да се обезбеди и зачува приватноста на важните податоци. Сајбер безбедност: заштитува цели мрежи и комуникациски системи, компјутерски системи и други дигитални компоненти и дигитални податоци складирани во нив. Дигитална безбедност: го штити присуството на интернет (идентитетот и поврзаните чувствителни информации, средства.

***Најдобра практика:*** Докажан метод или постапка што нуди најефективно решение во дадена област, што е докажано дека води до оптимални резултати и е воспоставено (предложено) како соодветен стандард за широко распространето усвојување. Во дигиталната безбедност, ова се дефинирани процедури за да се обезбеди заштита на поединец/организација во дигиталниот простор (на пр. препорачани техники, програми, упатства, прирачници).

# 2 Дигитална благосостојба

## 2.1 Што е благосостојба?

Терминот „ **благосостојба** “ ја опишува состојбата да се биде задоволен, радосен и здрав. Тоа ја вклучува физичката, менталната и емоционалната благосостојба на една личност, меѓу другите области на нивното постоење. Надвор од самото ослободување од болести или непријатност, благосостојбата се фокусира на целокупната среќа и квалитетот на животот.

***Физичката благосостојба*** е состојба на нечие тело, земајќи ги предвид работи како физичка подготвеност, исхрана и отсуство на болест или болест. Тоа подразбира одржување на здрав начин на живот преку постојано вежбање, хранлива храна, доволно сон и управување со стресот.

Когнитивното и емоционалното здравје на една личност се поврзани со неговата ***ментална благосостојба*** . Тоа подразбира да се има добар поглед, да се доживее исполнувањето и да се биде способен да се справи со стресот и тешкотиите во животот. Активностите како вежбање внимателност, преземање хоби, барање поддршка од најблиските и добивање професионална помош кога е потребно, може да помогнат во потхранувањето на нечија ментална благосостојба.

Да се има добро разбирање и капацитет да се контролираат своите емоции се нарекува ***емоционална благосостојба*** . Тоа подразбира негување на издржливост, одржување добри односи

и позитивно чувство за себе. Самосвеста, емоционалната контрола, ефикасната комуникација и развојот на поддржувачки односи придонесуваат за емоционална благосостојба.

Квалитетот на врските на една личност и чувството за припадност на заедницата се сите делови на ***социјалната благосостојба*** . Тоа подразбира негување трајни врски со најблиските, блиските пријатели и поголема социјална мрежа. Учеството во социјални активности, враќањето на заедницата и одржувањето на чувството на поврзаност и припадност може да ја подобри социјалната благосостојба.

Севкупно, **благосостојбата** е сеопфатна идеја која разгледува како различните аспекти од животот на една личност се меѓусебно поврзани. Тоа подразбира активно барање урамнотежена и задоволувачка егзистенција, грижа за своето телесно и ментално здравје, негување здрави односи и наоѓање смисла во својот живот.

## 2.2 Благосостојба и дигитализација

Со овозможување на комуникација, зголемување на ефикасноста и подобрување на пристапот до информации, технологијата и дигитализацијата имаат потенцијал да ја подобрат благосостојбата. За да управувате со дигиталната употреба, да ја заштитите приватноста и безбедноста и да постигнете добар баланс помеѓу технологијата и другите аспекти на животот, од клучно значење е да бидете свесни за можните недостатоци и да ги преземете неопходните мерки на претпазливост.

Технологијата и дигитализацијата значително го подобрија пристапот до информации и услуги, што има позитивен ефект врз благосостојбата. Луѓето сега имаат лесен пристап до дигитални алатки за личен развој, информации за здравствена заштита, групи за поддршка на интернет и образовни ресурси. Преку беспрекорна комуникација и поврзување на далечина, технологијата ги промовира социјалните врски и го намалува чувството на осаменост. Луѓето можат да останат во контакт со пријателите, семејството и заедниците благодарение на дигиталните платформи, социјалните медиуми и апликациите за пораки, кои ја подобруваат социјалната благосостојба. Многу аспекти на животот станаа поефикасни и поудобни благодарение на дигитализацијата. Преку употреба на дигитални алатки и услуги, задачите кои некогаш бараа многу време и напор, сега може да се завршат брзо и без напор. Ова може да помогне во општата благосостојба со ослободување на време и намалување на стресот. Згора на тоа, дигиталните способности стануваат се повеќе и повеќе клучни на пазарот на трудот како што се развива технологијата. Вработливоста и социо-економската благосостојба на една личност може да се подобрат со стекнување и користење на овие таленти. Дигиталниот јаз, кој се јавува кога некои луѓе или групи немаат пристап до технологија или дигитална писменост, може, сепак, да ги влоши веќе постоечките разлики.

Додека користењето на технологијата неправилно или прекумерно може да има штетни ефекти врз нечие ментално здравје, исто така може да има добри ефекти. Анксиозноста, очајот и ниската самодоверба може да бидат под влијание на премногу време на екранот, споредбата на социјалните мрежи и злоупотребата на интернет. За да се заштити менталното здравје, од клучно значење е да се одржи здрава рамнотежа и да се практикува внимателна употреба на технологија. Исто така, дигиталната средина има некои проблеми со приватноста и безбедноста. Сајбер заканите, прекршувањето на податоците и онлајн измамите можат да ја доведат во опасност финансиската безбедност и личните информации на луѓето. Одржувањето на целокупната благосостојба во дигиталната ера бара заштита на дигиталната безбедност и приватност.

## 2.3 Што е дигитална благосостојба?

Развојот на дигиталната отпорност и усвојувањето на безбедносните процедури доведува до состојба на оптимално здравје и општа благосостојба во дигиталната сфера, која се нарекува ***дигитална благосостојба*** . Дигиталната благосостојба потекнува од концептот на благосостојба и има врска со дигиталните животи на поединците. Капацитетот на луѓето да се прилагодат, управуваат и напредуваат во дигиталниот свет додека успешно управуваат со нивната благосостојба и безбедност се нарекува ***дигитална отпорност*** , што е мешавина од дигитална благосостојба и безбедност. Камен-темелникот на дигиталната отпорност е дигиталната благосостојба, која го нагласува зачувувањето на позитивната и разумна врска со технологијата. Тоа подразбира ограничување на времето поминато на екранот, ставање висок приоритет на менталното и емоционалното здравје, создавање на поддржувачки онлајн заедници и учење на дигитална писменост. Во контекст на благосостојбата, дигиталната отпорност им помага на луѓето да се справат со тешкотиите на интернет како што се сајбер-малтретирањето, онлајн вознемирувањето или изложеноста на опасна содржина, додека ја зачувуваат нивната општа благосостојба. Поединците можат да изградат силна дигитална еластичност што им овозможува да се движат низ дигиталниот свет со сигурност и одговорност преку интегрирање на дигиталната благосостојба со дигиталната безбедност. Тие се поспособни да управуваат со предизвиците на дигиталниот свет, да се приспособат на променливите опасности, да донесуваат мудри проценки, да ги заштитат своите лични информации и да го одржуваат своето ментално, емоционално и физичко здравје додека користат интернет. Дигиталната отпорност на крајот поттикнува побезбедно, поздраво и поисполнето онлајн искуство за луѓето.

### *2.3.1 Ментално здравје, благосостојба и дигитална благосостојба*

Целиот наш квалитет на живот е под влијание на длабоките врски помеѓу нашето ментално здравје и целокупната благосостојба. Нашата психолошка и емоционална благосостојба, вклучително и аспекти како што се нашите мисли, чувства и однесувања, се нарекуваат наше ментално здравје. Тоа е од фундаментално значење за нашето целосно здравје, исто толку важно како и физичката благосостојба. Спротивно на тоа, благосостојбата е сеопфатна состојба на рамнотежа, исполнетост и задоволство во животот. Врската помеѓу двете се заснова на тоа како нечие ментално здравје има значително влијание врз нивното физичко здравје и обратно. Нашата вкупна благосостојба се зголемува кога негуваме позитивно ментално здравје преку контролирање на стресот, надминување на пречките и градење здрави односи, што резултира со поисполнет и позначаен живот. Од друга страна, чувството на благосостојба може во голема мера да го подобри менталното здравје преку поттикнување на издржливост, емоционална стабилност и поголема способност за справување со предизвиците во животот. Можеме да создадеме среќен и просперитетен живот со ставање на фокус на врската помеѓу нашето ментално здравје и благосостојба.

Поради брзите подобрувања во технологијата и нејзината распространета интеграција во нашиот секојдневен живот, менталното здравје зазема сложена и динамична природа во дигиталната ера. Во контекст на дигиталната ера, нечија ментална и емоционална благосостојба се нарекува „дигитално ментално здравје“. Вклучува социјални медиуми, онлајн интеракции, психолошките ефекти на дигиталните технологии и континуираната поврзаност што го дефинира модерниот живот. Иако технологијата создаде многу предности и можности, таа исто така создаде значителни тешкотии за менталното здравје. И покрај постојаниот виртуелен контакт, дигиталната ера може да резултира со проблеми како зависност од интернет, сајбер-малтретирање,

преоптоварување со информации, социјална споредба и чувство на изолација. Сепак, тој обезбедува и врвни пристапи за управување со менталното здравје, како што се апликации за ментално здравје, онлајн терапија и виртуелни групи за поддршка. Одржувањето здрава рамнотежа помеѓу нашите животи на интернет и офлајн, да се биде свесен за тоа колку дигитални медиуми трошиме и активно да бараме дигитални алатки кои можат да ја подобрат нашата ментална благосостојба додека се чуваат од потенцијални замки се од суштинско значење додека поминуваме низ сложеноста на дигиталната возраста.

Во денешно време, постои сложена врска помеѓу менталното здравје и дигиталната благосостојба. Психолошката и емоционалната благосостојба на поединците, која вклучува фактори како што се расположението, мислите, чувствата и однесувањето, се нарекува нивно ментално здравје. Од друга страна, дигиталната благосостојба ја опишува рамнотежата и хармонијата што се чувствува кога се користи технологијата и се вклучува во дигитални односи. Дигиталната ера има многу придобивки, овозможувајќи поврзување, пристап до информации и шанси за личен развој. Меѓутоа, прекумерната употреба на технологијата, постојаните известувања, притисокот на социјалните мрежи и преоптоварувањето со информации може да имаат негативно влијание врз менталното здравје предизвикувајќи напнатост, загриженост и чувство на одвоеност од реалноста. Од друга страна, може да има благотворно влијание врз менталното здравје кога дигиталната благосостојба е дадена како приоритет со поставување на граници, правење редовни паузи од екраните и внимавање на дигиталната потрошувачка. Со цел да се поттикне и менталното здравје и дигиталната благосостојба и да се гарантира хармоничен соживот помеѓу нашиот виртуелен и реален живот, од суштинско значење е да се постигне здрава рамнотежа помеѓу дигиталното вклучување и офлајн активностите. Позначаен и добро избалансиран живот во дигиталната ера може да се постигне со намерно прифаќање на технологијата и користење на дигитални алатки за подобрување на менталното здравје.

### *2.3.2 Зошто ни е потребна дигитална благосостојба?*

Клучните двигатели на дигиталната благосостојба се квалитетот на животот, комуникацијата, продуктивноста и успехот, менталното и физичкото здравје. Бидејќи ја вклучува целата состојба на човек да се биде здрав, среќен и задоволен, дигиталната благосостојба е важна. Тоа се однесува на целокупното здравје на луѓето и заедниците, земајќи ги предвид нивните социјални, психолошки и физички аспекти. Употребата на мобилни телефони, социјални медиуми и видео игри прекумерна или нездрава може да биде штетна за менталното здравје. Анксиозноста, очајот, осаменоста и лошата самодоверба може да се влошат со прекумерно време на екранот, чести споредби со другите на социјалните мрежи или сајбер-малтретирање. Во овој поглед, дигиталната благосостојба е начин да имаме контрола врз нашиот сопствен живот. Клучно е да се има здрава врска со технологијата за да се поддржи доброто ментално здравје и дигиталната благосостојба. Поставувањето ограничувања за користење гаџети, вклучувањето во дигитални детоксикации, учеството во офлајн активности и давање врвен приоритет на грижата за себе и на интеракциите лице-в-лице, сето тоа може да биде дел од ова. Мора да бидеме свесни за влијанието што дигиталната технологија го има врз нашето ментално здравје и да преземеме проактивни мерки за да обезбедиме нејзино разумно користење.

Дигиталната благосостојба стана суштинска човечка потреба во дигиталната ера, особено во пресрет на пандемијата „Ковид-19“. Нашето потпирање на дигиталните платформи се зголеми бидејќи технологијата продолжува да го напаѓа секој дел од нашиот секојдневен живот, од комуникација и образование до вработување и забава. Епидемијата предизвика дигитализацијата да напредува со невидена брзина, барајќи далечна работна сила, онлајн школување и повеќе виртуелни

односи. Како резултат на тоа, одржувањето на нашата дигитална благосостојба е од клучно значење за водење исполнет и здрав живот. Можеме да ја користиме технологијата на совесен и одговорен начин за да се осигураме дека таа ги подобрува нашите животи наместо да претставува закана за нашата општа благосостојба во оваа брзопроменлива дигитална средина со тоа што ќе ја признаеме дигиталната благосостојба како основна човечка потреба.

### *2.3.3 Добра и лоша дигитална благосостојба*

Дигиталната благосостојба е сеопфатен термин кој опфаќа различни аспекти од дигиталниот свет. Се занимава и со физички, психолошки и социјално здрави индивидуи и со нивното чувство дигитално свесни, избалансирани, безбедни, задоволни и здрави од друга страна. Како што се гледа, значењето што му се припишува на терминот „дигитална благосостојба“ е главно кон поволната страна на дигитализацијата, која се однесува на добрата дигитална благосостојба. Спротивно на тоа, поединците кои доживуваат недостаток на дигитална благосостојба се однесува на лошата дигитална благосостојба. Имајќи го предвид ова, следните аспекти може да се наведат како меѓу главните индикатори за добра дигитална благосостојба:

- Дигитална безбедност: Обезбедувањето дигитална безбедност дава извонреден придонес за нечија дигитална благосостојба. Тоа опфаќа заштита на вашето онлајн присуство вклучувајќи го вашиот идентитет, податоци и средства.
- Дигитална безбедност: вклучува свесност на поединците за потенцијалните ризици во дигиталниот свет и има врска со способноста на поединците критички да идентификуваат и управуваат со различни закани во дигиталната средина.
- Дигитална рамнотежа: се однесува на намерна корист од технологијата и дигиталниот свет. Дигиталната рамнотежа има врска со користењето на дигиталниот свет, дигиталните алатки и опрема за области од животот, а не за сè. Редовната и конзистентна онлајн/офлајн рамнотежа и избегнувањето на големата зависност од технологијата се знаци за добра дигитална рамнотежа.
- Дигитална независност: Тоа е способност да се контролира времето поминато на интернет и да се избегне центрирање на дигиталниот свет во секојдневниот живот. Трошењето премногу време на интернет и планирањето помалку социјални активности поради прекумерното користење на интернет се некои знаци на дигитална зависност.
- Дигитално задоволство: Се однесува на постигнување задоволство и чувство на задоволство при користење на дигитални алатки и опрема и испреплетување со технологијата.
- Дигитални можности: Се занимава со придобивките од технологијата и дигитализацијата за да се отворат какви било нови можности поврзани со ширење на дигитални технологии и да се стекнат понови компетенции за да се изградат нови можности.
- Критична и одговорна употреба на технологијата: Заедно со нејзините можности, технологијата бара од корисниците да се однесуваат одговорно со заштита на сопствените права и почитување на правата на другите, да дејствуваат на одговорен и претпазлив начин и да размислуваат критички кон која било содржина во дигиталниот свет. .

Овие аспекти може да се земат предвид и меѓу димензиите на дигиталната благосостојба. Ако некој има или обезбедува релативно повисоко ниво на дигитална безбедност, безбедност, рамнотежа, независност, задоволство, можност и/или критичка и одговорна употреба на

технологијата при користење на дигитални алатки и опрема, тој/таа може да се смета дека има добра дигитална благосостојба. . Напротив, ако некој нема некои од горенаведените компоненти, тоа значи дека тој/таа има лоша дигитална благосостојба. Вреди да се одбележи да се запамети дека физичкиот, психолошкиот и социјално здравиот човек исто така се однесува на добрата дигитална благосостојба, а понатамошните аспекти имаат потенцијален придонес за дигиталната благосостојба на поединците и целокупната благосостојба.

### *2.3.4 Поттикнување на дигитална благосостојба на поединци: потенцијални профити за сите и за образование на возрасни*

Промовирањето на дигиталната благосостојба во образованието за возрасни или зајакнувањето на благосостојбата и дигиталната благосостојба на возрасните обезбедува многу можности. Прво и основно, благосостојбата е основна човечка потреба. Особено по СОВИД-19, повеќето луѓе поминуваат многу повеќе време на интернет и тие се повеќе изложени на технологијата заедно со нејзините ризици и закани. Ако луѓето намерно сакаат или не, тие го носат целото себе на работа, имено постои јасна поврзаност во сопствената благосостојба на луѓето и атмосферата во работната средина. Значи, потенцијалните активности за поттикнување на благосостојбата и дигиталната благосостојба на поединците придонесуваат за нив како човечки суштества и за организациите за кои работат. Од организациска перспектива, поттикнувањето на дигиталната благосостојба на работниците придонесува, но не е ограничено на перформансите на тимот, посветеноста, иновативноста и задоволството. Дигиталната благосостојба им овозможува на поединците да станат пофокусирани, ангажирани и попродуктивни, што придонесува за поздрав живот и внатре и надвор од работната средина. Усвојувањето на дигитални велнес практики на вработените им овозможува да станат помалку исцрпени и расеани. Промовирањето на акции за поддршка за дигитална благосостојба го поттикнува балансот помеѓу работата и животот на поединците. Понатаму, ги елиминира негативните влијанија од прекумерната изложеност на дигитализација, што овозможува да се доживее помалку анксиозност, очај, стрес итн.

Идејата за благосостојба во контекст на образованието за возрасни оди подалеку од конвенционалните идеи за академско достигнување и го вклучува целокупното здравје и исполнување на учениците. Концептот на „дигитална благосостојба“ стана поважен со доаѓањето на дигиталната ера, особено за дигиталните номади кои во голема мера се потпираат на технологијата додека живеат подвижен начин на живот. Во образованието за возрасни, терминот „дигитална благосостојба“ се однесува на обезбедување на способности и информации на учениците што им се потребни за разумно и етички да го користат интернетот. Промовирањето на дигиталната благосостојба е од клучно значење за создавање успешна средина за учење, бидејќи дигиталните номади често се соочуваат со посебни тешкотии како жонглирање на нивниот личен и професионален живот и надминување на емоциите на осаменост. Интегрирањето на дигиталната благосостојба во образованието за возрасни подразбира учење на учениците како правилно да го контролираат времето поминато на екранот, да градат позитивни онлајн заедници и да ја одржуваат свеста за нивната дигитална употреба. Таа, исто така опфаќа теми вклучувајќи сајбер безбедност, дигитална замор и приватност на податоците. Во денешниот дигитално управуван свет, воспитувачите можат да обезбедат позитивно и збогатувачко искуство за учење преку решавање на очигледната потреба за зајакнување на дигиталната благосостојба во образованието за возрасни и обезбедување на дигиталните номади и другите ученици со алатки за одржување здрава рамнотежа помеѓу нивните дигитални интеракции и целокупната благосостојба.

Потребна е внимателна и темелна стратегија за успешно интегрирање на дигиталната благосостојба во образованието за возрасни бидејќи тоа е комплициран и континуиран процес. Првиот и најважен чекор е да им се даде обука на возрасните ученици за да бидат свесни за вредноста на дигиталната благосостојба и како тоа влијае на нивното општо здравје и продуктивност. Тие ги стекнуваат потребните практични вештини за разумно и безбедно да се движат низ дигиталниот свет благодарение на оваа инструкција. Втората фаза е да се измени материјалот на курсот така што наставната програма ги одразува концептите на дигитална благосостојба. Ова подразбира инкорпорирање на идеи како што се контролирање на дигиталните одвлекувања, приватноста на интернет, дигиталниот бонтон и дигиталната писменост. Возрасните ученици можат подобро да ги сфатат предностите и недостатоците на технологијата и да научат како ефективно да ја користат со вградување на овие карактеристики во курсевите. Создадена е средина за поддршка каде што учениците можат да споделуваат искуства, да заменат техники и да ја потврдат својата посветеност на дигиталната благосостојба преку дизајнирање дополнителни настани за зајакнување, како што се семинари и разговори. За да биде релевантно и ефективно во поттикнувањето на благосостојбата во дигиталната ера, образованието за возрасни мора постојано да се развива со цел да биде во чекор со дигиталниот пејзаж кој брзо се менува.

# 3 Дигитална безбедност

## 3.1 Дигитална безбедност и сајбер безбедност

Според Организацијата за економска соработка и развој (ОЕЦД), **дигиталната безбедност** е од суштинско значење за довербата во дигиталната ера. ОЕЦД ја олеснува меѓународната соработка и развива анализа на политики и препораки во дигиталната безбедност од раните 1990-ти. Работата во оваа област има за цел да развие и промовира политики кои ја зајакнуваат довербата без да го инхибираат потенцијалот на информациските и комуникациските технологии (ИКТ) за поддршка на иновациите, конкурентноста и растот. Дигиталната безбедност се однесува на економските и социјалните аспекти на сајбер безбедноста, наспроти чисто техничките аспекти и оние поврзани со спроведувањето на кривичниот закон или националната и меѓународната безбедност. Терминот „дигитален“ е во согласност со изразите како што се дигитална економија, дигитална трансформација и дигитални технологии. Таа претставува основа за конструктивен меѓународен дијалог помеѓу засегнатите страни кои сакаат да ја поттикнат довербата и да ги максимизираат можностите од ИКТ [1].

**Дигиталната безбедност** и **сајбер безбедноста** се поврзани, но не се исти. И двете вклучуваат заштита на дигиталните средства и информации од неовластен пристап, употреба или оштетување, но тие се разликуваат по обем и фокус.

**Дигиталната безбедност** се однесува на практиката на заштита на дигиталните податоци, информации и средства од неовластен пристап, кражба или оштетување. Опфаќа поширок опсег на безбедносни мерки кои ги штитат податоците и информациите на различни дигитални платформи и уреди, вклучувајќи компјутери, паметни телефони, таблети и други дигитални технологии.

[1] HTTPS://WWW.OECD.ORG/DIGITAL/DIGITAL-SECURITY/

Мерките за дигитална безбедност може да вклучуваат:

- Заштита со лозинка: Создавање силни и уникатни лозинки за онлајн сметки и уреди.
- Шифрирање на податоци: кодирање податоци за да се спречи неовластен пристап или прекршување на податоците.
- Безбедна комуникација: Користење на протоколи за шифрирање за безбеден пренос на податоци.
- Контроли на пристап: Спроведување дозволи и ограничувања за ограничување на пристапот до чувствителни податоци.
- Безбедност на уредот: Користење функции како заклучување екран и далечинско бришење за изгубени или украдени уреди.

**Сајбер безбедноста** е подгрупа на дигиталната безбедност и се фокусира конкретно на заштита на дигиталните средства од сајбер закани и напади. Тоа вклучува одбрана од неовластен пристап, оштетување или нарушување на дигиталните системи, мрежи и инфраструктури.

Мерките за сајбер безбедност може да вклучуваат:

- Заштита на заштитен ѕид: Поставување бариери за да се спречи неовластен пристап до мрежа.
- Системи за откривање на упад: Мрежи за следење за сомнителни активности и потенцијални закани.
- Заштита од малициозен софтвер: Користење на антивирусен софтвер за откривање и отстранување на малициозен софтвер.
- Планирање на одговор на инциденти: Развивање протоколи за ефективно реагирање на инциденти од сајбер безбедноста.
- Интелигенција за сајбер закани: Собирање и анализа на информации за предвидување и спречување на сајбер заканите.

Дигиталната безбедност опфаќа поширок опсег на практики кои ги штитат податоците и информациите во дигиталната област, додека сајбер безбедноста е специјализирана област фокусирана на одбрана од сајбер закани и напади во дигиталните системи и мрежи. И двете се клучни компоненти за обезбедување на севкупната безбедност и заштита на дигиталните средства и информации.

## 3.2 Закани за сајбер безбедноста со кои се соочуваат возрасните

Возрасните се соочуваат со широк спектар на закани за сајбер безбедноста во денешниот дигитален свет. Еве неколку вообичаени закани за сајбер-безбедноста со кои често се среќаваат возрасните:

- ***Фишинг напади:*** Фишинг е техника што ја користат сајбер-криминалците за да ги измамат поединците да обезбедат чувствителни информации, како што се ингеренциите за најавување, броеви на кредитни картички или лични податоци. Фишинг-мејловите,

пораките или веб-локациите може да изгледаат како да се од доверливи извори, но тие имаат за цел да ги измамат корисниците да ги откријат нивните информации.

- ***Злонамерен софтвер:*** Злонамерниот софтвер е злонамерен софтвер дизајниран да се инфилтрира, оштети или да добие неовластен пристап до компјутерските системи. Видови на малициозен софтвер вклучуваат вируси, откупни софтвери, шпионски софтвери и тројанци. Злонамерниот софтвер може да се шири преку злонамерни прилози за е-пошта, заразени веб-локации или компромитиран софтвер.
- ***Кражба на идентитет:*** Сајбер-криминалците можат да украдат лични информации, како што се броеви за социјално осигурување, датуми на раѓање или финансиски податоци, за да извршат кражба на идентитет. Овие информации често се добиваат преку прекршување на податоците или обиди за фишинг.
- ***Онлајн измами:*** Постојат бројни онлајн измами насочени кон возрасни, како што се измами со лотарија, романтични измами, лажни измами за техничка поддршка и лажни инвестициски шеми. Измамниците користат различни тактики за да манипулираат со поединци да испраќаат пари или да даваат лични информации.
- ***Прекршување на податоците:*** Прекршувањето на податоците се случува кога чувствителни информации што ги поседуваат компании или организации се изложени или украдени. Како возрасен, може да бидете погодени од прекршување на податоците ако вашите лични податоци се зачувани од засегнати субјекти.
- ***Социјален инженеринг:*** Социјалниот инженеринг вклучува манипулирање со поединци за да се откријат доверливи информации или да се извршат одредени активности. Сајбер-криминалците може да користат техники на социјален инженеринг за да добијат неовластен пристап до системи или сметки.
- ***Напади со лозинки:*** слабите лозинки или повторната употреба на лозинката може да доведат до напади со лозинки, како што се напади со брутална сила или напади на речник, каде што сајбер-криминалците се обидуваат да погодат или пробијат лозинки за да добијат неовластен пристап.
- ***Јавни ризици за Wi-Fi:*** Користењето јавни Wi-Fi мрежи може да ги изложи возрасните на безбедносни ризици, бидејќи овие мрежи може да немаат соодветно шифрирање и се подложни на прислушување од напаѓачите.
- ***Внатрешни закани:*** Внатрешните закани вклучуваат вработени или поединци со овластен пристап до системи или податоци намерно или ненамерно предизвикуваат штета или протекуваат чувствителни информации.
- ***Ранливост на IoT:*** зголеменото усвојување на уредите „Интернет на нештата“ (IoT) може да создаде ризици за сајбер безбедноста, бидејќи многу од овие уреди може да имаат несоодветни безбедносни мерки и може да бидат искористени од сајбер-криминалци.

За да се заштитат од овие закани, возрасните треба да практикуваат добра сајбер-безбедност хигиена, вклучително и користење силни и уникатни лозинки, овозможување автентикација со повеќе фактори, ажурирање на софтверот и уредите, претпазливост на сомнителни е-пошта и линкови и внимавање на информациите тие споделуваат онлајн. Редовната обука за подигање на свеста за сајбер-безбедноста може да им помогне и на поединците да останат информирани за новите закани и најдобрите практики за да останат безбедни на интернет. Следниот дел детално ги прикажува некои од најважните практики за дигитална безбедност за возрасните за да го намалат ризикот да станат жртви на закани за сајбер безбедноста и да ги заштитат нивните дигитални идентитети и средства.

## 3.3 Практики за дигитална безбедност за возрасни

Практиките за дигитална безбедност се од суштинско значење за возрасните да ги заштитат своите лични информации, податоци и онлајн сметки од закани за сајбер-безбедноста. Еве неколку важни практики за дигитална безбедност што возрасните треба да ги следат:

- ***Користете силни и уникатни лозинки:*** Возрасните треба да креираат силни и уникатни лозинки за нивните онлајн сметки. Избегнувајте користење на лозинки кои лесно може да се погодат како „123456“ или „password“. Размислете за користење на управувач со лозинки за безбедно генерирање и складирање на сложени лозинки.
- ***Овозможи мулти-факторска автентикација (MFA):*** Секогаш кога е можно, овозможете повеќефакторска автентикација на вашите онлајн сметки. MFA додава дополнителен слој на безбедност со тоа што бара втор облик на потврда, како што е еднократна шифра испратена до вашиот мобилен уред, покрај лозинката.
- ***Одржувајте ги ажурирани софтверот и уредите:*** редовно ажурирајте го оперативниот систем, веб-прелистувачите и софтверските апликации. Ажурирањата често вклучуваат безбедносни закрпи кои се однесуваат на познатите пропусти.
- ***Бидете внимателни со е-пошта и врски:*** бидете внимателни кога отворате е-пошта од непознати испраќачи или кликнувате на сомнителни врски. Бидете особено внимателни на е-поштата што бараат чувствителни информации или ве упатуваат да се најавите на лажна веб-локација.
- ***Обезбедете ја вашата домашна мрежа:*** променете ја стандардната лозинка на вашиот домашен рутер за Wi-Fi и овозможете шифрирање WPA2 или WPA3 за да ја заштитите вашата безжична мрежа. Избегнувајте користење на јавни Wi-Fi мрежи за чувствителни активности освен ако не користите виртуелна приватна мрежа (VPN).
- ***Редовно правете резервни копии на податоците:*** редовно правете резервна копија од вашите важни датотеки и податоци на надворешен хард диск, складирање облак или безбедна услуга за резервна копија. Во случај на загуба на податоци или напади на откупнина, резервната копија гарантира дека можете да ги вратите вашите датотеки.
- ***Користете безбедна Wi-Fi и HTTPS:*** кога пристапувате до чувствителни веб-локации, проверете дали користат HTTPS шифрирање. Побарајте го симболот за катанец во лентата за адреси на прелистувачот за да ја потврдите безбедноста на веб-локацијата.
- ***Внимавајте на социјалните медиуми:*** Бидете внимателни за информациите што ги споделувате на платформите на социјалните медиуми. Избегнувајте објавување лични податоци како вашата адреса, телефонски број или планови за патување, бидејќи овие информации може да се користат за напади од социјален инженеринг.
- ***Инсталирајте антивирус и безбедносен софтвер:*** користете реномиран антивирус и безбедносен софтвер на вашите уреди за да се заштитите од малициозен софтвер и други закани. Одржувајте го софтверот ажуриран за да обезбедите оптимална заштита.
- ***Едуцирајте се за сајбер-безбедноста:*** бидете информирани за најновите закани и најдобри практики за сајбер-безбедноста со читање реномирани извори, присуство на вебинари или учество во програми за подигање на свеста за сајбер-безбедноста (Ве молиме погледнете ги ресурсите за дигитална безбедност достапни за возрасни.).

Со вклучување на овие практики за дигитална безбедност во нивните секојдневни рутини, возрасните можат значително да го намалат ризикот да станат жртви на заканите за сајбер безбедноста и да ги заштитат своите дигитални идентитети и средства.

## 3.4 Ресурси за дигитална безбедност достапни за возрасни

Едукативниот центар за сајбер безбедност [2](CEH) на Државниот универзитет во Калифорнија Сан Маркос нуди ресурси и насока за напорите на кампусот и заедницата за зголемување на образованието и свеста за дигиталната безбедност. CEH е заеднички напор на Канцеларијата за информатичка безбедност на кампусот, Колеџите за наука и математика и бизнис администрација.

CEH работи на тоа да осигура дека образовните програми за дигитална безбедност на кампусот се однесуваат на широки прашања поврзани со тековните настани во областа на дигиталната безбедност и обезбедува можности темите за дигитална безбедност да се вклучат во курсевите што се изучуваат низ универзитетот. CEH исто така нуди ресурси за студентите, студентските организации и поширокатa јавност. Ја промовира и олеснува комуникацијата и соработката со образованието за дигитална безбедност низ целата заедница. Тие обезбедија материјали за учење на теми како што се приватноста и социјалните медиуми, безбедноста на сајбер безбедноста за студентите, сајбер-безбедноста денес и концептите за сајбер-безбедност.

Покрај тоа, во 2008 година [3]беа воведени материјали за обука за сајбер безбедност на ENISA. Оттогаш е проширен со нови делови кои содржат критични информации за успех во областа на сајбер безбедноста. ENISA содржи материјали за обука како што се прирачници за наставници, алатки за ученици и виртуелни слики за дополнување на практични сесии за обука.

# 4 Најдобри практики за градење дигитална безбедност за возрасни

Дигиталната безбедност е сè поважна во нашето поврзано општество, а постарите луѓе се една од најранливите групи на интернет. Како што напредува технологијата, така се зголемуваат и сајбер заканите. Затоа е важно да се воспостават мерки и упатства за заштита на постарите возрасни лица во дигиталната средина. Подолу се дадени некои добри практики и успешни акции спроведени во неколку земји кои можат да послужат како референца за други.

Стратегијата за сајбер безбедност на Европската унија претставена во извештаите кои се достапни на официјалната веб-страница на Европската комисија и даваат вредни увиди во најдобрите практики за подобрување на дигиталната безбедност во Европа.

[2]https://www.csusm.edu/cybersec-hub/index.html

[3]https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material

## 4.1 Клучни прашања за изградба на дигитална безбедност

Овој дел може да изгледа како повторување на Дел 3.3. Практики за дигитална безбедност за возрасни, но содржи повеќе сценарија и примери од реалниот свет.

***Силни лозинки:*** Помогнете им да создадат силни и уникатни лозинки за секоја сметка. Лозинките мора да бидат долги и да содржат големи и мали букви, бројки и специјални знаци. Лозинките мора да бидат долги (најмалку 8 знаци), да содржат големи и мали букви, бројки и специјални знаци. Избегнувајте да користите предвидливи лични информации, како што се имиња или датуми на раѓање. Потсетете ги да не ги споделуваат своите лозинки со никого и редовно да ги менуваат.

На пример, силна лозинка може да биде „P@ssw0rd2023!“ кој комбинира големи букви, мали букви, бројки и специјални знаци. Избегнувајте да користите предвидливи лични информации како имиња или датуми на раѓање, како што се „John1980“ или „MarySmith123“.

***Образование и подигање на свеста:*** *информирајте* ги за ризиците и заканите преку Интернет, како што се фишинг, малициозен софтвер и кражба на идентитет. Помогнете им да разберат како да ги препознаат и избегнат овие ситуации. Важно е да ги едуцирате за ризиците на интернет, како што се фишинг (обиди за измама да се добијат доверливи информации), малициозен софтвер (малвер) и кражба на идентитет. Научете да ги препознавате овие предупредувачки знаци и избегнувајте да паднете во овие стапици. Објаснете ги можните негативни ефекти и како да се заштитите.

На пример, објаснете дека е-поштата за фишинг може да изгледа дека се од легитимни извори, барајќи од нив да кликнат на врски и да внесат чувствителни информации. Покажете им примери на сомнителни е-пошта и како да ги идентификувате. Обезбедете информации за вообичаените типови на малициозен софтвер, како лажен антивирусен софтвер или скокачки прозорци, и како да ги избегнете.

***Двофакторна автентикација (2FA):*** Помогнете им да имплементираат двофакторна автентикација секогаш кога е можно. Ова додава дополнителен слој на безбедност на вашите сметки. Двофакторната автентикација додава дополнителен слој на безбедност. Помогнете им да ја овозможат оваа функција на нивните сметки ако е можно. 2FA бара друг метод за автентикација покрај стандардната лозинка, како што е код за текстуална порака, автентикатор или отпечаток од прст.

На пример, откако ќе ја внесат лозинката, ќе добијат текстуална порака со код за потврда што треба да го внесат за да пристапат до нивната сметка. Ова додава дополнителен слој на безбедност и го отежнува пристапот на неовластени корисници до нивните сметки.

***Безбедно користење на мобилни уреди:*** *Помогнете* им да постават заклучување екран, препознавање лице или отпечатоци од прсти за да ги заштитат своите мобилни уреди. Потсетете ги да не ги споделуваат своите уреди со луѓе што не ги познаваат и да бидат внимателни кога преземаат апликации од несигурни извори.

На пример, покажете им како да овозможат PIN или да го користат отпечатокот за да го отклучат паметниот телефон. Потсетете ги да не ги споделуваат своите уреди со луѓе што не ги познаваат и да бидат внимателни кога преземаат апликации од несигурни извори.

***Ажурирања на софтверот:*** проверете дали вашите уреди (компјутери, таблети, паметни телефони) ги имаат инсталирано најновите безбедносни закрпи и ажурирања. Ажурирањата често вклучуваат поправки за познати пропусти, така што ажурирањето на вашите уреди помага да се заштитат.

***преку Интернет :*** Потсетете ги да купуваат само на сигурни и безбедни веб-локации и да користат безбедни начини на плаќање. Научете ги да бараат заклучување во лентата за адреси и да користат безбедни начини на плаќање, како што се кредитни картички со дополнителни безбедносни мерки.

***Безбедно користење на е-пошта:*** Предупредете ги за фишинг и советувајте ги да избегнуваат кликнување на врски или преземање прилози од непознати испраќачи. Предупредете ги за фишинг преку е-пошта, каде што измамниците се обидуваат да добијат чувствителни информации претставувајќи се како легитимни испраќачи. Ова ја нагласува важноста да не се кликаат врски или да не се преземаат прилози од сомнителни е-пошта или непознати испраќачи. Ве повикува да ја потврдите легитимноста на е-пораките со испраќачот пред да испратите доверливи информации.

***Социјални медиуми:*** Помогнете им да ги приспособат поставките за приватност на нивните социјални медиуми за да контролираат кој ги гледа нивните објави и да избегнуваат споделување чувствителни лични информации. Научете ги да избегнуваат да споделуваат чувствителни информации, како што се телефонски броеви, адреси или финансиски информации јавно на социјалните мрежи.

На пример, водете ги низ поставките за приватност на Facebook за да ограничите кој може да ги гледа нивните објави само на пријатели. Нагласете ја важноста да се биде внимателен при споделување информации како телефонски броеви, адреси или финансиски детали на платформите на социјалните медиуми.

***Безбедно прелистување:*** научете да ги препознавате овие безбедни веб-локации („https“ и „заклучување“) и избегнувајте кликнување на сомнителни врски или преземање непознати датотеки. Научете ги да разликуваат безбедни веб-локации со проверка на нивната лента за адреси за заклучување и дали се отворени. „http“ наместо „https“. Објаснете ја важноста од избегнување кликнување на сомнителни врски или преземање датотеки од непознати извори, бидејќи тие може да содржат малициозен софтвер или да ве пренасочат кон лажни веб-локации.

***Безбедност на Wi-Fi:*** проверете дали користат силни лозинки на нивната домашна Wi-Fi мрежа и избегнувајте поврзување со јавни или непознати Wi-Fi мрежи. Објаснете ја важноста од користењето силни лозинки на вашата домашна Wi-Fi мрежа и избегнувајте поврзување со јавни или

непознати Wi-Fi мрежи. Необезбедените Wi-Fi мрежи потенцијално може да бидат нападнати или пресретнати заради шпионажа на податоци.

***Неактивни сметки:*** Помогнете им да ги затворат или избришат онлајн сметките што веќе не ги користат за да го намалат безбедносниот ризик. Неактивните сметки може да бидат ранливи на напади, особено ако содржат лични информации.

***Пазете се од сомнителни повици и пораки:*** научете ги да не откриваат лични или финансиски информации на неочекувани повици или пораки. Научете ги да бидат внимателни кога откриваат лични или финансиски информации на неочекувани повици или СМС пораки. Охрабрете го испраќачот да го потврди својот идентитет пред да сподели чувствителни информации. На пример, наведете примери за вообичаени измами, како што се лажни повици за техничка поддршка или известувања за добивка на лотарија.

***Надзор и поддршка:*** Понудете им помош при редовните проверки на вашите онлајн сметки и помогнете им доколку се сомневаат во сомнителни активности или имаат безбедносни проблеми. Бидете во тек со најновите онлајн закани и давајте постојани насоки и поддршка. На пример, покажете им како да ја прегледаат нивната неодамнешна активност на сметката и најавувањата на различни платформи.

***Лични информации:*** Научете ги да бидат внимателни кога споделуваат лични информации на интернет и да го ограничат количеството на информации што ги објавуваат. Ограничете ја количината на информации што ги објавуваат, како што се адреси, телефонски броеви или информации за училиштата. Ја поттикнува приватноста и важноста за заштита на вашиот онлајн идентитет.

***Бекап на важни податоци:*** Редовно правете резервни копии на важни податоци за да спречите губење во случај на нарушување на безбедноста или дефект на уредот.

## 4.2 Најдобри практики низ светот

### *4.2.1 Сајбер Европа*

ENISA ја организира Cyber Europe [4]од 2010 година, серија вежби за управување со сајбер инциденти и кризи со возбудливи сценарија инспирирани од настани од реалниот живот и развиени од европски експерти за сајбер безбедност. На секои две години, јавниот и приватниот сектор од земјите на ЕУ и ЕЕА, како и европските институции, тела и агенции, соработуваат за зајакнување на нивните постоечки технички и оперативни способности.

Вежбата Cyber Europe се одржува во текот на два дена и симулира големи инциденти на сајбер безбедноста кои ескалираат до сајбер кризи што ја погодуваат целата ЕУ. Учесниците во оваа вежба

[4]https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises/cyber-europe-programme

ќе можат да анализираат напредни технички инциденти за сајбер-безбедност, да се справат со сложени деловни континуитет и ситуации за управување со кризи кои бараат координација и соработка, од локално до ниво на ЕУ.

Серијата вежби Cyber Europe има за цел да ја подобри подготвеноста на Европа за справување со големи инциденти и кризи од сајбер безбедноста, дозволувајќи им на учесниците да ја тестираат и подобрат својата подготвеност низ ЕУ, да градат доверба во екосистемот за сајбер безбедност на ЕУ и да обезбедат можности за обука.

Учеството во Сајбер Европа дава одлична можност да:

- Подигнување на сајбер свеста
- Креирајте и/или ставете ги на тест процедурите за управување со сајбер кризи
- Подобрете ја комуникацијата во ланецот на сајбер одговор
- Создадете заеднички јазик и подобрете го разбирањето еден со друг
- Развијте различни индивидуални и колективни способности и вештини за издржливост
- Анализирајте сложени технички инциденти за сајбер безбедноста; да се справи со сложените деловни континуитет и ситуации за управување со кризи.

### *4.2.2 Адаптација на интерфејс и технологија*

Јапонија е пионер во прилагодувањето на технологијата и уредите за да ги направи подостапни за постарите луѓе. На пример, некои јапонски паметни телефони и таблети имаат поедноставни кориснички интерфејси и подобрени функции за пристапност, што ги прави полесни за користење за луѓе со ограничени дигитални вештини. Други земји и производители на технологија може да усвојат такви политики за да се осигураат дека постарите возрасни лица можат безбедно и ефективно да ги користат дигиталните уреди. Усвојувањето на овие практики од страна на други земји и производители на технологија може да обезбеди дека постарите возрасни лица имаат пристап до повеќе кориснички дигитални уреди, помагајќи да се подобри нивната онлајн безбедност и учество.

Постојат неколку курсеви на европска територија кои имаат за цел да ја подигнат свеста за употребата на овие алатки од страна на постарите луѓе. На пример, здружението ACDA во Париз нуди евтини курсеви за воведување на постарите луѓе во светот на технологијата. Курсевите на оваа асоцијација нудат можност да научите од основите како да ракувате со компјутер. Откривање на компјутерски единици, апликации, формати на датотеки. После тоа, учесниците можат да стекнат понапредни вештини како што се управување и организирање на сопственото поштенско сандаче и учење на употребата на зборот за тоа како да се обработи пишан документ [5].

### *4.2.3 Линии за помош и специјализирана поддршка*

Сингапур воспостави сопствена линија за помош за постарите кои се соочуваат со проблеми со дигиталната безбедност. Оваа линија за помош нуди совети и техничка помош за решавање на проблемите со сајбер безбедноста. Други земји може да размислат за воведување слични услуги за да обезбедат директен и безбеден канал за комуникација за постарите лица на кои им е потребна

[5]http://www.aucoursdesages.fr/cours.php

помош преку Интернет. Овие услуги им обезбедуваат на постарите луѓе директен и безбеден комуникациски канал за да добијат помош за прашања поврзани со сајбер безбедноста, како што се онлајн измами или малициозен софтвер. Воведувањето слични услуги во други земји може да биде важна мрежа за поддршка за заштита на постарите луѓе во дигиталниот свет.

На пример, на европска територија, здружението AGE UK [6]дава приоритет на поддршката на постарите луѓе најранливи на дигитално исклучување.

Покрај обезбедувањето услуги за постарата популација, курсевите ќе се фокусираат конкретно на помагање на група со висок ризик за пристап до дигиталниот свет. Иако основните компоненти на програмата ќе останат во голема мера непроменети додека се работи со овие високоризични групи, веројатно ќе бидат неопходни некои прилагодувања за да се осигура дека програмата ќе остане достапна и ефикасна за оние на кои им е најпотребна.

Услугите со висок ризик во Програмата за дигитален шампион ќе бидат насочени кон постари луѓе кои:

- Имате деменција и/или губење на меморијата
- Имајте низок приход
- Живеј сам
- Имаат проблеми со подвижноста
- Се затворени дома.

### *4.2.4 Кампањи за подигање на свеста и едукација*

Земјите како Австралија и Канада спроведоа кампањи за сајбер-безбедност и програми за едукација за дигитална безбедност за постарите возрасни лица. Овие кампањи обезбедуваат информации за вообичаените сајбер закани, совети како да се заштитите од онлајн измами и важноста да ги ажурирате вашите уреди. Владите можат да соработуваат со локални организации, центри на заедницата и волонтерски групи за да допрат до постарата популација и да обезбедат обука за дигитални вештини. Овие информативни и едукативни кампањи имаат за цел да ги зајакнат старите лица преку едукација за дигитална безбедност. Тие се учат како да идентификуваат и избегнуваат онлајн измами, да ги заштитат своите лични податоци и да користат безбедносни алатки како што се антивирус и силни лозинки. Тие исто така се информирани за ризиците поврзани со користењето на социјалните медиуми и важноста на правилните поставки за приватност на интернет. Здружението наведено погоре ACDA во Париз нуди и курсеви за дигитална безбедност.

Друга асоцијација која се фокусира на дигиталната свест е Orange Foundation која ги информира кревките групи за најновата технологија и ги насочува кон побезбедна дигитална употреба [7].

Понатаму, Orange фондацијата организира низа бесплатни курсеви за дигитална обука низ Франција за млади луѓе и жени кои често се невработени, немаат квалификации, а понекогаш и во несигурни ситуации. Обучувајќи ги овие луѓе за дигитални вештини, тие им помагаат да се

[6]https://www.ageuk.org.uk/our-impact/programmes/digital-skills/digital-champions/

[7]https://fondationorange.com/en/digital-solidarity

ресоцијализираат, да бараат работа, да ја прифатат професионалната употреба на дигиталната технологија, да развијат бизнис, па дури и да ја направат дигиталната професија.

### *4.2.5 Програми за финансиска заштита*

Земјите како што се Велика Британија и САД [8]воведоа политики за заштита на пензионерите од онлајн финансиски измами. Овие политики вклучуваат ограничувања на одговорност за жртвите на измама и правни лекови за враќање на украдените средства. Другите земји можат да ги истражат овие иницијативи и да ги приспособат на нивните финансиски системи за да ги заштитат постарите лица од потенцијални финансиски загуби. Финансиската заштита за постарите возрасни лица е важен дел од дигиталната безбедност. Програмите специјално дизајнирани за спречување и ублажување на онлајн финансиската измама може да и обезбедат на оваа популација поголемо ниво на безбедност. Поставувањето ограничувања на одговорноста на жртвите на измама и создавање механизми за враќање на украдените пари се чекори што може да се преземат. Овие политики не само што ја штитат финансиската благосостојба на постарите возрасни лица, туку и испраќаат јасна порака дека нивната благосостојба и финансиска сигурност се сфаќаат сериозно.

Во Европа Поставувањето ограничувања на одговорноста на жртвите на измама е витален аспект за заштита на финансиската благосостојба на постарите возрасни лица. Кога жртвите на измама се одговорни за финансиските загуби што ги претрпуваат, тоа може да доведе до тешки последици, вклучувајќи финансиска пропаст и емоционална вознемиреност. Со имплементирање на политики кои воспоставуваат разумни ограничувања на одговорноста, општеството ги препознава уникатните ранливости со кои се соочуваат постарите возрасни лица и се обидува да го олесни товарот што им се става. Оваа мерка обезбедува безбедносна мрежа, осигурувајќи дека постарите возрасни лица не се неправедно оптоварени со последиците од измамните активности. Воспоставувањето ограничувања на одговорноста на жртвите на измама е клучен аспект за заштита на финансиската благосостојба на постарите лица. На европско тло, многу здруженија се посветени на заштита на старите лица кои често се жртви на онлајн измами, кои немаат свест и може да претрпат финансиски загуби. Една таква асоцијација е Маркетинг Менаџмент ІО (ММІО) сертифицирана агенција во Шпанија и Франција.[9]

Кога жртвите на измама се сметаат за одговорни за нивните финансиски загуби, тоа може да доведе до сериозни последици. Оттука и важноста на свесноста. Со имплементирање на политики кои поставуваат разумни граници на одговорноста, општеството ги препознава уникатните ранливости на постарите лица и се обидува да го олесни товарот врз нив. Оваа мерка обезбедува безбедносна мрежа, осигурувајќи дека постарите лица не се неправедно оптоварени од последиците од измамничките активности.

Маркетинг менаџмент ІО (ММІО) вклучува теми како што се можности за Интернет, природно референцирање, онлајн видливост, маркетинг на содржина и зголемување на продажбата. Концептите се поедноставени, а дејствијата се бесплатни. Достапни се и ресурси за бонуси.

[8]https://www.bankofamerica.com/signature-services/elder-financial-services/

[9]https://www.marketing-management.io/blog/formation-digital-marketing

Курсот вклучува 5 лекции со видеа. Фејсбук нуди платформа со бесплатен пристап до над 70 онлајн курсеви. Овие курсеви се фокусираат конкретно на користење на Facebook за подобрување на вашето онлајн присуство и бизнис продажба, безбедност и свесност.

### *4.2.6 Соработка со Технолошката индустрија*

Некои земји, како што се Соединетите држави, соработуваа со технолошки компании за да се справат со предизвиците за дигитална безбедност поврзани со стареењето на населението. Оваа соработка може да вклучува подобрување на безбедносниот софтвер, подобрување на откривањето измами и имплементирање безбедносни карактеристики во дигиталните производи и услуги. Соработката со технолошката индустрија може да биде ефикасен начин за следење на најновите безбедносни закани и решенија, како што се имплементација на напредни безбедносни технологии, подобрување на откривањето измами и промовирање безбедносни практики за дигитални производи и услуги наменети за стари лица. Соработката со технолошката индустрија обезбедува побрз и поажурен одговор на дигиталните закани.

Други земји како Франција и Англија имаат курсеви за дигитална безбедност за да им помогнат на постарите луѓе да ги разберат одбранбените технологии; понудените курсеви им овозможуваат да изградат основа за дигитализација и да разберат како безбедно да се движат на Интернет.

На пример, Konexio [10]нуди обука за дигитални вештини - од најосновните до најнапредните - за промовирање на социјалната и професионалната интеграција. Иновативни, базирани на практични студии на случај и со силен акцент на трансверзалните и релационите вештини или меките вештини, нашите курсеви за обука имаат за цел да им овозможат на сите да бидат вклучени во дигитализацијата на општеството. Тие нудат различни формации: дигитални вештини, веб-дизајнер, техничар за системи и мрежи, дигитални помошници. Програмата се фокусира на учење на меките вештини и социјалните кодови на професионалниот свет преку работилници. Исто така, нуди можности за директно поврзување со професионалниот свет преку нашата мрежа. Нуди редовно следење и персонализирана поддршка за да им помогне на нашите ученици да напредуваат и да ги решат сите тешкотии со кои може да се сретнат.

### *4.2.7 Меѓународни ресурси, извештаи и иницијативи*

Овие ресурси обезбедуваат вредни насоки и најдобри практики за подобрување на дигиталната безбедност во образованието за возрасни во ЕУ.

**Отворен, безбеден и безбеден сајбер-простор** : Овој извештај дава преглед на стратегијата за сајбер-безбедност на ЕУ, која има за цел да промовира отворен, безбеден и безбеден сајбер-простор во Европа. Извештајот вклучува најдобри практики за подобрување на сајбер безбедноста, вклучувајќи управување со ризик, одговор на инциденти и јавно-приватно партнерство.

**Извештај за пејзажот на заканите на ENISA:** Овој извештај на Агенцијата за сајбер безбедност на Европската унија (ENISA) дава преглед на тековниот пејзаж на закани од сајбер-безбедноста во Европа, вклучувајќи ги најчестите видови сајбер-напади и секторите кои се најзагрозени. Извештајот

[10]https://www.konexio.eu/formations.html

вклучува најдобри практики за спречување и ублажување на сајбер-напади, вклучително и обука за свесност за безбедноста, управување со ранливоста и планирање одговор на инциденти.

**Директива за НИС и Закон за сајбер-безбедност на ЕУ:** Овој извештај дава преглед на правната рамка на ЕУ за сајбер-безбедност, вклучувајќи ја Директивата за мрежи и информациски системи (НИС) и Законот за сајбер безбедност на ЕУ. Извештајот ги вклучува најдобрите практики за усогласување со законските барања, како што се известување за инциденти и управување со ризик.

**Рамка за сертификација на сајбер безбедност на ЕУ:** Овој извештај дава преглед на рамката за сертификација на сајбер безбедност на ЕУ, која има за цел да ја подобри безбедноста и доверливоста на дигиталните производи и услуги. Извештајот ги вклучува најдобрите практики за добивање и одржување на сертификати за сајбер-безбедност, вклучително и безбедност преку дизајн, тестирање и евалуација, како и тековно следење и оценување.

**Сајбер-безбедност за малите и средните претпријатија:** Овој извештај дава насоки и најдобри практики за малите и средни претпријатија (МСП) за тоа како да ја подобрат нивната сајбер-безбедност. Извештајот вклучува совети за управување со ризик, обука за свесност за безбедноста, безбеден развој на софтвер и планирање одговор на инциденти.

**Дигитални вештини кај возрасната популација:** Овој извештај на Европската комисија дава преглед на дигиталните вештини на возрасната популација во ЕУ. Вклучува дел за дигитална безбедност, кој ја нагласува потребата возрасните да имаат основни знаења и вештини за да се заштитат од сајбер заканите.

**Дигитални вештини за доживотно учење** : Овој извештај на Европската комисија обезбедува насоки и најдобри практики за развој на дигитални вештини кај возрасните. Вклучува дел за дигитална безбедност, кој дава совети за управување со ризик, безбедно прелистување, управување со лозинка и заштита на податоците.

**Проект Cybersecurity for Digital Education:** Овој проект на European Schoolnet обезбедува ресурси и обука за сајбер безбедноста за наставниците и учениците во Европа. Проектот вклучува низа материјали, вклучувајќи онлајн курсеви, планови за часови и алатки за оценување, сите фокусирани на подобрување на дигиталната безбедност во образованието.

**Проект за дигитална безбедност за постарите граѓани:** Овој проект на Агенцијата за сајбер безбедност на Европската унија (ENISA) обезбедува ресурси и обука за сајбер-безбедност за постарите граѓани. Проектот вклучува низа материјали, вклучувајќи онлајн курсеви, водичи и видеа, сите фокусирани на подобрување на дигиталната безбедност кај постарите возрасни лица.

**Коалиција за дигитални вештини и работни места:** Оваа иницијатива на Европската комисија има за цел да ги подобри дигиталните вештини на Европејците за да им овозможи целосно учество во дигиталната економија. Вклучува низа ресурси и можности за обука, вклучително и за дигитална безбедност.

# 4. 3 Најдобри практики за образование на возрасни за дигитална безбедност

***ENISA Обучи програма за обучувачи***

Сите онлајн материјали за обука и курсеви за обука во делот „Курсеви за обука за специјалисти за сајбер безбедност“ се засноваат на филозофијата „Обучи го тренерот“. Програмата и филозофијата „Обучи го тренерот“ имаат за цел да ја прошири мрежата на обучувачи и да промовира подобра размена на информации. Ова ќе служи за неколку цели, вклучувајќи:

- Споделување на материјали за обука за да заштедите време и пари за обука,
- Создавање регионални напори за обука,
- Поттикнување на соработка меѓу различни даватели на обуки,
- Промовирање на добри практики за обука,
- Намалување на конкуренцијата и дуплирање.

Онлајн материјалите за обука на ENISA ќе вклучуваат Прирачник за обучувачи, сет на алатки за студенти и Виртуелни машини за преземање. Ова им овозможува на потенцијалните обучувачи да го подготват курсот, а Прирачникот ќе им помогне да ги водат студентите низ курсот. Ќе содржи листови со измами, потенцијални мали тестови за да се види дали учениците ги сфатиле важните лекции од курсевите и дополнителни информации или вежби кои тренерот може да ги користи за да го направи курсот поинтересен или попредизвикуван.

Учењето од меѓусебните успеси и неуспеси им овозможува на почетниците и на искусните тренери подобро да дизајнираат и испорачуваат обуки, правејќи ги поуспешни, по „позабавни“ и со подобри и подолготрајни резултати.

***TiK – Технологија накратко***

Високо-технолошкиот проект следи меѓугенерациски пристап преку обуката што ја нудат млади волонтери (од 16 до 30 години) како т.н. „Тренери за таблети“, кои се едуцираат според специјален таблет-образовен наставен план. Курсевите се разликуваат од мноштво методи и флексибилни водечки прашања и посебна посветеност на младите обучувачи. Тие нудат курсеви со низок праг доброволно за само мал додаток за трошоци. Понатамошниот развој на курсевите е обезбеден со повратните информации на учесниците и обучувачите кои исто така им елаборираа специјални материјали и пратки без бариери за постарите лица. Курсевите се лесно достапни за заинтересираните и се посветува големо внимание на широката географска дистрибуција на „ТиКмодулите“ и информациите на www.digitaleseniorinnen.at. Учесници на курсевите се лица и особено економски загрозени жени на ниско образовно ниво. До крајот на 2018 година со модулите учеа повеќе од 2000 лица, а на курсот-програмата учествуваа уште 1000 лица. Најстариот учесник кој штотуку учествува на курс има 97 години, се образува кај млад човек во градинка. Проектот беше наградуван неколку пати на федерално и провинциско ниво.

# 5 Обука за возрасни: Како да се изгради дигитална еластичност

Андрагогијата како студија за учењето на возрасните потекнува од Европа во 1950-тите, но дури во 1970-тите била пионерска како теорија и модел на учење на возрасни од страна на Малколм Ноулс, американски практичар и теоретичар за образование на возрасни, кој ја дефинирал андрагогијата како „Уметноста и науката за помагање на возрасните да учат“ (Фидишун 2000). Фидишун (2000) предложи андрагошките принципи да се користат при дизајнирањето на онлајн часовите за да се олесни „флексибилноста и способноста на учениците да се движат низ часовите секогаш кога, каде и со сопствено темпо“.

## 5.1 Четири принципи на андрагогијата

Имајќи предвид дека возрасните имаат свој, уникатен начин на учење, постојат 4 централни принципи кои објаснуваат како најдобро да се развие обука за нив.

- Кога станува збор за учење, возрасните сакаат или треба да бидат вклучени во тоа како нивната обука се планира, испорачува и изведува. Тие сакаат да контролираат што, кога и како учат.
- Возрасните добиваат повеќе кога можат да ги привлечат минатите искуства во процесот на учење. Тие можат да се потпираат на она што претходно го знаеле за да додадат поголем контекст во нивното учење.
- Меморирањето на факти и информации не е вистинскиот начин за учење на возрасните. Тие треба да ги решат проблемите и да користат расудување за најдобро да ги прифатат информациите што им се презентирани.
- Возрасните сакаат да знаат „Како можам да ги користам овие информации сега?“. Она што го учат треба да биде применливо во нивните животи и веднаш да се имплементира.

## 5.2 Како тренерите за возрасни ќе спроведуваат андрагогија

### *Овозможување на самонасочено учење*

Во минатото, учењето честопати беше задолжителна активност што се извршуваше во одредено време. Сега со технологии како систем за управување со учење, можеме да создадеме многу посамо-насочена, независна средина за учење за возрасни ученици. Можеме да им дозволиме да тренираат кога и каде сакаат, да им понудиме избор на курсеви на кои можат да изберат да се запишат и да им овозможиме да имаат свои посебни цели за учење.

## *Користење на примери за учење од реалниот свет*

Како што вели теоријата, возрасните сакаат да знаат како обуката ќе има непосредна примена и корист за нив. Значи, кога креираме содржина на курсот, треба да внесеме што повеќе примери од реалниот свет.

Кога обучувате возрасни ученици за дигитална благосостојба и/или дигитална безбедност, одете ги чекор-по-чекор низ работниот тек што всушност ќе го користат и експлицитно наведете како и зошто би го користеле. Наведете како обуката ќе помогне, а потоа користете вистински примери за обука.

## *Дозволете им на возрасните ученици сами да го сфатат тоа*

Со оглед на тоа што возрасните претпочитаат решавање на проблеми наместо само факти, кога креирате содржина, добро е да не ги изложите сите одговори веднаш. Зошто наместо тоа да не бидете креативни и да не изградите курсеви што ќе го поттикнат мозокот на вашите ученици?

Можеме да го направиме тоа на неколку едноставни начини, вклучувајќи додавање проценки и симулации кои ги прикажуваат специфичните проблеми со кои всушност може да се сретне ученикот, а потоа да ги натераме возрасните ученици да ги користат своите вештини за да ги надминат.

# 6 Заклучок

Дигиталната безбедност на постарите луѓе е клучно прашање кое бара внимание и акција од страна на владите и општеството во целина. Со имплементирање на горенаведените добри практики, земјите можат да ја подобрат дигиталната заштита и благосостојбата на нивното стареење на населението. Подигнувањето на свеста, образованието, посветената поддршка, технолошката адаптација и индустриската соработка се клучните столбови за да се обезбеди безбедно и позитивно онлајн искуство за постарите возрасни лица.

Проектот DigiWELL има за цел да ги вклучи принципите за дигитална благосостојба во образованието за возрасни. Нејзините иницијативи се насочени кон придонес кон севкупните практики на организациите, мрежите и иницијативите за образование на возрасни. Проектот разбира колку е клучно да се реши како технологијата влијае на менталното здравје, продуктивноста и општата благосостојба на возрасните во дигиталната ера. Главната цел на DigiWELL е да им обезбеди на возрасните ученици информации, способности и ресурси неопходни за етичка и совесна навигација во дигиталниот свет. Проектот DigiWELL, исто така, вклучува создавање и извршување на дополнителни иницијативи за зајакнување на возрасните ученици. Целта на овие активности е да се обезбеди средина за поддршка каде што возрасните можат да ги споделат своите искуства, тешкотии и триумфи во промовирањето на дигиталната благосостојба. Имајќи го ова на ум, проектот DigiWELL претставува многу можности за поединци и организации за возрасни да станат свесни и просветлени за важноста на дигиталната благосостојба и за тоа како да се промовира дигиталната благосостојба на возрасни индивидуи и возрасни едукатори и обучувачи. Овозможувањето на дигиталната благосостојба со холистички пристап е многу повозможно доколку сите релевантни страни преземаат активности за поддршка на потребите за дигитална благосостојба на поединците. Следствено, информациите, советите и добрите практики презентирани во овој прирачник ги повикуваат луѓето и заинтересираните организации да преземат иницијативи за повеќе од нас да имаат подобра дигитална благосостојба, а исто така и посилен дигитален живот.

# 7 Референци

При подготовката на речникот се користени бесплатни достапни онлајн ресурси: онлајн речници, научни статии и литература од областа на информацискатa безбедност, дигитални технологии и услуги, дигитална благосостојба и дигитална отпорност, како и термини и дефиниции од предметот Информации безбедност. Сите извори се наведени во текстуалната база на податоци на работната верзија на речникот.


1 BAI. Речник на Комитетот за национални безбедносни системи (CNSS) (2015). Во *BAI Консалтинг и обука за безбедност на информации [онлајн]* . Преземено од: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

2 *Речник Каптера* . Каптера. (nd). https://www.capterra.com/glossary/

3 CSRC. (nd). *Речник* . Ресурсен центар за компјутерска безбедност. https://csrc.nist.gov/glossary/

4 *Речник на термини за сајбер-безбедност* . Глобално знаење. (nd). https://www.globalknowledge.com/ca-en/topics/cybersecurity/glossary-of-terms/

5 *Речник* . DigitalHealthEurope. (nd). https://digitalhealtheurope.eu/glossary/

6 *Речник* . Дигитална велнес лабораторија. (2022). https://digitalwellnesslab.org/parents/glossary/

7 ISO. (nd). *ISO/IEC 27032:2023(ен) Сајбер-безбедност — Упатства за безбедност на Интернет* . Платформа за онлајн прелистување (OBP) - ISO. https://www.iso.org/obp/ui/iso

8 Jirásek, P., Novák, L., Požár, J., & Vavrushka, K. (2022). *Výkladový Slovník kybernetické bezpečnosti = Речник за сајбер безбедност . Петто издание.* Praha: Česká pobočka AFCEA, 2022. стр. 352, ISBN 978-80-908388-4-0

9 Кисел, РЛ (2019, 16 јули). *Речник на клучни термини за безбедност на информациите* . НИСТ. https://www.nist.gov/publications/glossary-key-information-security-terms-1

10 МФ СР. (nd). *Metodický pokyn na použitie odborných výrazov pre oblasť informatizácie spoločnosti - CSIRT.SK* . CSIRT.SK. http://www.csirt.gov.sk/wp-content/uploads/2021/08/Metodicky_pokyn_glosar_pojmov.pdf

11 Paulsen, C., & Byers, RD (2021). *Речник на клучни термини за безбедност на информациите* . НИСТ. Преземено од: https://www.nist.gov/publications/glossary-key-information-security-terms-2

12 Stallings, W., & Brown, LV (2015). *Компјутерска безбедност: Принципи и пракса . Трето издание.* Boston, MA: Pearson, 2015. стр.838. ISBN 978-0-13-377392-7. Пирсон.

13 *ТВЕтипедија речник* . UNSECO-UNEVOC. (nd) https://unevoc.unesco.org/home/TVETipedia+Glossary

14 Фидишун, Д. (2000). Учење на возрасни ученици да користат компјутеризирани ресурси: Користење на клучевите на Лолер за учење на возрасни за да се направи наставата поефективна. *Информатичка технологија и библиотеки* , *19* (3), 157-157.

15 Европска комисија, Генерален директорат за образование, млади, спорт и култура, Клучни компетенции за доживотно учење, Канцеларија за публикации, 2019 година, https://data.europa.eu/doi/10.2766/569540