Brošura za obuku

Naslov	Internetska sigurnost: Što treba i što ne treba raditi
Ključne riječi	Internet, sigurnost, na mreži, izvan mreže, lozinke, privatnost
Osigurano od strane	Internet Web Solutions-a
Jezik	Hrvatski

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

Ciljevi / Ishodi učenja

Na kraju ovog modula ćete:

- Razumjeti važnost odgovornog ponašanja na internetu
- Identificirati uobičajene rizike na internetu
- Prepoznati prednosti interneta
- Naučiti najbolje prakse za sigurnost na internetu
- Razviti vještine digitalne pismenosti

Opis

Ovaj tečaj nudi opsežan pregled o tome kako ostati siguran tijekom korištenja interneta, pružajući praktične savjete o tome što treba i što ne treba raditi na mreži, uključujući savjete o sigurnim vezama, upravljanju zaporkama, postavkama privatnosti za društvene medije, praksi sigurne kupnje na mreži te prepoznavanju i izbjegavanje pronevjere i prijevara. Slijedeći ove smjernice, moći ćete se sigurno kretati online svijetom i zaštititi se od potencijalnih prijetnji.

Kazalo sadržaja (3 razine)

Sufinancira Europska unija

Ova publikacija [priopćenje] odražava samo stajališta autora te se Komisija ne može smatrati odgovornom za bilo kakvu upotrebu informacija sadržanih u njoj.

2.2. Zaporke
2.3. Privatnost i društveni mediji
2.4. Online kupovina
2.5. Pronevjere i prijevare

Poglavlje 3: Dodatan dio: Što treba i što ne treba raditi kada niste na mreži
3.1. Digitalni uređaji

Razvijeni sadržaj

Modul: Internetska sigurnost: Što treba i što ne treba raditi

Poglavlje 1: Uvod u internetsku sigurnost

Odjeljak 1.1: Što znači biti siguran na internetu?

Biti siguran na internetu znači poduzeti mjere opreza i odgovorno se ponašati tijekom korištenja interneta. Uključuje razumijevanje i upravljanje **potencijalnim rizicima i prijetnjama** povezanim s mrežnim aktivnostima radi zaštite osobnih podataka, financijskih resursa i općeg blagostanja.

Kibernetički prostor je poput autoceste: morate se njome kretati sigurno kako biste izbjegli nesreće. Baš kao i vezanje sigurnosnog pojasa, neke osnovne sigurnosne prakse na internetu mogu pomoći osigurati da vaše iskustvo na internetu bude sigurno i ugodno.

Biti siguran na internetu važno je iz nekoliko razloga. Pomaže u **zaštiti vaših osobnih podataka** od pada u pogrešne ruke. Osobni podaci poput vašeg imena, adrese, telefonskog broja i financijskih podataka mogu se koristiti za krađu identiteta, prijevaru ili druge zlonamjerne aktivnosti ako im pristupe kibernetički kriminalci. Vaša prisutnost na mreži pridonosi vašem ugledu, kako osobnom tako i poslovnom.

Ako ste sigurni na internetu, možete **spriječiti širenje neprimjerenog ili štetnog sadržaja** koji može negativno utjecati na vašu sliku i odnose. Očuvanje vaše internetske sigurnosti **osigurava zaštitu vaše privatnosti i štiti vas od financijskih prijevara i pronevjera.**

Biti siguran na mreži također pomaže u **izbjegavanju slučajeva internetskog nasilja i uznemiravanja**. Primjenom sigurnosnih mjera možete smanjiti rizik od susreta sa štetnim pojedincima ili situacijama koje mogu dovesti do emocionalnog stresa ili ozljede. Sigurnost na internetu također je ključna za **zaštitu djece** i osiguranje njihove dobrobiti u digitalnom svijetu.

Sufinancira Europska unija

Ova publikacija [priopćenje] odražava samo stajališta autora te se Komisija ne može smatrati odgovornom za bilo kakvu upotrebu informacija sadržanih u njoj.

Odjeljak 1.2: Koji su rizici nesigurna korištenja internetom?

Nesigurno korištenje interneta predstavlja opasnost za starije osobe. Oni su možda manje upoznati s internetskim platformama i prijetnjama, pa je važno razumjeti specifične rizike s kojima se suočavaju.

Neki uobičajeni rizici su:

- **Phishing i prijevare:** Starije su osobe osjetljivije na phishing e-poruke, lažne web-stranice i telefonske prijevare, gdje ih prevaranti navedu na otkrivanje osjetljivih podataka.
- **Krađa identiteta:** Nesigurna internetska navigacija povećava rizik od krađe osobnih podataka i identiteta, što dovodi do financijskih gubitaka i poremećaja u njihovim životima.
- **Financijska prijevara:** Starije osobe cilj su lažnim investicijskim shemama, prijevarama na lutriji ili lažnim kupnjama, iskorištavajući njihovo povjerenje i ranjivost.
- **Zlonamjerni softver i virusi:** Nesigurna korištenje interneta može dovesti do nenamjernog preuzimanja štetnog softvera koji ugrožava sigurnost uređaja i osobne podatke.
- **Internetsko uznemiravanje i internetsko zlostavljanje:** Starije osobe mogu patiti od emocionalnog stresa i psihičkih problema zbog internetskog uznemiravanja.
- **Povrede privatnosti:** Neadekvatne navike zaštite privatnosti mogu razotkriti osobne podatke, što može dovesti do krađe identiteta ili neželjenog traženja.
- **Prijevare tehničke podrške:** Starije osobe podložnije su prijevarama u kojima se prevaranti predstavljaju kao predstavnici tehničke podrške.
- **Nedostatak digitalne pismenosti:** Nesigurna korištenje interneta pogoršana je nedostatkom digitalne pismenosti među starijim osobama, što ih čini ranjivijima na prijetnje i prijevare.

Starije osobe trebale bi biti svjesne ovih rizika i poduzeti proaktivne mjere kako bi ih spriječile, na primjer traženjem pomoći i podrške od osoba od povjerenja ili prijavljivanjem zabrinutosti relevantnim tijelima ili platformama.

Odjeljak 1.3: Zašto ne biste trebali prestati s korištenjem interneta čak i uz ove rizike?

Sigurnost na internetu važna je, ali ne mora biti stresna. Svijest je snažan prvi korak u zaštiti sebe zajedno s pouzdanim antivirusnim softverom (mnogi su besplatni!).

Ne biste trebali u potpunosti prestati koristiti internet unatoč rizicima na internetu jer internet može imati goleme prednosti za vaše blagostanje i društvenu uključenost. Internet nudi ogromnu količinu **informacija i resursa** koji vam mogu biti od velike

Sufinancira Europska unija

Ova publikacija [priopćenje] odražava samo stajališta autora te se Komisija ne može smatrati odgovornom za bilo kakvu upotrebu informacija sadržanih u njoj.

koristi. Omogućuje pristup vijestima, obrazovnim materijalima, zdravstvenim resursima, komunikacijskim alatima i raznim internetskim uslugama.

U smislu **društvene povezanosti**, internet omogućuje da ostanete povezani s obitelji, prijateljima i zajednicama, posebno kada fizička mobilnost ili udaljenost predstavljaju prepreku. Platforme društvenih medija, video pozivi i internetski forumi omogućuju održavanje odnosa, razmjenu iskustava i borbu protiv izolacije ili usamljenosti. Online platforme nude pogodnost i **neovisnost** za sve ljude u različitim aspektima svakodnevnog života. Možete **kupovati putem interneta, pristupati uslugama internet bankarstva, zakazivati sastanke i naručivati lijekove**, pružajući veću pogodnost i **smanjujući potrebu za fizičkim putovanjem ili pomoći**.

Kretanje internetom je također izvor **kognitivne stimulacije i mentalnog angažmana** budući da nudi prilike za učenje, igranje igrica, sudjelovanje u virtualnim hobijima ili zajednicama i ostanak mentalne aktivnosti, što može doprinijeti općem blagostanju.

Krećući se internetom i usvajajući sigurne online prakse, možete **razviti vještine digitalne pismenosti**, povećati svoje samopouzdanje i zadržati osjećaj **osnaženosti**. Internet pruža obilje **resursa za učenje**, uključujući online tečajeve, poduke i obrazovne platforme. Možete istražiti nove interese, naučiti nove vještine i uključiti se u mogućnosti cjeloživotnog učenja, promičući osobni rast i intelektualnu stimulaciju.

Iako je važno biti svjestan rizika na internetu i poduzeti mjere opreza, **potpuno izbjegavanje interneta može dovesti do izolacije, ograničenog pristupa resursima i propuštenih prilika**.

Poglavlje 2: Što treba i što ne treba raditi na internetu

Odjeljak 2.1: Sigurne veze

Što treba raditi:

Koristite sigurne Wi-Fi mreže: Povežite se na sigurne i pouzdane Wi-Fi mreže kad god je to moguće. Ove mreže obično zahtijevaju lozinku i enkripciju, što omogućuje sigurnije okruženje pregledavanja. Izbjegavajte pristup osjetljivim računima ili obavljanje financijskih transakcija na javnoj Wi-Fi mreži.

Provjerite sigurnost web-mjesta: Prije unosa osjetljivih podataka ili obavljanja online transakcija, provjerite ima li web-mjesto sigurnu vezu. Potražite "https://" u adresi web stranice i simbol lokota u adresnoj traci preglednika.

Sufinancira Europska unija

Ova publikacija [priopćenje] odražava samo stajališta autora te se Komisija ne može smatrati odgovornom za bilo kakvu upotrebu informacija sadržanih u njoj.

Održavajte softver ažuriranim: Redovito ažurirajte operativni sustav vašeg uređaja, web preglednike i sigurnosni softver. Ažuriranja softvera često uključuju sigurnosne zakrpe koje pomažu u zaštiti od poznatih ranjivosti.

Koristite zaštitu vatrozidom: Omogućite i održavajte vatrozid na vašem računalu ili usmjerivaču koji će djelovati kao prepreka neovlaštenom pristupu i potencijalnim prijetnjama s interneta.

Što ne treba raditi:

Nemojte dijeliti osjetljive podatke: Izbjegavajte unos osjetljivih podataka, poput zaporki, podataka o kreditnoj kartici ili brojeva socijalnog osiguranja.

Izbjegavajte sumnjive web stranice: Izbjegavajte posjećivanje sumnjivih ili nepoznatih web stranica. Držite se uglednih i pouzdanih web stranica za online aktivnosti.

Ne ignorirajte upozorenja preglednika: Obratite pažnju na upozorenja preglednika i upozorenja o potencijalnim sigurnosnim rizicima ili nepouzdanim web stranicama.

Nemojte se automatski povezivati s mrežama: Onemogućite značajku automatskog povezivanja na svojim uređajima jer se može automatski povezati s nezaštićenim mrežama bez vašeg znanja.

Odjeljak 2.2: Zaporke

Što treba raditi:

Stvorite jake i jedinstvene zaporke: Koristite jake i jedinstvene zaporke za svaki online račun. Trebala bi sadržavati kombinaciju velikih i malih slova, brojeva i posebnih znakova. Izbjegavajte korištenje informacija koje se mogu pretpostaviti kao što su rođendani ili imena.

Neka zaporke budu dugačke: Odlučite se za duže zaporke jer su općenito sigurnije. Nastojte imati najmanje 12 znakova. Razmislite o korištenju zaporki poput: niz riječi ili rečenica koje je lakše zapamtiti, ali ih je drugima teško pogoditi. Na primjer, "MojaOmiljenaBojaJePlava!".

Omogućite dvofaktorsku autentifikaciju (2FA): Kad god je to moguće, omogućite dvofaktorsku autentifikaciju za svoje online račune. To dodaje dodatnu razinu sigurnosti zahtijevajući drugi korak provjere, kao što je jedinstveni kod poslan na vaš mobilni uređaj.

Redovito ažurirajte zaporke: Povremeno mijenjajte svoje zaporke, po mogućnosti svakih nekoliko mjeseci.

Sufinancira Europska unija

Ova publikacija [priopćenje] odražava samo stajališta autora te se Komisija ne može smatrati odgovornom za bilo kakvu upotrebu informacija sadržanih u njoj.

Što ne treba raditi:

Nemojte ponovno koristiti zaporke: Nikada nemojte ponovno koristiti istu zaporku na više računa. Ako je jedan račun ugrožen, potencijalno bi mogao omogućiti pristup i drugim računima. Koristite jedinstvene zaporke za svaku internetsku uslugu ili platformu.

Izbjegavajte uobičajene zaporke: Izbjegavajte uobičajene ili jednostavne zaporke, poput "123456", "lozinka" ili "qwerty". Ove su zaporke često na meti hakera i mogu se lako probiti.

Nemojte dijeliti niti zapisivati zaporke: Izbjegavajte dijeliti svoje zaporke s drugima, uključujući obitelj ili prijatelje. Osim toga, izbjegavajte zapisivati zaporke u bilješke ili ih pohranjivati u lako dostupnim digitalnim datotekama.

Nemojte spremati zaporke u preglednike: Suzdržite se od spremanja zaporki u web preglednicima ili korištenja značajke "Zapamti me". Iako može pružiti pogodnost, predstavlja sigurnosni rizik ako netko dobije neovlašteni pristup vašem uređaju.

Odjeljak 2.3: Privatnost i društveni mediji

Što treba raditi:

Pregledajte postavke privatnosti: Upoznajte se s postavkama privatnosti platformi društvenih medija koje koristite. Prilagodite postavke da biste kontrolirali tko može vidjeti vaš profil, objave i osobne podatke. Razmislite o ograničavanju pristupa na prijatelje i članove obitelji kojima vjerujete.

Budite selektivni sa zahtjevima za prijateljstvo: Budite oprezni kada prihvaćate zahtjeve za prijateljstvo ili zahtjeve za povezivanjem od nepoznatih osoba. Provjerite identitet osobe prije nego što prihvatite njen zahtjev.

Razmislite prije dijeljenja: Budite oprezni kada dijelite osobne podatke, fotografije ili ažuriranja na platformama društvenih medija. Izbjegavajte javno dijeljenje osjetljivih podataka poput vaše pune adrese, telefonskog broja ili financijskih podataka.

Redovito pregledavajte i ažurirajte popis prijatelja: Povremeno pregledajte svoj popis prijatelja ili veza na platformama društvenih medija. Uklonite ili poništite kao prijatelje osobe kojima više ne vjerujete ili ih ne prepoznajete.

Što ne treba raditi:

Nemojte kliktati na sumnjive poveznice: Budite oprezni s kliktanjem na poveznice koje dijelite na društvenim medijima, osobito one iz nepoznatih ili sumnjivih izvora.

Sufinancira Europska unija

Ova publikacija [priopćenje] odražava samo stajališta autora te se Komisija ne može smatrati odgovornom za bilo kakvu upotrebu informacija sadržanih u njoj.

Ove veze mogu voditi do web stranica za krađu identiteta ili preuzimanja zlonamjernog softvera. Prije klika provjerite izvor.

Budite oprezni s aplikacijama trećih strana: Budite selektivni pri davanju dopuštenja aplikacijama trećih strana koje zahtijevaju pristup vašim računima društvenih medija. Pregledajte zatražena dopuštenja i razmotrite vjerodostojnost aplikacije prije nego što odobrite pristup.

Izbjegavajte objavljivanje osobnih događaja: Izbjegavajte najave nadolazećih godišnjih odmora ili duljeg odsustva od kuće na platformama društvenih medija. Na taj način možete upozoriti potencijalne provalnike ili kriminalce da u vašem domu nema nikoga.

Odjeljak 2.4: Online kupovina

Što treba raditi:

Kupujte na pouzdanim web stranicama: Prilikom kupnje, držite se renomiranih i poznatih trgovaca na internetu. Potražite web stranice koje imaju pozitivne recenzije kupaca i sigurne opcije plaćanja kao što su kreditne kartice ili renomirane platforme za plaćanje.

Provjerite sigurnost web stranice: Prije unosa podataka o plaćanju ili osobnih podataka, provjerite ima li web stranica sigurnu vezu. Potražite "https://" u adresi web stranice i simbol lokota u adresnoj traci preglednika.

Pratite transakcije: Održavajte evidenciju svojih transakcija kupnje na mreži, uključujući potvrde narudžbi, račune i brojeve za praćenje. To vam omogućuje praćenje isporuka i rješavanje bilo kakvih problema koji se mogu pojaviti.

Što ne treba raditi:

Nemojte dijeliti nepotrebne podatke: Budite oprezni s dijeljenjem nepotrebnih osobnih podataka tijekom procesa naplate. Trgovci obično traže osnovne podatke kao što su adresa za dostavu i podaci o plaćanju.

Čuvajte se e-pošte ili veza za krađu identiteta: Budite oprezni s e-poštom ili porukama za koje se tvrdi da dolaze od prodavača na internetu, osobito ako traže osobne podatke ili vas pozivaju da kliknete na sumnjive veze.

Izbjegavajte nezaštićeni Wi-Fi za transakcije: Kada kupujete putem interneta, izbjegavajte korištenje nezaštićenih ili javnih Wi-Fi mreža. Ove mreže mogu biti ranjive te postoje hakeri koji mogu presresti vaše osobne i financijske podatke.

Sufinancira Europska unija

Ova publikacija [priopćenje] odražava samo stajališta autora te se Komisija ne može smatrati odgovornom za bilo kakvu upotrebu informacija sadržanih u njoj.

Ne nasjedajte na prijevare lažnim predstavljanjem: Budite oprezni s online prodavačima koji se lažno predstavljaju kao renomirane marke ili koriste obmanjujuće taktike kako bi dobili vaše osobne ili financijske podatke. Provjerite autentičnost prodavatelja i njegove web stranice prije kupnje.

Odjeljak 2.5: Pronevjere i prijevare

Što treba raditi:

Budite skeptični i oprezni: Zadržite zdrav skepticizam kada naiđete na neželjenu e-poštu, telefonske pozive ili poruke u kojima se traže osobni podaci ili nude čudne ponude. Prije davanja bilo kakvih informacija ili preuzimanja financijskih obveza provjerite legitimnost izvora.

Educirajte se: Informirajte se o uobičajenim online prijevarama i taktikama prijevare usmjerenim na starije osobe. Upoznajte se sa znakovima prijevare, kao što su zahtjevi za plaćanje nekonvencionalnim metodama ili pritisak da se brzo djeluje.

Provjerite identitet kontakta: Kada pojedinci tvrde da predstavljaju organizacije, zatražite službene kontakt podatke i potvrdite njihovu autentičnost tako da se izravno obratite organizaciji koristeći potvrđene kontakt podatke.

Posavjetujte se s osobama od povjerenja: Ako primite sumnjiv zahtjev ili naiđete na nepoznatu situaciju na internetu, potražite savjet od osoba od povjerenja, poput člana obitelji, prijatelja ili stručnjaka.

Ignorirajte neželjene telefonske pozive i "robocallove": Sve neželjene telefonske pozive tretirajte sa skepticizmom. Živa osoba ili snimljeni glas mogu vam dati lažne informacije koje zvuče važne i vremenski osjetljive. Mogu tvrditi da su rođaci u nevolji, da jamstvo vašeg automobila ističe i da je potrebno plaćanje, mogu se predstaviti kao "tehnička podrška" i reći vam da vaše računalo treba popraviti uz naknadu.

Što ne treba raditi:

Nemojte žuriti niti se osjećati pod pritiskom: Prevaranti često koriste taktike za stvaranje osjećaja hitnosti ili pritiska, prisiljavajući žrtve na donošenje brzih odluka bez odgovarajućeg razmatranja. Uzmite si vremena, provedite istraživanje i budite oprezni prije nego što poduzmete bilo kakve financijske obveze.

Ne šaljite novac nepoznatim osobama: Budite oprezni sa zahtjevima za novcem ili bankovnim transferima od osoba koje ne poznajete osobno. Provjerite identitet i legitimitet pojedinca prije upuštanja u bilo kakve financijske transakcije.

Sufinancira Europska unija

Ova publikacija [priopćenje] odražava samo stajališta autora te se Komisija ne može smatrati odgovornom za bilo kakvu upotrebu informacija sadržanih u njoj.

Nemojte kliktati na poveznice u e-porukama nepoznatih pošiljatelja: Budite oprezni s čudnim ili neočekivanim porukama, čak i ako dolaze od ljudi koje poznajete. Mogu sadržavati zlonamjerne veze ili veze za krađu identiteta. Ako poruka izgleda sumnjivo, ali se čini da je od nekoga koga poznajete i kojem vjerujete, provjerite s njim prije nego što kliknete.

Nemojte otvarati nikakve privitke: Ne otvarajte privitke koje ne očekujete ili koji su od nepoznatog kontakta, posebno ako imaju ekstenziju .exe ili .zip. Ako se čini da je datoteka(e) od prijatelja ili člana obitelji, zamolite ih da provjeri jesu li vam nešto poslali. Ovo sigurnosno pravilo također se odnosi na privitke poslane putem tekstualnih poruka i društvenih medija.

Nemojte kliktati skočne prozore na svom telefonu ili računalu: Uobičajena skočna smicalica je softver za zastrašivanje koji koristi skočna sigurnosna upozorenja kako bi vas zastrašio i natjerao vas da preuzmete ili platite lažni softver koji je prerušen kao prava zaštita kibernetičke sigurnosti. Na primjer, pojavit će se upozorenje koje vas obavještava da je vaš uređaj ugrožen i da ga treba popraviti. Kada nazovete podršku, prevaranti mogu zatražiti pristup vašem računalu na daljinu i zatražiti naknadu. Druga tehnika zlonamjernog softvera je korištenje varljivih gumba "Zatvori" ili "X", koji automatski instaliraju virus kada se klikne na njih.

Poglavlje 3: Dodatan dio: Što treba i što ne treba raditi kada niste na mreži

Odjeljak 3.1: Digitalni uređaji

Što treba raditi:

Zaključajte svoje uređaje: Pobrinite se da se uređaji s pristupom osjetljivim informacijama automatski zaključavaju i zahtijevaju lozinku za ponovnu aktivaciju. Provjerite jeste li konfigurirali kućni Wi-Fi usmjerivač i pristupne točke s jedinstvenim korisničkim imenima i lozinkama koje nisu zadane.

Čuvajte uređaje sigurnima: Provjerite jesu li vaši digitalni uređaji, poput pametnih telefona, tableta ili prijenosnih računala, fizički sigurni. Čuvajte ih na sigurnom i zaštićenom mjestu kada nisu u uporabi.

Redovito ažurirajte softver: Održavajte operativni sustav i aplikacije na svojim uređajima ažuriranima. Ažuriranja softvera često uključuju važne sigurnosne zakrpe koje pomažu u zaštiti od ranjivosti i osiguravaju optimalne performanse.

Omogući praćenje i zaključavanje na daljinu: Aktivirajte značajke praćenja i zaključavanja na daljinu na svojim uređajima, ako su dostupne. To vam omogućuje lociranje vašeg uređaja ili zaključavanje uređaja na daljinu u slučaju gubitka ili krađe.

Sufinancira Europska unija

Ova publikacija [priopćenje] odražava samo stajališta autora te se Komisija ne može smatrati odgovornom za bilo kakvu upotrebu informacija sadržanih u njoj.

Sigurno zbrinite stare uređaje: Kada odlažete stare digitalne uređaje, osigurajte da su svi osobni podaci u potpunosti izbrisani s uređaja. Izvršite vraćanje na tvorničke postavke ili koristite specijalizirani softver za sigurno brisanje podataka.

Što ne treba raditi:

Ne ostavljajte uređaje bez nadzora: Izbjegavajte ostavljati svoje digitalne uređaje bez nadzora na javnim mjestima, poput kafića ili javnog prijevoza. Uvijek ih držite na dohvat ruke ili na sigurnom mjestu.

Nemojte instalirati neautorizirane aplikacije: Izbjegavajte preuzimanje i instaliranje aplikacija iz nepouzdanih izvora. Držite se službenih trgovina aplikacijama, kao što su Google Play Store ili Apple App Store, kako biste smanjili rizik od preuzimanja zlonamjernih ili krivotvorenih aplikacija.

Pet stavki u pojmovniku

Zaporka: Zaporka je tajna kombinacija znakova koja se koristi za autentifikaciju i dobivanje pristupa uređaju ili računu. Preporuča se postaviti snažnu zaporku za zaštitu osjetljivih podataka.
Društveni mediji: Društveni mediji odnose se na internetske platforme i tehnologije koje korisnicima omogućuju stvaranje, dijeljenje i razmjenu informacija, ideja i sadržaja s drugima. Ove platforme obično uključuju sadržaj koji stvaraju korisnici i olakšavaju komunikaciju, umrežavanje i interakciju među pojedincima ili grupama.
Internetska sigurnost: Internetska sigurnost odnosi se na mjere i mjere opreza koje se poduzimaju za zaštitu pojedinaca i njihovih osobnih podataka tijekom korištenja interneta i uključenja u online aktivnosti. Obuhvaća prakse i smjernice kojima je cilj spriječiti različite rizike na internetu kao što su kibernetičko zlostavljanje, krađa identiteta, prijevara, hakiranje i izlaganje neprimjerenom sadržaju. Internetska sigurnost uključuje razumijevanje i provedbu strategija za zaštitu privatnosti, sigurnosti i dobrobiti tijekom korištenja digitalnih platformi.
Zlonamjerne aplikacije: Zlonamjerne aplikacije su aplikacije koje su osmišljene kako bi oštetile ili ugrozile sigurnost uređaja ili podataka korisnika. Instaliranje aplikacija iz nepouzdanih izvora povećava rizik od preuzimanja zlonamjernih aplikacija koje mogu ukrasti osobne podatke ili izvesti neovlaštene radnje.
Osjetljive informacije: Osjetljive informacije odnose se na sve podatke ili pojedinosti koji bi, ako se otkriju ili im pristupe neovlaštene osobe, mogli predstavljati rizik za privatnost, sigurnost ili dobrobit pojedinca. Uključuje osobne identifikacijske podatke (PII) kao što su puna imena, adrese, telefonski brojevi, brojevi socijalnog osiguranja, financijski podaci, vjerodajnice za prijavu i medicinska dokumentacija. Osjetljive informacije zahtijevaju posebnu zaštitu i rukovanje kako bi se spriječila zlouporaba, krađa identiteta, prijevara ili druge štetne posljedice.

Sufinancira Europska unija

Ova publikacija [priopćenje] odražava samo stajališta autora te se Komisija ne može smatrati odgovornom za bilo kakvu upotrebu informacija sadržanih u njoj.

Pet pitanja s višestrukim izborom za samoocjenjivanje

Pitanje 1. Što je potrebno za Wi-Fi vezu da bi bila sigurna?
a) Zahtijeva da bude privatna, s uporabom zaporke i enkripcije.
b) Zahtijeva neograničenu uporabu podataka.
c) Zahtijeva veliku brzinu interneta.
d) Zahtijeva da Wi-Fi veza bude javno dostupna.
Točan odabir: a

Pitanje 2. Zašto je važno redovito ažurirati softver svog uređaja?
a) Zato što povećava prostor za pohranu uređaja.
b) Zato što čini da sučelje uređaja izgleda lijepo.
c) Zato što vas štiti od poznatih ranjivosti i sigurnosnih prijetnji.
d) Zato što produljuje trajanje baterije uređaja.
Točan odabir: c

Pitanje 3. Kako možete prepoznati potencijalne pronevjere ili prijevare?
a) Zanemarujući sigurnosna upozorenja.
b) Dijeleći osobne i financijske podatke bilo gdje.
c) Brzo ulijećući u financijske obveze.
d) Učeći o uobičajenim prijevarama na internetu i ostankom na oprezu.
Točan odabir: d

Pitanje 4. Kako možete kreirati jake zaporke?
a) Koristeći jednu riječ napisanu malim slovima, bez brojeva ili posebnih znakova.
b) Koristeći velika i mala slova, brojeve i posebne znakove.
c) Koristeći istu zaporku za nekoliko računa.
d) Odabrati zaporku koju je lako pogoditi te ju podijeliti s prijateljima kako je ne biste zaboravili.
Točan odabir: b

Pitanje 5: Kada kupujete online, što trebate učiniti ako web-mjesto nema sigurnu vezu?
a) Svejedno nastavite s kupnjom.
b) Najbolje je izbjegavati unos osobnih podataka ili podataka o plaćanju na tom web-mjestu i kupnju izvršiti na pouzdanijem web-mjestu sa sigurnom vezom.
c) Trebao bih zamoliti nekoga drugoga da upotrijebi svoje podatke i obavi kupnju umjesto mene na tom web-mjestu.
d) Ako kupnju izvršim putem javne Wi-Fi mreže, neće biti problema s dijeljenjem mojih podataka s tim web-mjestom.
Točan odabir: b

Sufinancira Europska unija

Ova publikacija [priopćenje] odražava samo stajališta autora te se Komisija ne može smatrati odgovornom za bilo kakvu upotrebu informacija sadržanih u njoj.

Bibliografija i dodatne reference	
https://www.enisa.europa.eu/ http://www.eun.org/ https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 https://www.microfocus.com/en-us/what-is/cyber-security https://www.redseguridad.com/actualidad/cibercrimen/que-es-el-malware-tipos-y-maneras-de-evitar-ataques-de-este-tipo_20210410.html https://openwebinars.net/blog/origen-e-importancia-de-la-ciberseguridad/ https://www.europol.europa.eu/wannacry-ransomware	
Povezani materijali	BOOMER_OnlineSafety_IWS_EN
Referentna poveznica	-
Video u Powtoon formatu	https://youtu.be/PYixkF0A34c

Sufinancira Europska unija