



## Vaje za mobilno plačevanje

### **MODUL 2**

#### **Vaja 1**

#### Preverjanje znanja

#### **Predvideno trajanje:**

10 minut

#### **Potrebujete:**

Napravo z dostopom do spleta za razjasnjevanje dvomov; papir in svinčnik

#### **Navodila:**

Na naslednji strani je 5 vprašanj o zaščiti in varnosti na spletu, s katerimi boste preverili svoje znanje.

Obkrožite odgovore in na 3. strani preverite pravilnost ter preberite pojasnila – pa brez kukanja!

: -)



1. Kateri je najpogostejši način prenosa virusov?
  - A. E-pošta
  - B. Takojšnje sporočanje
  - C. Prenos s spleta
  - D. Prenosni pomnilniški mediji
  
2. Kaj od naštetega bi bilo najboljše geslo?
  - A. MySecret
  - B. Iw2c^tILV
  - C. Abc123
  - D. George1234
  
3. Sestra vam iz službe pošlje e-poštno sporočilo z ohranjevalnikom zaslona, za katerega pravi, da bi vam bil všeč. Kaj morate storiti?
  - A. Prenesti si ga moram na svoj računalnik, saj je iz zanesljivega vira.
    - B. Sporočilo moram posredovati prijateljem, da ga bodo delili še z drugimi.
  
4. Poklicate moram tehnično podporo in prositi, naj mi ga pomagajo namestiti.
  - A. Sporočilo moram izbrisati.
  
5. Kadar prejmete e-poštno sporočilo neznanega pošiljatelja, ki vsebuje prilogo, morate:
  - A. Odpreti prilogo in si ogledati njeno vsebino.
  - B. Izbrisati e-poštno sporočilo.
  - C. Posredovati sporočilo svojim sodelavcem, da bodo lahko prilogo najprej odprli oni.
  - D. Preposlati sporočilo v svoj osebni e-poštni račun, da ga lahko odprem doma.



## 1. **Kateri je najpogostejši način prenosa virusov?**

### **A. E-pošta**

E-pošta je najpogostejši način prenosa virusov. Kibernetični kriminalci pogosto uporabljajo e-pošto kot pot za širjenje zlonamerne programske opreme. Ta e-poštna sporočila lahko zbuja vtis, da prihajajo iz zanesljivih virov, zato so še posebej nevarna. Ko prejemnik odpre prilogo ali klikne povezavo, se virus lahko prenese v njegovo napravo in začne delovati.

## 2. **Kaj od naštetega bi bilo najboljše geslo?**

### **B. Iw2c^tILV**

Ker upošteva ključna načela ustvarjanja močnega gesla:

**Zapletenost:** vsebuje kombinacijo velikih in malih tiskanih črk, števil in posebnih znakov, zato ga napadalci težko uganejo ali razvozljajo z metodo grobe sile.

**Dolžina:** je dovolj dolgo, kar pomeni dodatno zaščito. Daljša gesla je v splošnem težje razvozlati.

**Nepredvidljivost:** Geslo ne vsebuje besed ali vzorcev, ki bi jih zlahka uganili – pogostih, preprostih ali takih, ki bi bili povezani z uporabnikom.

## 3. **Sestra vam iz službe pošlje e-poštno sporočilo z ohranjevalnikom zaslona.**

### **D. Sporočilo moram izbrisati.**

Štiri velika tveganja:

1. Nekateri ohranjevalniki zaslona vsebujejo viruse.
2. S klikom na zlonamerno povezavo lahko okužimo računalnik.
3. E-poštni naslov je lahko ponarejen, in čeprav je v sporočilu navedeno, da ga pošilja oseba, ki jo poznate, ste o tem lahko prepričani šele, ko preverite.
4. Nekatera spletna mesta in povezave dajejo vtis zakonitosti, v resnici pa so prevarantska in je njihov namen krasti vaše podatke.

**Bodite varni in uživajte v digitalnem svetu!**



Vaje za mobilno plačevanje

## **MODUL 2**

### **Vaja 2**

#### **Je povezavo varno odpreti?**

**Predvideno trajanje:**

10 minut

**Potrebujete:**

Napravo z dostopom do spleta za razjasnjevanje  
dvomov; papir in svinčnik

**Navodila:**

Preberite besedilo.  
Razmislite.

Vajo bomo opravili skupaj, da boste razumeli, zakaj  
je povezava varna oziroma zakaj ni.



### 1. Odločite se, ali je povezavo varno odpreti:

Recimo, da od banke prejmete e-poštno sporočilo, v katerem vas prosijo, da kliknete povezavo, kakršno vidite spodaj, in posredujete osebne podatke, kot so uporabniško ime, gesla in podatki o kreditni kartici.

[http://url5423.eka.de/ls/click?](http://url5423.eka.de/ls/click?upn=V1OaWNMSPs2Lb0JqHpnyTLRlk2703ToIFpo2vd2MKt5gB6dYAUvw1B-2FnC6T5iVsCdbcug7l6pkTad-2FBfACSIC-2BKw-3D-3DhmuAs-OaWNMSPs2Lb0JqHpny-asDvdva)

[upn=V1OaWNMSPs2Lb0JqHpnyTLRlk2703ToIFpo2vd2MKt5gB6dYAUvw1B-2FnC6T5iVsCdbcug7l6pkTad-2FBfACSIC-2BKw-3D-3DhmuAs-OaWNMSPs2Lb0JqHpny-asDvdva](http://url5423.eka.de/ls/click?upn=V1OaWNMSPs2Lb0JqHpnyTLRlk2703ToIFpo2vd2MKt5gB6dYAUvw1B-2FnC6T5iVsCdbcug7l6pkTad-2FBfACSIC-2BKw-3D-3DhmuAs-OaWNMSPs2Lb0JqHpny-asDvdva)

Ne hitite, dobro premislite in se odločite, ali je to povezavo varno odpreti.

Razmislite o razlogih.

### **Odgovor:**

Povezava **ni** varna iz številnih razlogov:

- Uporablja protokol 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 nikoli ne prosi za posredovanje uporabniških imen, gesel ali podatkov o kreditni kartici.



## Vaje za mobilno plačevanje

### **MODUL 2**

### **Vaja 3**

## Ocena vaše spletne varnosti

#### **Predvideno trajanje:**

10 minut

#### **Potrebujete:**

Napravo z dostopom do spleta za test na spletu;  
svinčnik za test na papirju.

#### **Navodila:**

Test lahko opravite individualno ali v skupini, na spletu ali s papirjem in svinčnikom. Možna odgovora sta DA in NE.

Če ste test opravili na spletu, nato dobite rezultat, sicer pa vam ga pripravi in pojasni mentor.



Odgovorite z DA ali NE.

1. Ali na svojih napravah uporabljate dvofaktorsko avtentikacijo, na primer avtentikacijo s prstnim odtisom in tudi geslo?
2. Ali uporabljate shrambo gesel? To je aplikacija, v kateri varno hranite vsa vaša gesla za različne račune.
3. Ali na spletu uporabljate način "zasebno brskanje"?
4. Ali imate vse svoje profile na družbenih omrežjih nastavljene kot zasebne?
5. Ali na družbenih omrežjih redno objavljate fotografije, iz katerih je razvidno, kje se nahajate?
6. Ali redno pregledujete svoje bančne transakcije in preverjate, da med njimi ni neznanih izdatkov?
7. Ali pri spletnem nakupovanju pred vnosom podatkov o kreditni kartici poiščete znak ključavnice ali drug dokaz o varnosti spletnega mesta, ki ste ga obiskali?
8. Ali imate v svojem računalniku nameščeno zaščitno programsko opremo, npr. protivirusni program, protivohunski program ali požarni zid?
9. Če vas računalnik pozove k posodabljanju programske opreme, ali bi to storili takoj?
10. Ali uporabljate drugačno geslo za vsak račun, ki ga imate?

Čestitke!

Ocena vaše spletne varnosti je \*\*\*\*\* \_\_\_\_\_ \*\*\*\*\*

Vrhunska varnost!