



MOBILE MONEY

Modul 4

Prejemanje in pošiljanje denarja



Sofinancira
Evropska unija

Projekt financira Evropska unija. Izražena stališča in mnenja so izključno stališča in mnenja avtorjev in ni nujno, da odražajo stališča in mnenja Evropske unije ali Evropske izvajalske agencije za izobraževanje in kulturo (EACEA). Niti Evropska unija niti EACEA ne moreta odgovarjati zanje. Številka projekta: 2023-1-RO01-KA220-ADU-000157797





Asociația Four Change, Romunija



ZAVOD IZRIIS

Zavod IZRIIS, Slovenija



E-SENIORS: INITIATION DES
SENIORS AUXNTIC
ASSOCIATION, Francija



GUnet, Grčija



Asociația Niciodata Singur –
Prietenii Varstnicilor, Romunija



Fundació Gesmed Fundació de la
Comunitat Valenciana, Španija



MOBILE
MONEY

Moduli

1. Osnovne veščine digitalne pismenosti

2. Varnost in preventiva

3. Upravljanje bančnega računa prek spleta

4. Spletne rešitve za prejemanje in pošiljanje denarja

5. Uporaba kreditne kartice za nakupovanje blaga in storitev prek spleta

6. Postopki spletnega plačevanja davkov in javnih storitev

Enota 1

Uvod

Cilji

Ob zaključku te enote boste seznanjeni

- ✓ z učnimi cilji in vsebino usposabljanja v tem modulu,
- ✓ z uporabljeno metodologijo uposabljanja in s trajanjem tega modula.





Kompetence

Ko zaključite ta modul, boste:

- Razumeli in izvajali digitalne transakcije.
 - ✓ Vedeli, katere informacije so potrebne za pošiljanje denarja.
 - ✓ Vedeli, kaj pomeni IBAN in kako ga uporabljamo.
 - ✓ Razumeli, čemu služi uporabniško ime.
 - ✓ Vedeli, kdaj in zakaj uporabimo telefonsko številko.
 - ✓ Znali dodati jasen podatek o namenu plačila.
- Suvereno izvajali korake za zagotavljanje varnosti.
 - ✓ Razumeli, kako PIN koda ščiti vaš račun.
 - ✓ Učinkovito in varno uporabljali gesla.
 - ✓ Prepoznali SMS kodo kot dodatno zaščito.
 - ✓ Pazili, da občutljivih podatkov ne delite z drugimi.
 - ✓ Poznali znake varnih povezav (npr. ikono ključavnice).



Vsebina usposabljanja



MOBILE
MONEY

1. Uvod k digitalnim denarnim nakazilom: Pregled osnovnih digitalnih veščin, potrebnih za nakazovanje denarja prek mobilne naprave.
2. Razumevanje obrazcev in obveznih podatkovnih polj: IBAN, uporabniško ime, telefonska številka in podatek o namenu plačila.
3. Aplikacije za pošiljanje in prejemanje denarja: Pregled pogosto uporabljenih aplikacij za denarna nakazila in njihovih funkcij, opis nameščanja.
4. Prepoznavanje pogostih goljufij in izogibanje goljufijam: Prepoznavanje poskusov ribarjenja in varno ravnanje z osebnimi podatki z namenom preprečevanja goljufij.
5. Dostop do zgodovine transakcij in njeno razumevanje: Pregled preteklih plačil, podatkov o pošiljateljih in vodenje evidenc s pomočjo mobilnih aplikacij.
6. Nasveti in praktične vaje.



Metodologija in trajanje usposabljanja

Trajanje: 4 ure

- Izobraževanje v živo: 2 uri
- Usposabljanje prek spleta: 2 uri

Metodologija

- Aktivno in participativno usposabljanje
- Usposabljanje v živo:
 - ✓ Dialog
 - ✓ Igranje vlog
 - ✓ Timsko delo
- Usposabljanje prek spleta:
 - ✓ Izbrani videoposnetki ali videoposnetki lastne izdelave
 - ✓ Praktična uporaba nekaterih nasvetov, sprejetih v učilnici
 - ✓ Nekaj sodelovalnega dela
 - ✓ Simulacija

Enota 2

Uvod k digitalnim denarnim nakazilom

Cilji

Ob zaključku te enote boste:

- ✓ razumeli vlogo digitalnih denarnih nakazil,
- ✓ poznali osnovne digitalne veščine,
- ✓ razumeli pomembnost digitalnih orodij,
- ✓ Imeli večje zaupanje v uporabo tehnologije.



Kaj je digitalno denarno nakazilo?

Digitalno denarno nakazilo je **elektronska storitev za pošiljanje ali prejemanje denarja s pomočjo mobilnih aplikacij ali spletnih platform, pri kateri ne potrebujemo gotovine ali čekov.**

Kako deluje: Ko vpišete prejemnikov IBAN, uporabniško ime in druge podatke, se denar prek banke ali aplikacije varno prenese na njegov račun.



Vloga digitalnih denarnih nakazil

Digitalna denarna nakazila predstavljajo povsem nov način upravljanja s financami in so varna, učinkovita in hitra rešitev za pošiljanje in prejemanje denarja. Uporabnik jih opravi brez stika s fizično gotovino, kar zmanjšuje tveganje, da bi mu denar kdo ukradel ali bi ga izgubil; transakcijo lahko izvede tudi v udobju svojega doma. Poleg tega je ohranjen natančen zapis o vsaki transakciji, kar zagotavlja preprosto spremljanje in preverjanje ter večjo finančno odgovornost.

Glavne prednosti digitalnih denarnih nakazil:

- **Udobnost:** Transakcijo lahko opravimo kadarkoli in kjerkoli.
- **Hitrost:** Prenos denarja z računa na račun se opravi takoj, tako rekoč v trenutku.
- **Varnost:** Denar je zaščiten z vešstopenjsko avtentikacijo in kodiranjem.
- **Vodenje evidence:** Za boljše upravljanje financ natančno spremljamo zgodovino transakcij.
- **Ekonomičnost:** Nižji stroški v primerjavi s tradicionalnimi metodami, npr. bančnimi menicami in nakaznicami.



Primeri plačevanja z digitalnimi denarnimi nakazili

- Pošiljanje denarja družini ali prijateljem
- Plačevanje storitev
- Prejemanje pokojnine ali finančne podpore
- Nakupovanje prek spleta
- Deljenje zneskov na računih s prijatelji
- Doniranje



Osnovne veščine, potrebne za digitalna denarna nakazila (1/2)

- 1. Uporaba mobilne naprave ali računalnika:** Znati moramo uporabljati pametni telefon, tablico ali računalnik, da bomo lahko dostopali do aplikacij ali spletnih mest.
- 2. Izpolnjevanje obrazcev:** Znati moramo natančno vnesti IBAN, prejemnikovo ime, znesek plačila in druge zahtevane podatke.
- 3. Navigiranje po aplikacijah in spletnih mestih:** Naučiti se moramo uporabljati aplikacije in spletna mesta za denarna nakazila (kako jih odpremo, kako se vanje prijavimo itd.).



Osnovne veščine, potrebne za digitalna denarna nakazila (2/2)

- 1. Razumevanje korakov za zagotavljanje varnosti:** Za varne transakcije moramo znati uporabljati PIN kode, gesla in SMS kode.
- 4. Preverjanje zgodovine transakcij:** Znati moramo poiskati in pregledati pretekle transakcije, da potrdimo plačila ali prejeme.
- 5. Jasen prenos informacij:** Vnašati in zahtevati moramo točne podatke (IBAN, referenca transakcije itd.), da ne bo prihajalo do napak.



Kaj gre pri digitalnih denarnih nakazilih lahko narobe?

- Vnesemo napačen podatek.
- Nasedemo goljufiji.
- Šibke varnostne prakse.
- Težave z internetno povezavo.
- Uporaba zastarelih aplikacij ali programske opreme.
- Napačno razumevanje provizij ali menjalnih tečajev.



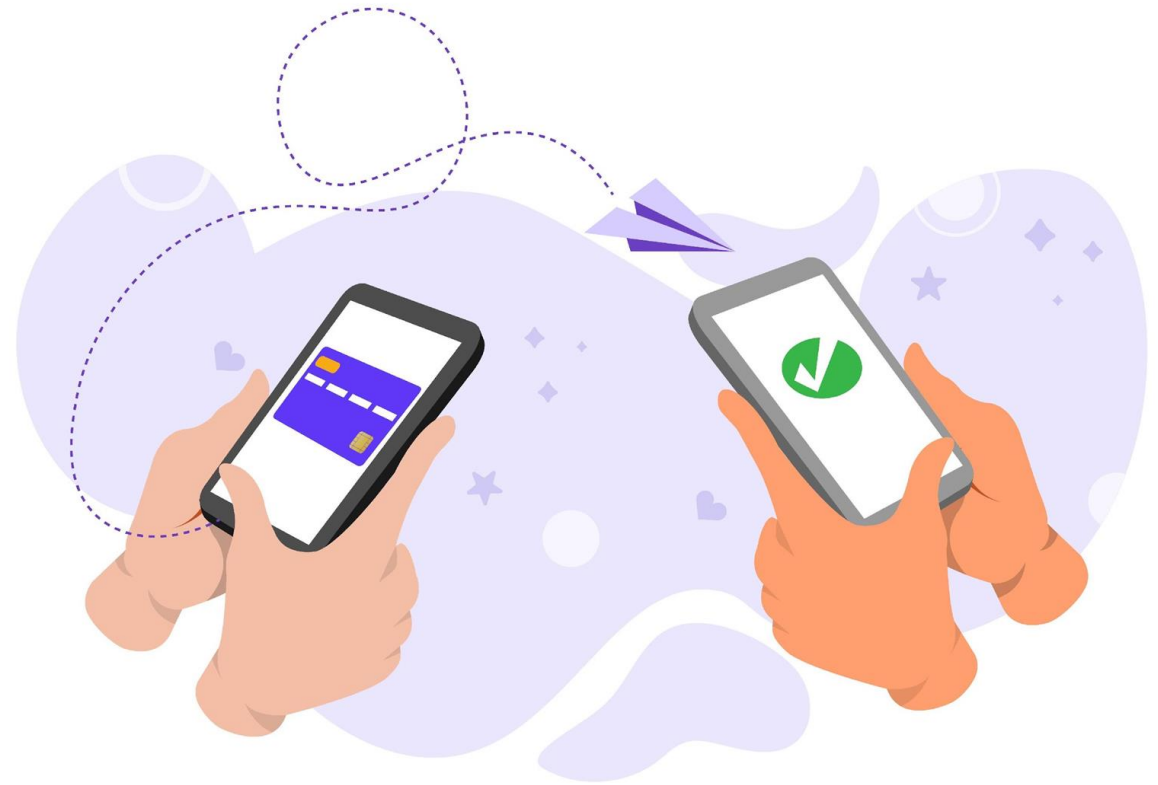
Enota 3

Razumevanje obrazcev in obveznih podatkovnih polj

Cilji

Ob zaključku te enote boste znali:

- ✓ prepoznati glavna polja za vnos podatkov,
- ✓ zagotavljati natančnost,
- ✓ razločevati obvezna in neobvezna polja,
- ✓ preverjati podatke, ki jih vnesejo drugi.



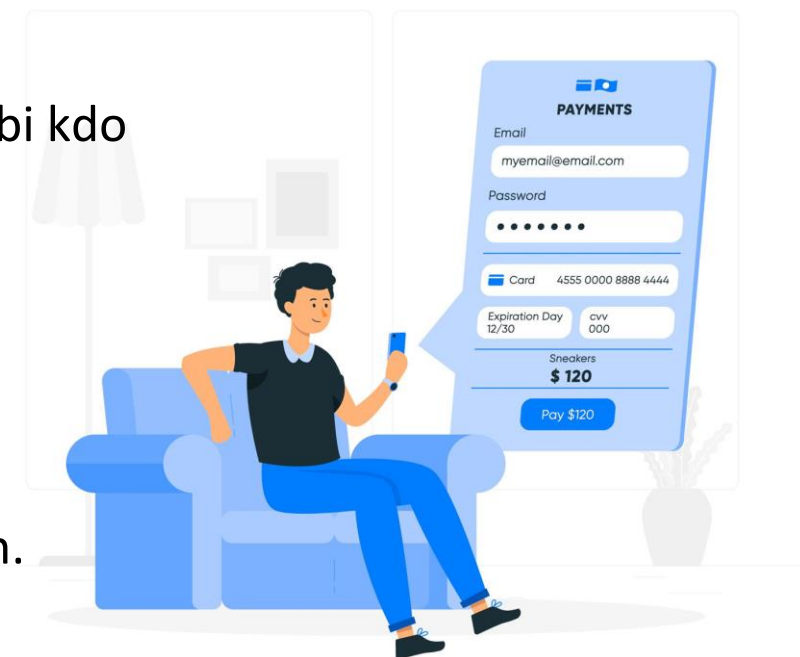
Glavna podatkovna polja

- **IBAN (Mednarodna številka bančnega računa)**
 - Edinstvena koda, ki označuje prejemnikov bančni račun.
 - Nujna, da denar zagotovo prispe na pravi naslov.
- **Uporabniško ime ali Ime**
 - Ime osebe, ki prejema denar, ali prejemnikovo uporabniško ime v aplikaciji.
 - Pomaga potrditi identiteto prejemnika.
- **Telefonska številka**
 - Uporablja se v določenih plačilnih aplikacijah ali kot dodatni korak preverjanja.
 - Zagotavlja varne in točne transakcije.
- **Podatek o namenu plačila**
 - Kratek zapis, ki opisuje namen nakazila (npr. "Darilo za vnuka")
 - Tako pošiljatelju kot prejemniku pomaga pri preglednosti transakcije.



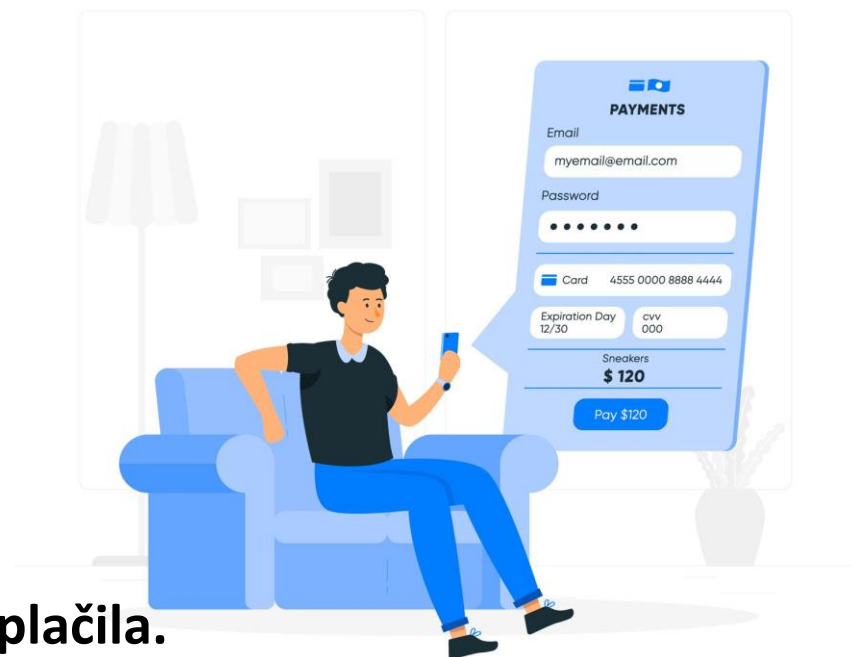
Nasveti za zagotavljanje točnosti pri digitalnih denarnih nakazilih (1/2)

- **Ne uporabljajte javnega brezžičnega omrežja.**
 - Uporabljajte varna omrežja ali mobilne podatke in preprečite, da bi kdo nepooblaščen dostopal do vaših podatkov.
- **Pazljivo preglejte vse podatke.**
 - Preverite IBAN, uporabniško ime, telefonsko številko in podatek o namenu plačila.
 - Že majhna tipkarska napaka lahko usmeri denar na napačen račun.
- **Preverite podatke s prejemnikovo potrditvijo.**
 - Prosite prejemnika, naj potrdi podatke, še posebno pri novih nakazilih.
 - Preverjene podatke varno shranite za prihodnjo uporabo.



Nasveti za zagotavljanje točnosti pri digitalnih denarnih nakazilih (2/2)

- **Vzemite si čas.**
 - Pri vnašanju podatkov ne hitite.
 - Umirjenost zmanjšuje možnost napak.
- **Bodite previdni pri samodejnem izpolnjevanju polj.**
 - Preden uporabite možnost samodejnega izpolnjevanja polj, se prepričajte, da so shranjeni podatki pravilni.
 - Posodobite zastarele podatke v aplikaciji ali računu.
- **Preglejte povzetek, ki se pokaže na zaslonu pred potrditvijo plačila.**
 - Preverite končni pregled transakcije, preden jo potrdite.
 - Bodite pozorni na prejemnikovo ime in znesek nakazila.



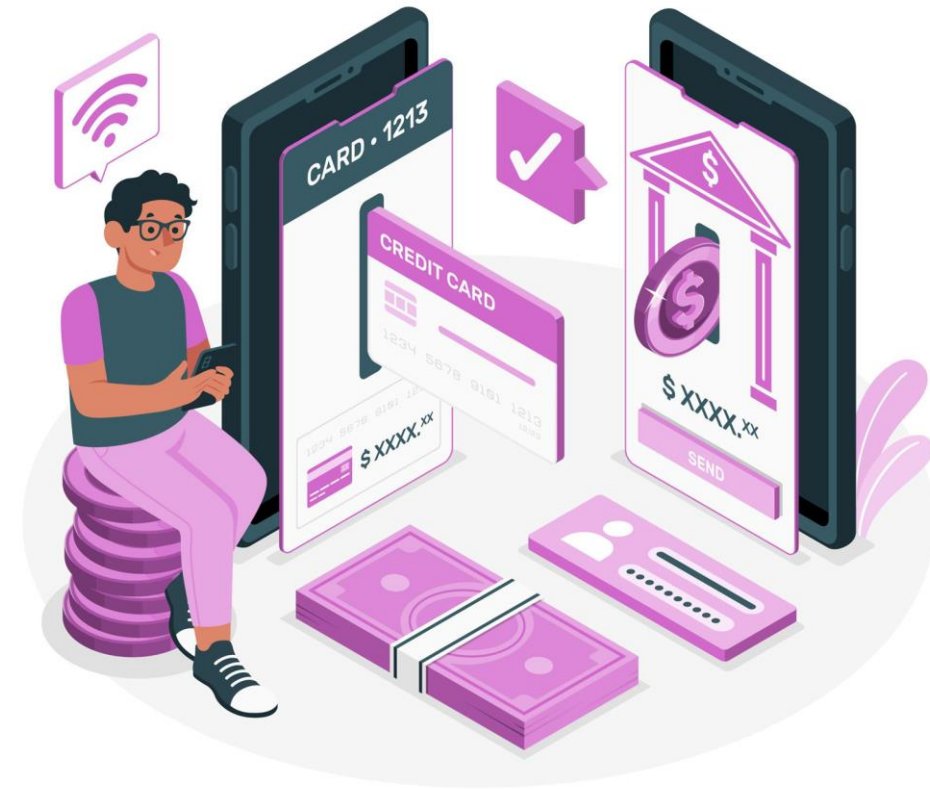
Enota 4

Aplikacije za pošiljanje in prejemanje denarja

Cilji

Ob zaključku te enote boste:

- ✓ poznali pogosto uporabljane aplikacije,
- ✓ razumeli funkcije aplikacij,
- ✓ znali aplikacije namestiti in jih nastaviti za uporabo,
- ✓ znali primerjati, kaj aplikacije omogočajo.



Pogosto uporabljane aplikacije za pošiljanje in prejemanje denarja v Romuniji (1/2)

- **George:** Aplikacijo George, prvo romunsko inteligentno bančno platformo, je razvila Banca Comercială Română (BCR). Odlikuje jo uporabniku prijazen vmesnik za upravljanje računov, plačil in prihrankov. Ima več kot 1,15 milijona aktivnih uporabnikov in dosega visoke ocene v trgovinah z aplikacijami.
- **ING Home'Bank:** Ta aplikacija, ki jo je razvila banka ING, omogoča uporabnikom izvajanje plačil, nakazil, upravljanje računov in druge bančne operacije. Za ponavljajoče se transakcije je na voljo funkcija 'Priljubljena plačila'.
- **BT Pay:** Ta aplikacija, ki jo ponuja Banca Transilvania, služi kot digitalna denarnica in omogoča uporabnikom, da izvajajo plačila, nakazujejo denar in upravljajo račune neposredno prek svojih pametnih telefonov.
- **Revolut:** Ta globalna finančna aplikacija, ki je v Romuniji priljubljena in ima več kakor 16 milijonov uporabnikov po vsem svetu, ponuja storitve, kot so mednarodna nakazila in menjava valut, ter orodja za upravljanje osebnih financ.



Pogosto uporabljane aplikacije za pošiljanje in prejemanje denarja v Romuniji (2/2)

- **Raiffeisen Smart Mobile:** Ta aplikacija, ki jo ponuja banka Raiffeisen, ponuja celostne storitve mobilnega bančništva, vključno s plačili, nakazili in upravljanjem računov, s poudarkom na varnosti in uporabniški izkušnji.
- **PayPal:** Po vsem svetu cenjena platforma za spletna plačila in denarna nakazila. Mnogi Romuni uporabljajo PayPal za spletno nakupovanje in prejemanje plačil iz tujine.
- **Western Union:** Ponuja tako spletne kot fizične lokacije za denarna nakazila. Western Union v Romuniji velja za zanesljivo možnost pošiljanja in prejemanja denarja, še posebno za mednarodna nakazila.



Nameščanje aplikacij za denarna nakazila in njihova priprava za uporabo

- **Izberite pravo aplikacijo:** Ugotovite, katera aplikacija ustreza vašim potrebam (npr. Revolut, PayPal ali aplikacija vaše banke).
- **Aplikacijo namestite:** Pojdite v trgovino App Store (iPhone) ali Google Play Store (Android). Vpišite ime aplikacije, in ko jo najdete, in kliknite "Namesti".
- **Ustvarite račun:** Odprite aplikacijo in sledite postopku prijave. Vpišite svoje ime, e-poštni naslov, telefonsko številko, varno geslo in druge podatke, ki jih priskrbi banka. Običajno morate za vzpostavitev spletnega bančnega računa najprej obiskati banko.
- **Povežite svoj bančni račun ali kartico:** Pri nekaterih aplikacijah je naslednji korak, da varno vpišete svoj IBAN ali številko kartice. Zaključite vse zahtevane korake preverjanja (npr. z SMS kodo ali e-pošno kodo).
- **Vzpostavite varnostne funkcije:** Nastavite PIN kodo, geslo ali biometrično avtentikacijo (prstni odtis / prepoznavanje obraza). Za dodatno zaščito vklopite dvofaktorsko avtentikacijo.
- **Vadite navigiranje po aplikaciji:** Raziščite ta vmesnik in poiščite funkcije, kot so pošiljanje denarja, ogled transakcij in posodabljanje podatkov. Seznanite se z možnostmi pomoči in podpore v primeru težav.



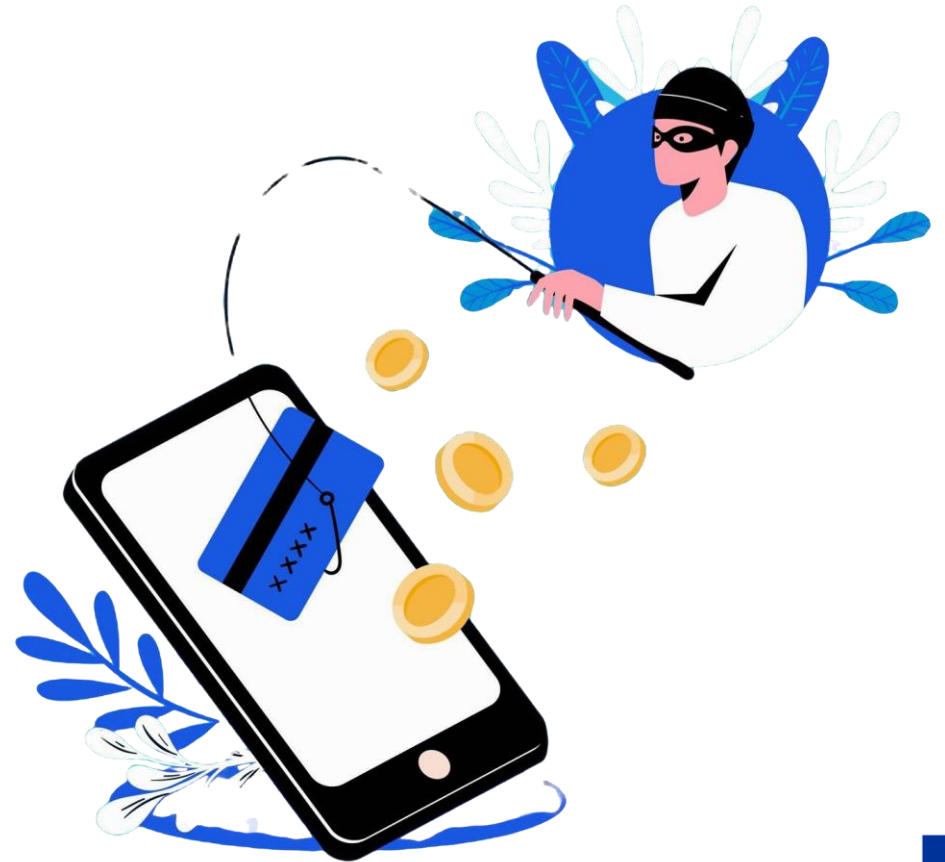
Enota 5

Prepoznavanje pogostih goljufij in izogibanje goljufijam

Cilji

Ob zaključku te enote boste:

- ✓ znali prepoznati poskuse ribarjenja,
- ✓ razumeli prakse varnega deljenja podatkov,
- ✓ znali preveriti legitimne zahteve in ponudbe,
- ✓ poznali varne komunikacijske kanale.



Kaj so poskusi ribarjenja?

- **Ribarjenje je goljufija, pri kateri vas napadalci z lažnimi sporočili, e-poštnimi dopisi ali spletnimi mesti poskušajo pretentati, da jim posredujete osebne ali finančne podatke.**
- **Kako deluje:**
 - Goljufi se predstavljajo kot zaupanja vredne ustanove (banke, vladne agencije ali ponudniki storitev).
 - Ljudem pošiljajo sporočila, v katerih jih pozivajo, naj kliknejo povezavo, vpišejo prijavne podatke ali potrdijo transakcijo.

▪ Pogosti znaki ribarjenja

- Postavljanje ultimativ, npr. "Vaš račun bo blokirano!"
- Neznani e-poštni naslovi in telefonske številke.
- Pravopisne in slovnične napake.
- Zahteve po občutljivih podatkih, npr. PIN kodah in geslih.
- Sumljive povezave, ki se ne ujemajo z uradnim spletnim mestom.

▪ Primeri ribarjenja

- Lažno e-poštno sporočilo, ki naj bi ga poslala vaša banka zaradi preverjanja računa.
- SMS s povezavo na "reševanje" težave z vašim računom.
- Telefonski klic z obvestilom, da ste dobitnik nagrade, in zahtevo po podatkih za izplačilo.



Prakse varnega deljenja podatkov

Za pošiljanje denarja

- Pred potrditvijo pazljivo preverite prejemnikove podatke (IBAN, uporabniško ime itd.).
- Delite samo preverjene in točne podatke, da se izognete napakam.
- Občutljivih podatkov, kot so gesla in varnostne kode, ne delite z drugimi ljudmi.
- Ko je nakazilo zaključeno, poskrbite, da je prejemnik o njem obveščen.

Za prejemanje denarja

- Navajajte jasne in pravilne podatke o računu (IBAN, telefonska številka itd.).
- Za deljenje podatkov o računu uporabljajte varne kanale (zanesljive aplikacije ali uradno komunikacijo).
- Potrdite prejem denarja in obvestite pošiljatelja, če se pojavijo kakšna neujojanja.
- Preverjajte obvestila in zapise o transakcijah ter se prepričajte, da je bil prenos pravilno opravljen.

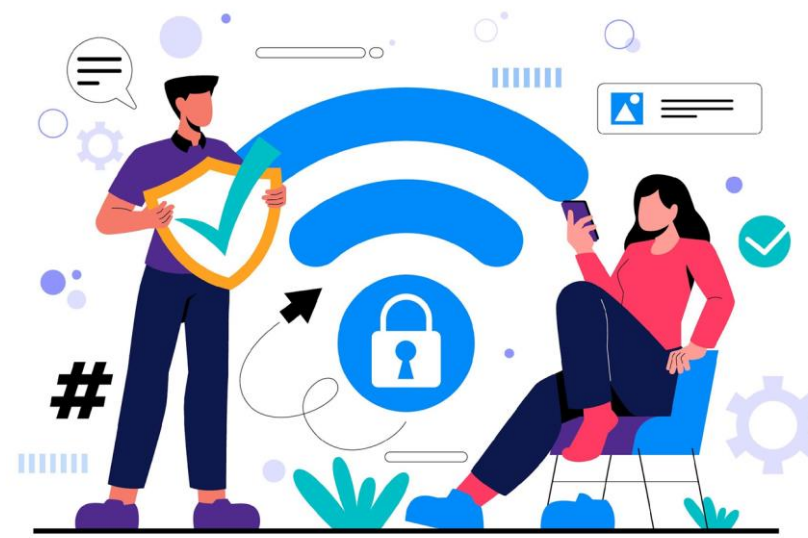


Kaj je večfaktorska avtentikacija?

Večfaktorska avtentikacija je varnostna metoda, ki zahteva, da pred prijavo v sistem ali transakcijo opravimo dva ali več korakov preverjanja identitete.

Kako deluje:

- Prvi korak:
 - Vnesemo svoje geslo ali PIN kodo.
- Drugi korak:
 - Opravimo dodatno preverjanje, npr:
 - Potrditev enkratne kode, ki jo prejmemo kot SMS.
 - Uporaba prstnega odtisa ali prepoznavanje obraza.
 - Generiranje kode iz aplikacije za avtentikacijo.





Enota 6

Dostop do zgodovine transakcij in razumevanje funkcije

Cilji

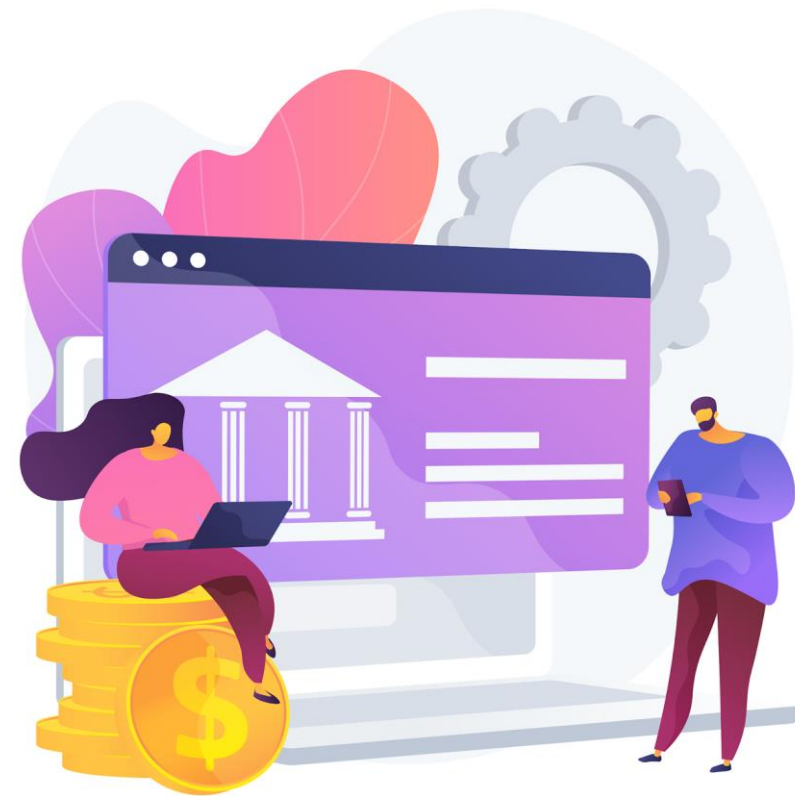
Ob zaključku te enote boste:

- ✓ znali navigirati po zgodovini transakcij,
- ✓ razumeli glavne podatke v zapisu o transakciji,
- ✓ znali preverjati plačila in prejeme,
- ✓ obvladali prenos datotek z zapisi in urejanje zapisov.



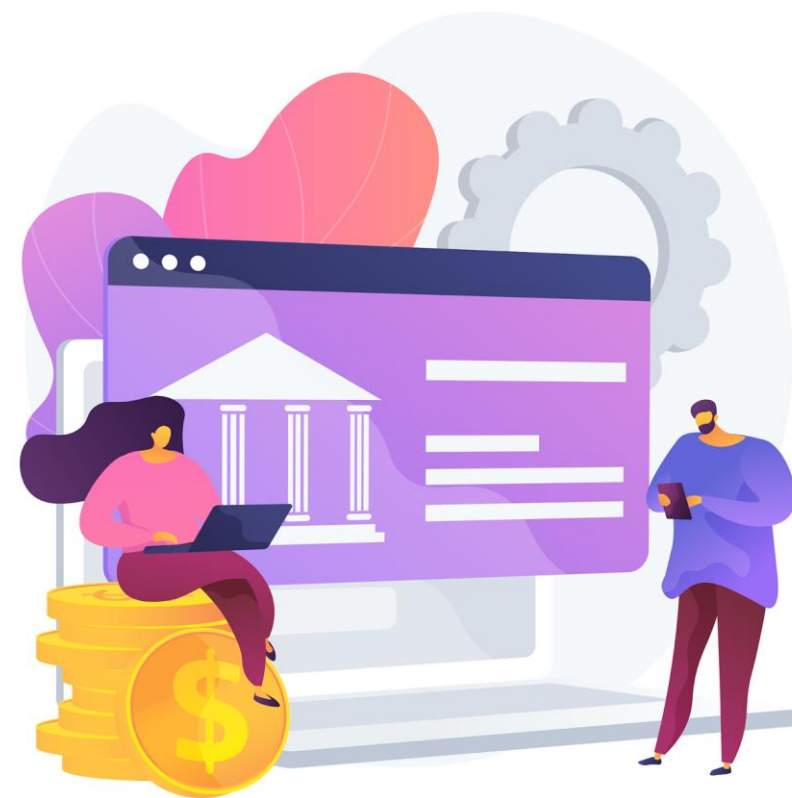
Navigiranje po zgodovini transakcij (1)

- **Odprite aplikacijo ali spletno mesto.**
 - S svojimi podatki za dostop se prijavite v bančno aplikacijo ali platformo za denarna nakazila.
 - Poiščite ustrezni razdelek: odprite zavihek ali meni z napisom “Zgodovina transakcij”, “Aktivnosti” ali “Plačila”. Pogosto se nahaja na domačem zaslonu ali v glavnem meniju.
- **Filtrirajte rezultate iskanja.**
 - Za iskanje določenih transakcij uporabite razpoložljive filtre, kot so datum, znesek ali vrsta transakcije. Rezultate iskanja lahko omejite tako, da izberete npr. “Poslano” ali “Prejeto”.



Navigiranje po zgodovini transakcij (2)

- **Oglejte si podatke.**
 - Kliknite ali tapnite na transakcijo, da se vam prikažejo ime pošiljatelja, znesek, referenčna številka in vsi ostali podatki.
 - Preverite ustreznost podatkov.
- **Shranite jih za prihodnjo uporabo.**
 - Po potrebi si prenesite datoteko s podatki o transakciji ali si jih natisnite za osebno evidenco ali kot dokazilo o plačilu.



Zakaj je to pomembno?

- **Preverjanje transakcij**
 - Potrdite lahko, da so bila plačila uspešno poslana ali prejeta.
- **Dokazilo o plačilu**
 - Po potrebi lahko uporabite zgodovino transakcij kot dokaz za poslana ali prejeta plačila.
- **Nadzor nad financami**
 - S spremljanjem svojih izdatkov in prihodkov bolje upravljate svoj proračun.
- **Odpravljanje napak**
 - Hitro lahko prepoznate neujemanja ali nepooblaščne transakcije in jih nemudoma odpravite.





Aktivnost: Poznajte svoj IBAN (1)

Odločite se, po kateri poti najlažje pridete do svojega IBAN-a.

Opisali boste, kako poiščete svoj IBAN s pomočjo bančne aplikacije, spletnega mesta ali na natisnjem izpisku z računa. Način, ki ste ga izbrali, delite s skupino, da boste vsem članom pomagali razumeti različne možnosti, ki so na voljo.

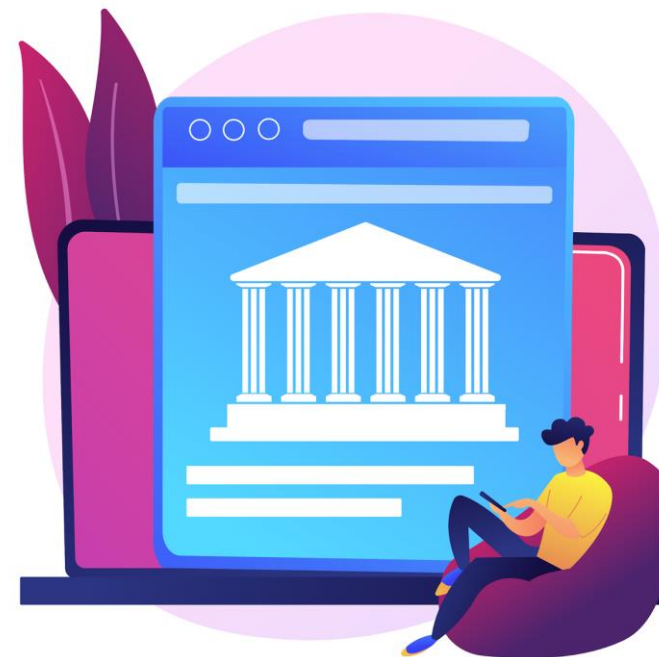




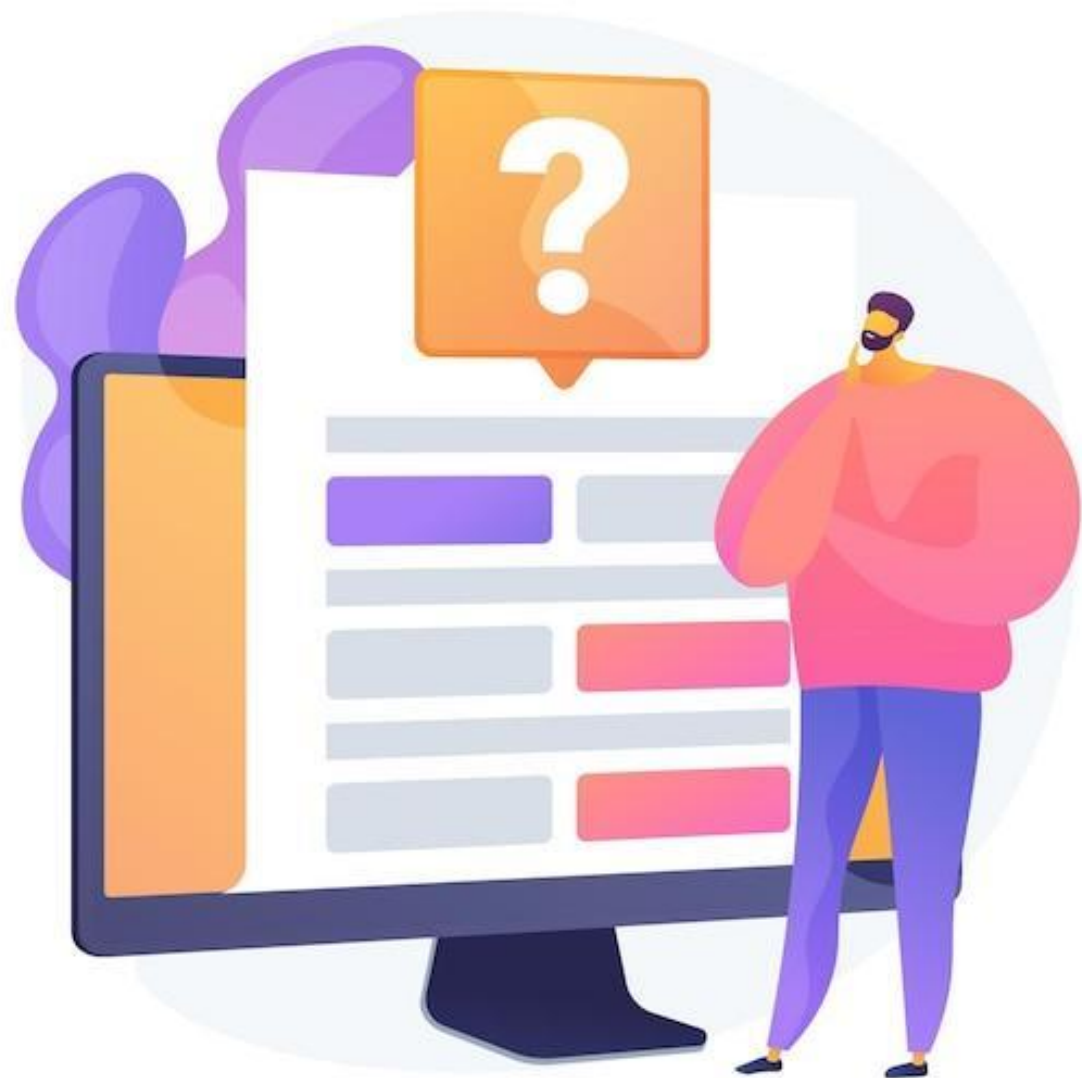
Aktivnost: Poznajte svoj IBAN (2)

Vprašanja za skupino

- Katera orodja ali sredstva ste uporabljali, da ste našli svoj IBAN?
- Če ste med iskanjem svojega IBAN-a naleteli na kakšne težave, kako ste jih rešili?
- Kako bi ravnali, da bi varno delili svoj IBAN z nekom, ki vam želi poslati denar?



Preverite svoje znanje!



1. Kaj morate storiti, če prejmete e-poštno sporočilo z zahtevo po podatkih o vašem računu?

Samo en odgovor je pravilen!

A. Nemudoma poslati odgovor s svojimi podatki

B. Klikniti povezavo v e-poštnem sporočilu za potrditev svojega računa

C. Ignorirati e-poštno sporočilo in ga izbrisati

D. Varno deliti svoj IBAN po e-pošti



2. Kaj od naštetega je primer metode večfaktorske avtentikacije?

Samo en odgovor je pravilen!

A. Uporabljam samo geslo

B. Po vnosu gesla prejmem SMS kodo

C. Do svojega računa dostopam v javnem brezžičnem omrežju

D. Prijavim se brez PIN kode



3. Kaj morate storiti, preden potrdite denarno nakazilo?

Samo en odgovor je pravilen!

A. Tako ga potrdim

B. Pazljivo preverim prejemnikove podatke

C. Zahtevam, da aplikacija samodejno shrani moje geslo

D. Potrdim ga brez preverjanja zneska



4. Zakaj za digitalna denarna nakazila ni varno uporabljati javno brezžično omrežje?

Samo en odgovor je pravilen!

A. Ker je prepočasno za velike transakcije

B. Ker omogoča nepooblaščen dostopanje do občutljivih podatkov

C. Ker zahteva geslo za povezavo

D. Ker ne podpira spletnih plačil



5. Kaj morate storiti, če opazite neujezanje v zgodovini transakcij?

Samo en odgovor je pravilen!

A. To ignoriram in čakam, da se bo uredilo samo

B. Izbrišem aplikacijo in jo ponovno namestim

C. Nemudoma se obrnem na banko ali uporabniško podporo v aplikaciji

D. Sam poskušam razveljaviti transakcijo



6. Kaj od naštetega je glavni namen zgodovine transakcij?

Samo en odgovor je pravilen!

A. Pošiljanje denarja več
prejemnikom

B. Ogled podatkov, kot so datum,
znesek in referenčna številka

C. Polaganje gotovine na račun

D. Dodajanje novih plačilnih metod



7. Kaj od naštetega je znak, da gre za poskus ribarjenja?

Samo en odgovor je pravilen!

A. E-sporočilo s postavljanjem ultimata in z zahtevo po osebnih podatkih

B. Varno spletno mesto z ikono ključavnice v naslovni vrstici

C. Obvestilo bančne aplikacije o nedavni transakciji

D. Sporočilo znanega stika brez sumljivih povezav





IMOBILE
MONEY

Čestitke!
Zaključili ste ta modul!



Sofinancira
Evropska unija

Projekt financira Evropska unija. Izražena stališča in mnenja so izključno stališča in mnenja avtorjev in ni nujno odražajo stališča in mnenja Evropske unije ali Evropske izvajalske agencije za izobraževanje in kulturo (EACEA). Evropska unija niti EACEA ne moreta odgovarjati zanje. Številka projekta: 2023-1-RO01-KA220-ADU-0001577