MOBILE MONEY

Modul 2
Varnost in preventiva

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

Partnerji

Asociatia Four Change, Romunija

Zavod IZRIIS, Slovenija

E-SENIORS: INITIATION DES SENIORS AUXNTIC ASSOCIATION, Francija

GUnet, Grčija

Asociatia Niciodata Singur – Prietenii Varstnicilor, Romunija

Fundació Gesmed Fundació de la Comunitat Valenciana, Španija

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

MOBILE MONEY

Kompetence

Ko zaključite ta modul, boste

- imeli veščine, potrebne za varno in samozavestno uporabo storitev mobilnega denarja:
  - ✓Uporabljanje naprav IKT in njihovo posodabljanje
  - ✓Upravljanje e-poštnega računa: pošiljanje in prejemanje e-poštnih sporočil, odgovarjanje nanje, njihovo urejanje, pripenjanje datotek in upravljanje seznama stikov
  - ✓Navigacija po spletu
  - ✓Osnovno upravljanje datotek (ustvarjanje, shranjevanje, urejanje datotek in map)
  - ✓Nastavitev parametrov zasebnosti
- Imeli znanje za ravnanje s pametnim telefonom:
  - ✓Razumevanje osnovne terminologije
  - ✓Navigacija po mobilnih vmesnikih in menijih
  - ✓Uporaba zaslona na dotik in gumbov
  - ✓Zmožnost prenašanja in posodabljanja mobilnih aplikacij
  - ✓Raziskovanje različnih posebnosti določene mobilne aplikacije

Sofinancira Evropska unija

MOBILE MONEY

Vsebina usposabljanja

1. Uvod v izobraževanje: trajanje, cilji, vsebina in metodologija
2. Razumevanje osnovnih varnostnih načel (močno geslo, zaščita osebnih podatkov, ne razkrivamo občutljivih podatkov, kot so številka kreditne kartice, bančnega računa itd.)
3. Zaščita naprave IKT ali mobilne naprave (biometrija, PIN), posodabljanje operacijskega sistema in antivirusnega programa.
4. Zaščita računov mobilnega denarja (najboljše prakse, dvojna avtentikacija).
6. Potrditev transakcije in prejem potrdil (preverjanje podrobnosti o transakciji pred potrditvijo, hranjenje spletnih potrdil)
7. Razumevanje, kaj so prevare, in prepoznavanje najpogostejših (finančnih) prevar
8. Razlika med ribarjenjem (oškodovanje) in neželeno pošto
9. Prijavljanje primerov ogrožene varnosti: ribarjenja in/ali neželene pošte
10. Nasveti in praktične vaje

Sofinancira Evropska unija

MOBILE MONEY

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

Sofinancira Evropska unija

Enota 1

Predstavitev pojmov spletna varnost, osebni podatki in zasebnost

Cilji

Ob zaključku te enote boste vedeli:

- ✓ kaj so osebni podatki,
- ✓ kaj pomenita pojma zasebnost in varnost,
- ✓ kaj sta neželena e-pošta in ribarjenje ter kako se odzvati nanju,
- ✓ po katerih merilih se odločamo, katere povezave je varno odpirati,
- ✓ kaj je Splošna uredba o varstvu podatkov (GDPR).

Slika: Vectorjuice, Freepik

Sofinancira Evropska unija

Spletna varnost

Na spletu smo izpostavljeni **varnostnim grožnjam**. Kadar uporabniki prek spleta pošiljamo podatke (pakete informacij, npr. video ali glasovni klic, klepet, e-poštno sporočilo ali številko kreditne kartice, spletno mesto), **nimamo nadzora nad tem, kdo lahko dostopa do njih**. Podatki potujejo skozi številne strežnike, usmerjevalnike in druge naprave, kjer lahko do njih dostopa in jih bere vsak heker, ponudnik storitve ali predstavnik državne službe.

vedeli

Zato je nadvse pomembno, da uporabniki spleta načrtno:

- zaščitimo svoje **občutljive osebne podatke;**
- uporabljamo spletna orodja in storitve, kot je šifriranje podatkov, ki med komuniciranjem prek spleta **zagotavljajo zasebnost in varnost** informacij.

Kaj so osebni podatki?

Osebni podatki so vse informacije, ki se nanašajo na **živečega posameznika, katerega identiteta je znana ali jo je mogoče ugotoviti**.

Razne informacije, ki skupaj lahko služijo za **identifikacijo določenega posameznika,** so prav tako osebni podatki.

Slika: Storyset, Freepik

Primeri osebnih podatkov

Primeri osebnih podatkov so:

- ime in priimek;
- domači naslov;
- e-poštni naslov, kot na primer

  ime.priimek@podjetje.com;
- podatki o lokaciji, kot so podatki lokacijske funkcije na mobilnem telefonu;
- številka osebne izkaznice;
- naslov internetnega protokola (IP);
- identifikator piškotka;
- oglaševalski identifikator telefona;
- podatki, ki jih ima bolnišnica ali zdravnik in so lahko oznaka za unikatno identifikacijo osebe.

Kateri osebni podatki veljajo za občutljive?

Občutljivi osebni podatki

Naslednji osebni podatki veljajo za '**občutljive**' in zanje veljajo posebni pogoji obdelave:

- osebni podatki, ki razkrivajo rasno ali etnično poreklo, politična mnenja, verska ali filozofska prepričanja;
- fotografije, videoposnetki;
- članstvo v sindikatu;
- genetski podatki, biometrični podatki, ki se obdelujejo izključno z namenom človekove identifikacije;
- podatki v zvezi z zdravjem;
- podatki v zvezi s spolnim življenjem ali spolno usmerjenostjo osebe.

Občutljivi finančni podatki

- Račun in geslo za e-bančni sistem
- Varnostna koda kartice (CVC), datum poteka veljavnosti kreditne ali debetne kartice
- Osebna identifikacijska številka (PIN koda) mobilnega telefona

Slika: Redgreystock, Freepik

Kaj je zasebnost?

Pri **zasebnosti** gre za to:

- kako **nadzorujemo svoje osebne podatke,** in
- kako jih na varen način **uporabljajo** tretje osebe, ki so jih prejele.

Razmislite o **politiki zasebnosti**, o kateri preberete in se z njo strinjate, ko obiščete spletno mesto ali prenesete novo aplikacijo za pametni telefon.

Slika: Storyset, Freepik

Kaj je varnost?

Pri varnosti gre za to, **kako zavarovati, zaščititi osebne podatke** pred **nepooblaščenim dostopom,** najsibo v naši napravi, na oddaljenem spletnem strežniku ali med komunikacijo prek spleta.

Na tehnični ravni uporabljamo **varnostne kontrole**, ki omejujejo, kdo lahko dostopa do podatkov. Te kontrole delujejo:

- v naših napravah (osebni računalnik, tablica, mobilni telefon) – posodabljanje operacijskega sistema in programske opreme, uporaba močnih gesel;
- na oddaljenem spletnem strežniku – uporaba močnih gesel;
- med pošiljanjem informacij prek spleta – uporaba varnega protokola **https**.

Slika: Vectorjuice, Freepik

Varnost in zasebnost

- Pri varnosti gre za **zaščito podatkov**, pri zasebnosti pa za **zaščito identitete uporabnikov.**

  Na primer, osebje bolnišnic in klinik uporablja varne sisteme za komunikacijo s pacienti o njihovem zdravju in ne pošilja informacij prek osebnih e-poštnih računov. Tovrstna komunikacija je primer zagotavljanja varnosti.

- Zasebnost pa zagotavljajo pravilnik in določila, ki omejujejo dostop do pacientove zdravstvene dokumentacije na **določene člane bolnišničnega osebja**, na primer zdravnike, medicinske sestre in zdravstvene asistente.

- **Možno je zagotavljati varnost brez zagotavljanja zasebnosti**.

  Na primer, osebni podatki se dejansko lahko varno prenašajo in hranijo na spletnem mestu, spletno mesto pa jih še vedno lahko prodaja.

- **Zasebnosti ni možno zagotavljati brez zagotavljanja varnosti.**

  Na primer, heker bi dejansko lahko nepooblaščeno dostopil do vaše naprave, spletnega strežnika ali prenesenih podatkov in ukradel vaše osebne podatke.

Neželena pošta in ribarjenje

Morda ste že kdaj prejeli nadležna, običajno komercialna e-poštna sporočila **neznanega pošiljatelja**.

Taka sporočila **so lahko** tudi **nevarna, ker** lahko vsebujejo povezave do spletnih mest, namenjenih kraji podatkov, spletnih mest z zlonamerno programsko opremo ali takih, ki vsebujejo zlonamerno programsko opremo kot priponko.

Zato **ne odpirajte priloženih datotek in ne klikajte na povezave**. In nikoli ne razkrivajte svojih osebnih podatkov, podatkov o e-bančnem računu (uporabniško ime, geslo) ali kreditni/debetni kartici, na primer datuma poteka veljavnosti in trimestne številke CVC.

To se imenuje **ribarjenje:** hudodelci pošiljajo na videz uradna e-poštna sporočila in vas hočejo pretentati, da bi razkrili podatke, ki bi jih lahko uporabili za krajo identitete.

Slika: Vectorjuice, Freepik

Kako prepoznam neželeno pošto?

E-poštno sporočilo je sumljivo, če vsebuje eno ali več naslednjih značilnosti:

- Slovnične in pravopisne napake
- Napisano v tujem jeziku
- Manjka ime pošiljatelja
- Nujna potreba po ukrepanju – zlasti v kombinaciji z grožnjo

- Poziv k vnašanju osebnih podatkov (npr. kode PIN ali TAN)
- Zahteva po odpiranju datoteke
- Nikoli prejeli nobenega e-poštnega sporočila od te banke ali stranke

Slika: Freepik

Kaj storiti in česa ne?

- ✓ Ne odpirajte priponk, če niso bile pregledane z antivirusnim programom.
- ✓ Ne pozabite se odjaviti, zlasti če uporabljate javni računalnik, ki ga delite z drugimi.
- ✓ Izbrišite vsa e-poštna sporočila neznanih ljudi.
- ✓ Nikoli ne odgovarjajte na neželeno pošto!
- ✓ Ne klikajte na povezave v neželeni pošti.

Aktivnost: Ali je povezavo varno odpreti?

Odločite se, ali je povezavo varno odpreti:

Recimo, da prejmete e-poštno sporočilo banke, ki vas poziva, da kliknete na povezavo, kot je spodnja, in posredujete osebne podatke, kot so uporabniško ime, gesla in podrobnosti o kreditni kartici.

http://url5423.eka.de/ls/click?upn=V1OaWNMSPs2Lb0JqHpnyTLRlk2703ToIFpo2vd2MKt5gB6dYAUvw1B-2FnC6T5iVsCdbcug7l6pkTad-2FBfACSlC-2BKw-3D-3DhmuAs-OaWNMSPs2Lb0JqHpn-asDvdva

1. *Ne hitite, dobro premislite in se odločite, ali je povezavo varno odpreti.*
2. *Razmislite o razlogih.*

Slika: Pch.vector, Freepik

Slika: Freepik

Aktivnost: Ali je povezavo varno odpreti? (2)

Odgovor. *Ta povezava* **ni varna** iz več razlogov:

- Uporablja http namesto https.
- Domensko ime ni povezano z uradnim imenom banke.
- Povezava je sumljivo dolga.
- Domensko ime povezave se razlikuje od domenskega imena pošiljateljevega e-poštnega naslova.
- Prava banka ne bo nikoli zahtevala uporabniških imen, gesel ali podatkov o kreditnih karticah.

Slika: Pch.vector, Freepik

Kaj je uredba GDPR in kdo jo mora upoštevati

Kaj je uredba GDPR?

- **Splošna uredba o varstvu podatkov (GDPR)** je zakon Evropske unije, ki je bil uveden 25. maja 2018. Od organizacij zahteva spoštovanje pravice do zasebnosti in varovanje osebnih podatkov vsake osebe na območju EU.

Kdo mora upoštevati uredbo GDPR?

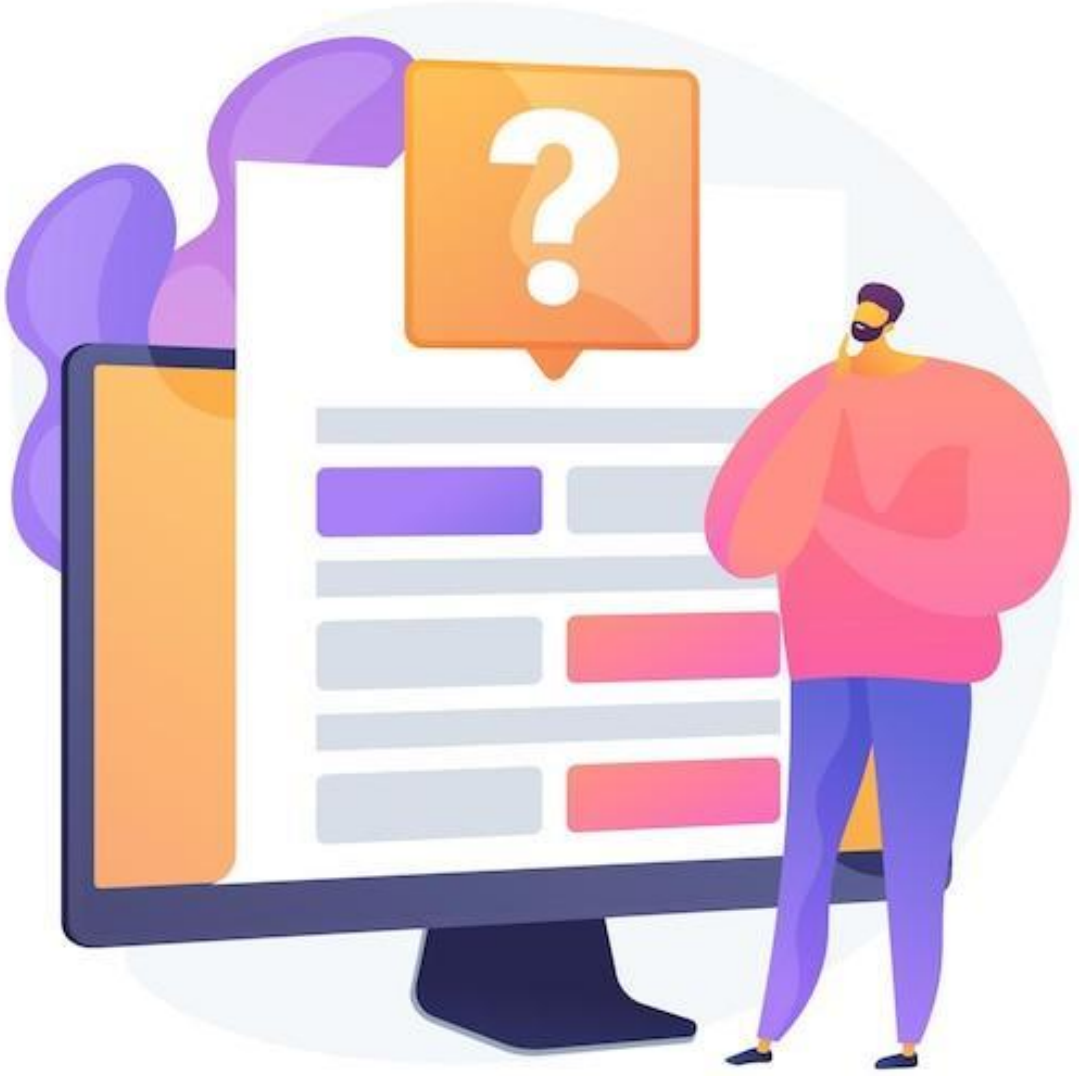
- Vsaka organizacija, ki obdeluje osebne podatke posameznikov v EU, mora upoštevati uredbo GDPR.
- "**Obdelava**" je širok pojem, ki zajema skoraj vse, kar se lahko počne s podatki: zbiranje, shranjevanje, prenašanje, analiziranje itd.
- "**Osebni podatki**" so vse informacije, ki se nanašajo na posameznika, na primer ime, e-poštni naslov, naslov IP, barva oči, politična prepričanja itd.

Organizacija, ki obdeluje osebne podatke ljudi v EU (na primer s sledenjem na svojem spletnem mestu), mora upoštevati uredbo GDPR, tudi če sicer nima nobene zveze z EU. Uredba GDPR tudi ni omejena samo na pridobitna podjetja.

Slika: Pch.vector, Freepik

MOBILE MONEY

Preverite svoje znanje!



Slika: Vectorjuice, Freepik

1. Katero od naslednjih gesel je najmočnejše?

Samo en odgovor je pravilen!

A. John1234

B. John1990

C. John051190

D. J0Hn!2nO

2. Kaj od naštetega so osebni podatki?

Samo en odgovor je pravilen!

A. Naslov IP

B. E-poštni naslov

C. Vse našteto

D. Identifikatorji piškotkov v brskalniku

3. Če se v brskalniku prikaže znak ključavnice, to pomeni, da je brskalnik stran zaklenil, ker ni varna.

Yes, the statement is correct

No, the statement is wrong

4. Kaj od naštetega NISO občutljivi osebni podatki

Samo en odgovor je pravilen!

A. Fotografije

B. Domači naslov

C. Podatki v zvezi z zdravjem

D. Politična mnenja

6. Ali je pošiljatelj lahko pokazatelj, da je e-poštno sporočilo neželena pošta?

Da

Ne

7. Kaj nikoli ni pravi odziv, če prejmete domnevno neželeno e-poštno sporočilo?

Samo en odgovor je pravilen!

A. Izbrisati e-poštno sporočilo

B. Preveriti pošiljatelja

C. Preveriti referenčno vrstico

D. Odgovoriti in vprašati, ali je to neželena pošta

MOBILE MONEY

Čestitke!

To temo ste zaključili!

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