Obrazac za obuku

Naslov	Cyber sigurnost za starije osobe: Alati za sigurnu navigaciju
Ključne riječi	Cyber sigurnost, online sigurnost, digitalna ovisnost, sigurno pregledavanje, zdravstvena tehnologija
Osigurao	Hrvatski telekom d.d.
Jezik	Engleski

Područje za obuku (X gdje je primjenjivo)	
	Informacijska pismenost
	Komunikacija i suradnja
x	Sigurnost
	Rješavanje problema

Ciljevi / Ishodi učenja

Cilj: Cilj ove obuke je educirati starije osobe o kibernetičkoj sigurnosti i pružiti im potrebne alate i znanje za sigurno snalaženje u online svijetu. Ishodi učenja - do kraja ove obuke sudionici će moći:

- Razumjeti važnost kibernetičke sigurnosti
- Prepoznati uobičajene cyber prijetnje
- Vježbajte sigurno pregledavanje interneta
- Zaštitite osobne podatke
- Odgovorite na cyber incidente
- Koristite digitalne tehnologije za zdravlje i dobrobit

Opis

Ova obuka oprema starije osobe osnovnim znanjem i alatima za sigurno snalaženje u online svijetu. Sudionici će naučiti o rizicima kibernetičke sigurnosti i prepoznati uobičajene prijetnje. Razumjet će sigurno pregledavanje interneta i sigurnost e-pošte, osigurati osobne uređaje, zaštititi osobne podatke i ostati sigurni. Obuka također pokriva odgovor na incidente i važnost ažuriranja novonastalih kibernetičkih prijetnji. Također će moći sigurno upravljati digitalnim tehnologijama u odnosu na svoje

Co-funded by the European Union

zdravlje i dobrobit, donositi informirane odluke i iskoristiti mogućnosti koje one pružaju. Na kraju ćete biti ovlašteni zaštititi sebe i svoje osobne podatke na internetu.

Indeks sadržaja (3 razine)

Modul: Kibernetički sigurnosni alati za sigurnu navigaciju

Jedinica 1: Uvod u kibernetičku sigurnost

1.1. Razumijevanje rizika kibernetičke sigurnosti

1.2. Uobičajene vrste kibernetičkih prijetnji

1.3. Važnost kibernetičke sigurnosti za starije osobe

Jedinica 2: Sigurno pregledavanje interneta

2.1. Najbolji primjeri iz prakse za sigurnost u digitalnom okruženju

2.2. Povećanje sigurnosti na mreži pomoću alata za sigurno pregledavanje

Jedinica 3: Zdravlje i dobrobit u digitalnom dobu

3.1. Rizici od prekomjernog vremena ispred ekrana i digitalne ovisnosti

3.2. Zdravlje i digitalni alati

Razrađeni sadržaj

Modul: Kibernetički sigurnosni alati za sigurnu navigaciju

Jedinica 1: Uvod u kibernetičku sigurnost

1.1. Razumijevanje rizika kibernetičke sigurnosti

Razmišljajte o rizicima kibernetičke sigurnosti kao o potencijalnim opasnostima kada idete na internet. Baš kao što poduzimate mjere opreza da biste ostali sigurni u fizičkom svijetu, kao što je zaključavanje vrata, svijest o kibernetičkim rizicima pomaže vam da ostanete sigurni u digitalnom svijetu. Ti rizici mogu uključivati stvari kao što su hakeri koji pokušavaju ukrasti vaše osobne podatke, prijevare koje vas navedu da date svoj novac ili viruse koji mogu oštetiti vaše računalo. Štoviše, kibernetička sigurnost naglašava njegovanje kulture osviještene o sigurnosti promicanjem svijesti i obrazovanja o sigurnim online praksama.

Učenjem o ovim rizicima možete se bolje zaštititi. To je kao da znate znakove skliskog poda kako biste mogli hodati pažljivo i izbjeći pad. Razgovarat ćemo o uobičajenim kibernetičkim rizicima i kako ih prepoznati, tako da možete s povjerenjem upravljati

Co-funded by the European Union

internetskim svijetom i donositi informirane odluke kako biste zaštitili sebe i svoje podatke. Upamtite, znanje je moć, a razumijevanjem rizika kibernetičke sigurnosti poduzimate važan korak prema zaštiti sebe na internetu.

1.2. Uobičajene vrste kibernetičkih prijetnji

U ovoj jedinici istražit ćemo uobičajene vrste cyber prijetnji, a to su različiti načini na koje loši akteri pokušavaju naštetiti vama ili vašem računalu dok koristite internet. Razumijevanje ovih prijetnji pomaže vam da ostanete sigurni i izbjegnete potencijalnu štetu. Razložimo to jednostavnim riječima.

Zamislite kibernetičke prijetnje kao lukave trikove ili zamke koje zli ljudi koriste na mreži. Žele ukrasti vaše osobne podatke, zaraziti vaše računalo štetnim softverom ili vas prevariti da im date svoj novac. Neke uobičajene vrste kibernetičkih (engl *cyber*) prijetnji uključuju stvari poput krađe identiteta, zlonamjernog softvera i krađe identiteta.

Phishing je poput lažne e-pošte ili poruke koja se pretvara da je od nekoga kome vjerujete, ali vas pokušava prevariti da odate svoje osobne podatke. To je kao da se netko pretvara da je prijatelj kako bi dobio pristup tvojim tajnama. Uobičajene phishing poruke su: lažna e-pošta od banke, lažna izvješća o dobicima od kockanja ili igara na sreću, besplatnih nagrada, lažni računi pružatelja IT ili usluga plaćanja, internetskih trgovina, lažne potvrde navodnih naloga ili lažni podsjetnici za plaćanje, lažne poruke o politici privatnosti osobnih podataka ili uvjetima koje treba prihvatiti.

Poruka e-pošte za krađu identiteta može glasiti: Vaša kreditna kartica je istekla, Vaš račun je istekao, privremeno blokiran ili potvrdite svoje podatke za prijavu. Izgled (korporacijski dizajn), adresa pošiljatelja ili izravan pozdrav korisniku mogu stvoriti dojam da se radi o e-poruci koju je poslala banka ili drugi pružatelj usluge. E-mail poruke u HTML formatu prikazuju "legalnu" vezu do primatelja, koja sadrži skrivenu poveznicu u pozadini, koja vodi izravno na lažni ili zlonamjerni sadržaj.

Malware je poput virusa koji može zaraziti vaše računalo i uzrokovati štetu. Može usporiti vaše računalo ili čak ukrasti vaše osobne podatke.

Krađa identiteta je kada netko ukrade vaše osobne podatke, poput vašeg imena, adrese ili podataka o kreditnoj kartici, i koristi ih bez vašeg dopuštenja. To je kao da se netko pretvara da ste vi i koristi vaš novac ili kupuje stvari u vaše ime.

Kradljivci identiteta također mogu u svoje poruke e-pošte integrirati zlonamjerni softver poput virusa ili trojanskog softvera kao poveznicu, privitak ili izvorni kod u poruci e-pošte u HTML formatu. Samo klikanje na sliku u phishing poruci može imati ozbiljne posljedice. Prevaranti koji kradu identitete često koriste adrese koje se tek neznatno razlikuju od originalnih. Kradljivac identiteta može zamijeniti znakove za stvaranje lažnih URL-ova. Na primjer, umjesto originalne adrese kao što je

Co-funded by the European Union

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

http://www.onlinebank.com.hr može koristiti adresu kao što je http://www.on1inebank.com.hr.

Kako znati je li nešto zlonamjerno?

- LAŽNA ADRESA POŠILJATELJA
  Zadržite pokazivač miša iznad adrese pošiljatelja. Sadrži li adresa e-pošte sumnjive elemente? Ima li pravopisnih grešaka u adresi, čak i ako su beznačajne?
- ZAHTJEV ZA POVJERLJIVIM PODACIMA
  Traži li poveznica u e-poruci unos osobnih podataka? Jeste li dužni dati povjerljive informacije poput PIN-a ili lozinke?
- HITNOST
  Traži li e-mail da djelujete odmah ili hitno? Sadrži li poruka prijetnju ili upozorenje?
- VEZE NA LAŽNE WEB-STRANICE
  Koji se URL pojavljuje kada mišem prijeđete preko veze? Je li to sigurna stranica (URL treba započeti s "https://") i šifrirana (simbol lokota ispred URL-a)?
- ČUDNE FORMULACIJE I PRAVOPISNE POGREŠKE
  Je li pozdravna poruka e-poštom općenita? Sadrži li pravopisne pogreške, netočnu interpunkciju ili posebne znakove?

Učenjem o ovim uobičajenim vrstama cyber prijetnji, možete ih prepoznati i poduzeti korake da se zaštitite. Razgovarat ćemo o strategijama kako ostati siguran i izbjeći da postanete žrtva ovih prijetnji, osnažujući vas da uživate u online svijetu s povjerenjem i mirom.

1.3. Važnost kibernetičke sigurnosti za starije osobe

Zamislite kibernetičku sigurnost kao svog osobnog tjelohranitelja u digitalnom svijetu koji brine o vašoj dobrobiti. To je kao da imate nekoga tko pazi na vas i brine da vaši osobni podaci ostanu sigurni, a vaši uređaji sigurni. Kako bismo osigurali kibernetičku sigurnost, moramo prakticirati sigurne internetske navike, kao što je stvaranje jakih i jedinstvenih lozinki, biti oprezni pri klikanju na sumnjive poveznice ili preuzimanju datoteka iz nepoznatih izvora, te održavati svoje uređaje i softver ažuriranima. Nikada nemojte potvrditi svoj broj računa, lozinku ili druge tajne informacije ako se to od vas traži u poruci e-pošte. Prave banke i tvrtke to nikada ne bi koristile iz sigurnosnih razloga.
Prije unosa osobnih podataka provjerite sigurnosni status web stranica. HTTPS ne jamči da je web stranica stvarna. Kliknite na simbol lokota prikazan pokraj URL-a u vašem pregledniku kako biste provjerili sigurnosni certifikat web stranice.
Vjera u nepogrešivost tehnologije može ostaviti prostora za phishing napade. Zdrava razina nepovjerenja sprječava napadače da vam ukradu identitet i pristup vašim računima i informacijskim sustavima.

Jedinica 2: Sigurno pregledavanje interneta

2.1. Najbolji primjeri iz prakse za sigurnost u digitalnom okruženju

Co-funded by the European Union

- Vježbajte navike sigurnog pregledavanja: Držite se pouzdanih web stranica kada kupujete, obavljate bankarstvo ili dijelite osobne podatke na mreži. Potražite simbol lokota i "https://" u adresi web stranice, što ukazuje na sigurnu vezu.
- Budite oprezni s društvenim inženjeringom: čuvajte se neželjenih poziva, poruka ili e-pošte u kojima se traže osobni podaci ili financijski detalji. Legitimne organizacije neće tražiti takve informacije putem neželjenih sredstava
- Redovito sigurnosno kopirajte svoje podatke: izradite sigurnosne kopije važnih datoteka i podataka na zasebnom uređaju za pohranu ili usluzi u oblaku. To pomaže u zaštiti od gubitka podataka zbog kvara hardvera, krađe ili napada (engl *ransomwarea*).
- Omogući dvofaktorsku provjeru autentičnosti (2FA): Aktivirajte 2FA kada god je dostupna. Ovo dodaje dodatnu razinu sigurnosti zahtijevajući sekundarni korak provjere, kao što je jedinstveni kod poslan na vaš mobilni uređaj, uz vašu lozinku.
- Vodite računa o dijeljenju na društvenim mrežama: budite oprezni kada dijelite osobne podatke, detalje o lokaciji ili planove za odmor na platformama društvenih mreža. Prekomjerno dijeljenje može pružiti vrijedne informacije cyber kriminalcima ili potencijalnim provalnicima.
- Osigurajte svoje mobilne uređaje: Primijenite sigurnosne značajke, kao što su šifre, otisak prsta ili prepoznavanje lica, da zaključate svoje pametne telefone i tablete. Instalirajte renomirane sigurnosne aplikacije koje nude značajke poput daljinskog praćenja i brisanja u slučaju gubitka ili krađe.
- Vjerujte svojim instinktima: Ako se nešto čini predobro da bi bilo istinito ili vam se čini sumnjivim, vjerujte svojim instinktima. Budite skeptični prema neočekivanim ponudama, zahtjevima za novcem ili hitnim zahtjevima za osobnim podacima.
- Redovito brisanje podataka pregledavanja: Redovito brišite svoju povijest pregledavanja, kolačiće i podatke u predmemoriji. To pomaže zaštititi vašu privatnost uklanjanjem pohranjenih informacija kojima bi potencijalno mogle pristupiti neovlaštene osobe.

2.2. Povećanje sigurnosti na mreži pomoću alata za sigurno pregledavanje

Poboljšanje internetske sigurnosti alatima za sigurno pregledavanje važan je aspekt kibernetičke sigurnosti. Korištenjem ovih alata možete zaštititi svoju privatnost, osigurati svoje osobne podatke i smanjiti rizik od online prijetnji. Evo nekoliko bitnih savjeta za povećanje vaše online sigurnosti pomoću alata za sigurno pregledavanje:

• Instalirajte i koristite pouzdani web-preglednik: Odaberite renomirani web-preglednik, kao što su Google Chrome, Mozilla Firefox ili Microsoft Edge. Ovi preglednici daju prednost sigurnosti i redovito objavljuju ažuriranja za rješavanje ranjivosti.

Co-funded by the European Union

• Aktivirajte sigurnosne značajke preglednika: Upoznajte se sa sigurnosnim značajkama koje nudi vaš web preglednik. Omogućite značajke kao što su blokatori skočnih prozora, način sigurnog pregledavanja i postavke privatnosti kako biste poboljšali svoju sigurnost na mreži.

• Omogući zaštitu od krađe identiteta i zlonamjernog softvera: Aktivirajte ugrađene značajke zaštite od krađe identiteta i zlonamjernog softvera koje nudi vaš web preglednik. Ove vas značajke mogu upozoriti na sumnjiva web-mjesta i spriječiti vas da posjetite poznata zlonamjerna web-mjesta.

• Budite informirani i ažurirani: Budite informirani o najnovijim prijetnjama na mreži i najboljim praksama za sigurno pregledavanje. Redovito čitajte pouzdane izvore, poput uglednih web-mjesta ili blogova o kiber sigurnosti, kako biste bili u tijeku s razvojem krajolika internetske sigurnosti.

Jedinica 3: Zdravlje i dobrobit u digitalnom dobu

3.1. Rizici od prekomjernog vremena ispred ekrana i digitalne ovisnosti

Kako biste ublažili rizike od prekomjernog vremena ispred ekrana i digitalne ovisnosti, evo nekoliko strategija i praksi koje treba razmotriti:

• Postavite vremenska ograničenja za korištenje zaslona: odredite određena vremenska ograničenja za korištenje zaslona, kako za slobodne aktivnosti tako i za radne zadatke. To pomaže stvoriti zdravu ravnotežu između vremena ispred ekrana i drugih aktivnosti.

• Pravite redovite pauze: uključite redovite pauze od ekrana u svoju dnevnu rutinu. Ustanite, rastegnite se i bavite se fizičkim aktivnostima ili hobijima koji ne uključuju digitalne uređaje.

• Vježbajte digitalnu detoksikaciju: posvetite određena razdoblja, poput vikenda ili večeri, potpunom odvajanju od digitalnih uređaja. Iskoristite ovo vrijeme za izvanmrežne aktivnosti, provedite vrijeme s voljenima ili se bavite hobijima.

• Pažljivo koristite tehnologiju: vodite računa o tome kako koristite tehnologiju i o utjecaju koji ona ima na vašu dobrobit. Razmislite o svojim digitalnim navikama, procijenite njihov učinak na vaš život i donesite svjesne odluke kako biste umanjili negativne posljedice.

• Tražite podršku i odgovornost: Podijelite svoje brige s pouzdanim članovima obitelji, prijateljima ili grupama za podršku. Uspostavite uzajamnu odgovornost za poticanje odgovorne upotrebe tehnologije i pružanje podrške u održavanju zdravih navika.

• Postavite digitalne granice: Definirajte jasne granice za korištenje tehnologije, kao što je isključivanje obavijesti u određeno vrijeme, izbjegavanje vremena ispred ekrana

Co-funded by the European Union

prije spavanja ili postavljanje smjernica za korištenje uređaja tijekom obiteljskih obroka.

Zapamtite, cilj je razviti zdrav odnos s tehnologijom i osigurati da ona obogaćuje vaš život, a ne da postane izvor pretjerane ovisnosti. Primjenom ovih strategija možete ublažiti rizike povezane s prekomjernim vremenom provedenim pred zaslonom i promovirati uravnoteženiji i ispunjeniji način života.

3.2. Zdravlje i digitalni alati

Tehnologija može ponuditi brojne načine za podršku i poboljšanje vašeg zdravlja. Evo nekoliko načina na koje vam tehnologija može pomoći u vašem zdravlju:

- Pristup informacijama: Internet pruža mnoštvo informacija vezanih uz zdravlje, omogućujući vam istraživanje simptoma, stanja, tretmana i preventivnih mjera. Pouzdana web-mjesta, zdravstvene aplikacije i internetske zajednice mogu vas osnažiti da donosite informirane odluke o svom zdravlju.
- Praćenje zdravlja: nosivi uređaji, kao što su uređaji za praćenje fitnessa i pametni satovi, mogu pratiti različite aspekte vašeg zdravlja, uključujući broj otkucaja srca, obrasce spavanja, fizičku aktivnost i potrošene kalorije. Ovi uređaji mogu pružiti dragocjene uvide u vaše cjelokupno blagostanje i pomoći vam u praćenju napretka prema zdravstvenim ciljevima.
- Telezdravstvo i konzultacije na daljinu: Telezdravstvene usluge omogućuju vam da se savjetujete sa zdravstvenim radnicima na daljinu putem video poziva ili online chatova. Ovaj praktični pristup štedi vrijeme i može biti posebno koristan za naknadne preglede, rutinske preglede ili medicinske konzultacije koje nisu hitne.
- Upravljanje lijekovima: Mobilne aplikacije i pametni organizatori tableta mogu vam pomoći u upravljanju lijekovima pružanjem podsjetnika za uzimanje tableta, praćenjem rasporeda uzimanja lijekova i pružanjem upozorenja za ponovno punjenje na recept. Ova tehnologija može spriječiti propuštene doze i potaknuti pridržavanje režima uzimanja lijekova.
- Podrška za mentalno zdravlje: razne aplikacije za mentalno zdravlje i online platforme pružaju resurse za upravljanje stresom, tjeskobom i depresijom. Ti alati mogu uključivati vođenu meditaciju, vježbe disanja, praćenje raspoloženja i terapijske sesije koje se provode putem digitalnih platformi.
- Upravljanje zdravstvenim zapisima: Digitalni zdravstveni zapisi i portali za pacijente omogućuju vam pristup i upravljanje svojom medicinskom poviješću, rezultatima testova i rasporedima termina. Time se pojednostavljuje komunikacija s pružateljima zdravstvenih usluga i osigurava kontinuitet skrbi.
- Podrška i motivacija: Online zajednice i platforme društvenih medija posvećene zdravlju i blagostanju mogu pružiti podršku, motivaciju i ohrabrenje. Povezivanje s istomišljenicima može potaknuti osjećaj zajedništva i pomoći vam da ostanete odgovorni za svoje zdravstvene ciljeve.
- Praćenje zdravlja i analiza podataka: Tehnologija vam omogućuje praćenje i analizu zdravstvenih podataka tijekom vremena, poput krvnog tlaka, razine glukoze u krvi ili težine. Praćenjem trendova i obrazaca možete identificirati

Co-funded by the European Union

područja za poboljšanje i napraviti potrebne prilagodbe kako biste optimizirali svoje zdravlje.

Upamtite, iako tehnologija može biti vrijedan alat u podršci vašem zdravlju, važno ju je koristiti mudro i u kombinaciji s profesionalnim medicinskim savjetima. Uvijek se posavjetujte sa zdravstvenim radnicima za točnu dijagnozu, preporuke za liječenje i personalizirane upute.

Rječnik

Cyber sigurnost odnosi se na praksu zaštite računalnih sustava, mreža i digitalnih informacija od neovlaštenog pristupa, krađe i oštećenja. Uključuje provedbu mjera za sprječavanje cyber prijetnji, kao što su hakiranje, povrede podataka i napadi zlonamjernim softverom. Cilj kibernetičke sigurnosti je osigurati povjerljivost, integritet i dostupnost digitalne imovine, štiteći pojedince i organizacije od potencijalnih rizika i ranjivosti u međusobno povezanom digitalnom svijetu.

Identificiraj krađu odnosi se na lažno stjecanje i korištenje nečijih osobnih podataka, poput imena, broja socijalnog osiguranja ili financijskih podataka, bez pristanka osobe. Uključuje lažno predstavljanje žrtve kako bi se izvršile razne nezakonite aktivnosti, uključujući financijske prijevare, neovlaštene kupnje ili počinjenje drugih oblika zločina povezanih s identitetom.

Društveni inženjering je manipulativna tehnika koju kibernetički kriminalci koriste kako bi prevarili pojedince i iskoristili njihovo povjerenje i emocije. Uključuje psihološku manipulaciju, a ne tehničke metode za prevaru ljudi da otkriju osjetljive informacije ili izvedu radnje koje mogu ugroziti njihovu sigurnost. Primjeri tehnika društvenog inženjeringa uključuju phishing e-poštu, telefonske prijevare, izgovorene poruke i lažno predstavljanje. Cilj društvenog inženjeringa je manipulirati ljudskim ponašanjem kako bi se dobio neovlašteni pristup sustavima, mrežama ili osobnim podacima.

pitanja za samoprocjenu s višestrukim izborom

1. U kibernetičkoj sigurnosti rizici se odnose na:

a) Potencijalne opasnosti prilikom povezivanja na internet.

b) Mjere fizičke sigurnosti.

c) Mjere opreza protiv skliskih podova.

Co-funded by the European Union

d) Sigurne online prakse.

Ispravna opcija: a

2. Koje su neke uobičajene vrste cyber prijetnji?

a) Fizički napadi na računala.

b) Trikovi ili zamke koje koriste loši ljudi na internetu.

c) Sigurnosne mjere za online kupovinu.

d) Strategije za zaštitu osobnih podataka.

Ispravna opcija: b

3. Što je društveni inženjering?

a) Tehnika koju koriste kibernetički kriminalci.

b) Proučavanje ljudskog ponašanja.

c) Alat za sigurno pregledavanje.

d) Vrsta računalnog virusa.

Ispravna opcija: a

4. Kako možete poboljšati online sigurnost pomoću alata za sigurno pregledavanje?

a) Korištenjem renomiranih web preglednika i aktiviranjem sigurnosnih značajki.

b) Povećanjem vremena ispred ekrana i digitalne ovisnosti.

c) Dijeljenjem osobnih podataka na društvenim mrežama.

d) Ignoriranjem phishing e-pošte i upozorenja o zlonamjernom softveru.

Ispravna opcija: a

5. Koje su neke strategije za ublažavanje rizika od prekomjernog vremena provedenog pred ekranom?

a) Postavljanje ograničenja vremena ispred ekrana i redovite pauze.

b) Povećanje korištenja tehnologije za bolje zdravlje.

c) Potpuno odspajanje s digitalnih uređaja.

d) Traženje podrške i odgovornosti.

Co-funded by the European Union

Ispravna opcija: a

Bibliografija i daljnje reference	
▪ https://staysafeonline.org/ ▪ https://www.consumer.ftc.gov/topics/online-security ▪ https://www.cisa.gov/cybersecurity ▪ https://www.getsafeonline.org/ ▪ https://us.norton.com/internetsecurity ▪ https://www.staysmartonline.gov.au/ ▪ https://www.commonsense.org/education/digital-citizenship/privacy-and-security	
Povezani materijal	BOOMER_Cyber_security_HT
Referentni link	
Video u Powtoon formatu	https://www.youtube.com/watch?v=lvLhhqDhZJY

Co-funded by the European Union