Spletna varnost v šolskem okolju.

eAsistent

Socialni inženiring

Socialni inženiring je manipulativna tehnika, ki jo uporabljajo kriminalci, da pridobijo zaupne informacije ali izvedejo napade na ciljne osebe ali organizacije. Namesto izkoriščanja ranljivosti v tehnologiji se socialni inženiring osredotoča na izkoriščanje človeških psiholoških mehanizmov in interakcij.

V šolskem okolju se pogosto pojavljajo naslednje oblike napadov socialnega inženiringa:

1. **Prevarantski telefonski klici:**
   Napadalci se lahko predstavijo kot starši, uradniki šolske uprave, ministrstva za šolstvo ali centra za socialno delo in poskušajo pridobiti zaupne informacije, kot so osebni podatki učencev ali dostop do šolskih sistemov.

2. **Ribarjenje (phishing):**
   Napadalci lahko pošljejo lažna elektronska sporočila, ki se zdijo, da prihajajo iz šolskih ali drugih institucij s katerimi šola sodeluje, in prosijo učiteljice, naj razkrijejo svoje uporabniško ime in geslo ali dostopne podatke do e-učilnic

3. **Manipulacija prek družbenih omrežij:**
   Napadalci preučujejo profile učiteljic na družbenih omrežjih in lahko uporabijo pridobljene informacije, da se pretvarjajo, da so učenci ali starši ter pridobijo zaupne podatke.

Da bi se zaščitili pred napadi socialnega inženiringa, je pomembno upoštevati naslednje smernice:

1. **Previdnost pri komunikaciji:**
   Bodite previdni pri deljenju osebnih informacij prek telefona ali elektronske pošte. Vedno preverite verodostojnost sogovornika in se posvetujte s pristojnimi osebami, če imate kakršne koli dvome. Upoštevajte pravilo manj je več!

2. **Prepoznavanje sumljivih sporočil:**
   Bodite pozorni na sumljiva elektronska sporočila, ki prosijo za osebne podatke ali vas preusmerjajo na nepreverjene spletne strani. Preverite naslov pošiljatelja in se posvetujte z IT osebjem šole, če imate kakršne koli dvome.

3. **Omejitev dostopa do osebnih podatkov:**
   Skrbno ravnajte z osebnimi podatki med katere štejejo tudi gesla in do programske opreme dostopajte samo na varnih in zaupnih mestih. Uporabljajte dvofaktorsko indetifikacijo, če je na voljo.

Če sumite, da ste žrtev napada socialnega inženiringa, upoštevajte naslednje korake:

1. **Prekinite komunikacijo:**
   Če prejmete sumljiv telefonski klic ali elektronsko sporočilo, prekinite stik s pošiljateljem. Ne delite nobenih osebnih ali zaupnih informacij.

2. **Obvestite pristojne osebe:**
   Takoj obvestite vodstvo šole ali IT osebje o incidentu. Povejte jim podrobnosti napada in posredujte morebitne dokaze.

3. **Spremljajte račune in aktivnosti:**
   Redno preverjajte svoje šolske račune, e-pošto in druge sisteme. Če opazite nenavadne ali sumljive aktivnosti, nemudoma obvestite pristojne osebe.

Poleg tega je priporočljivo upoštevati naslednje dobre prakse za varnostno upravljanje v šolskem okolju:

1. **Močna gesla in večfaktorsko preverjanje:**
   Uporabljajte močna gesla za svoje šolske račune in omogočite večfaktorsko preverjanje, kar dodatno povečuje varnost dostopa.

2. **Posodabljanje programov in sistemov:**
   Redno posodabljajte programsko opremo na računalnikih in drugih napravah. S tem boste odpravili morebitne varnostne ranljivosti.

3. **Preverjanje varnosti spletnih strani:**
   Preden vnesete osebne podatke na spletno stran, preverite, ali uporablja varno povezavo (HTTPS) in ali je pristnost strani preverjena.

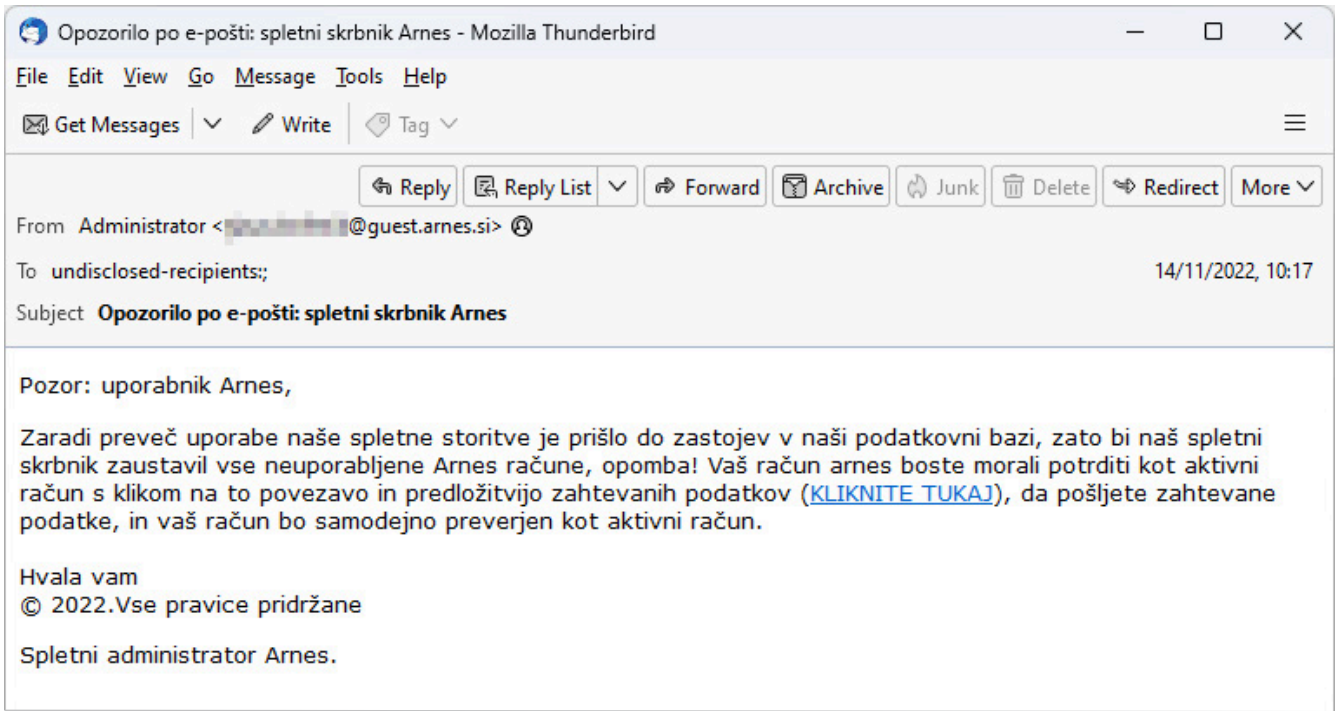
Kaj je “ribarjenje”?

Ribarjenje (phishing) je oblika napada socialnega inženiringa, pri kateri napadalci poskušajo pridobiti osebne podatke, kot so uporabniška imena, gesla, številke kreditnih kartic ali druge zaupne informacije, s pretvarjanjem, da so zaupanja vredne institucije ali osebe. To storijo s pošiljanjem lažnih elektronskih sporočil, ki se zdijo, da prihajajo iz znanih organizacij, kot so banke, šolska uprava ali družbena omrežja.

Da bi se zaščitili pred ribarjenjem, lahko upoštevate naslednje smernice:

1. **Bodite pozorni na sumljiva sporočila:**
   Preverite podrobnosti, kot so naslov pošiljatelja in pravopisne napake v sporočilu. Sumljiva sporočila pogosto vsebujejo nujne zahteve, grožnje ali obljube o nagradah.

2. **Ne klikajte na sumljive povezave:**
   Preverite URL povezave v elektronskih sporočilih. Če se zdi sumljiva ali nepreverjena, se izogibajte klikanju nanje. Namesto tega obiščite spletno stran neposredno tako, da jo vnesete v spletni brskalnik.



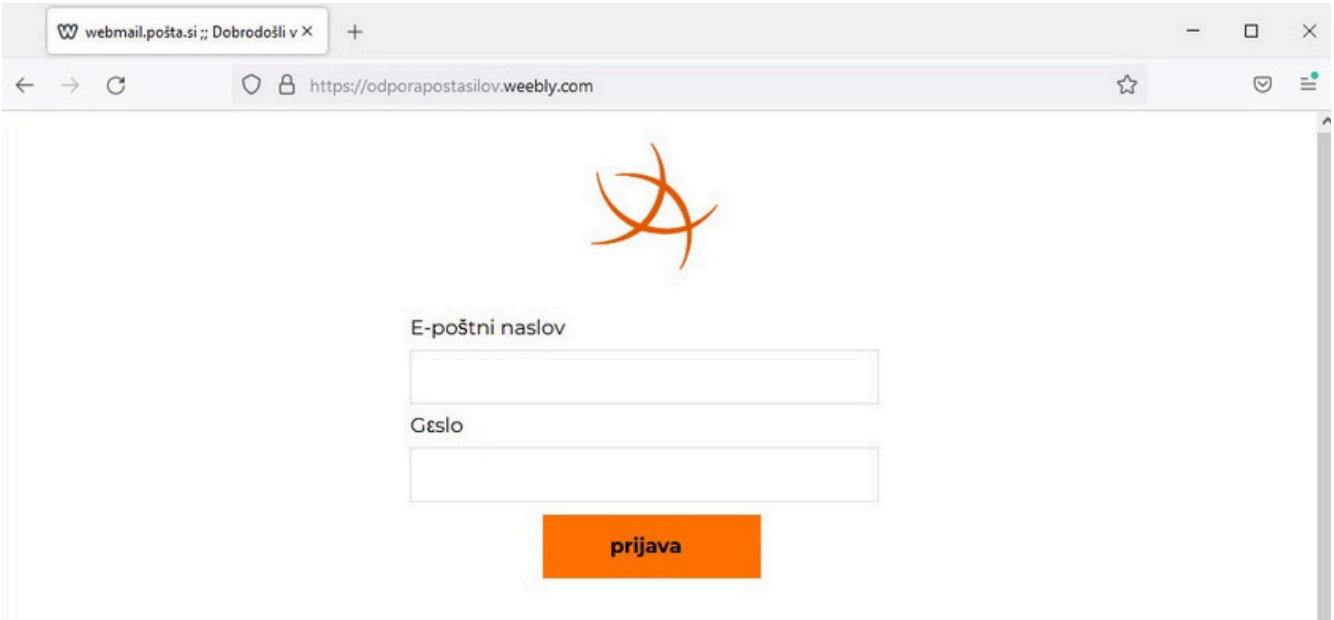
Kaj so spletne prevare?

Spletne prevare so oblike napadov, pri katerih napadalci izkoriščajo spletno okolje za zavajanje, izsiljevanje ali pridobivanje osebnih podatkov od učiteljic. Te prevare vključujejo različne metode, kot so lažna spletna mesta, lažne nagradne igre, prevarantski nakupi ali lažna predstavitev podjetij ali organizacij.

Da bi se zaščitili pred spletnimi prevarami, lahko upoštevate naslednje smernice:

1. **Preverjanje verodostojnosti spletnih mest:**
   Preden vnesete osebne podatke ali opravite nakup prek spleta, preverite verodostojnost spletnega mesta. Pazite na pravopisne napake, sumljive URL naslove ali odsotnost zaščitne enkripcije (HTTPS).

2. **Previdnost pri deljenju osebnih podatkov:**
   Ne razkrivajte osebnih podatkov, kot so številke osebnih dokumentov, bančni podatki ali gesla, na nepreverjenih spletnih mestih ali prek nezaščitenih komunikacijskih kanalov.



Priporočila za zaščito

Multifaktorska avtentikacija

Multifaktorska avtentikacija je varnostni postopek, pri katerem se za potrditev identitete zahteva več kot en način avtentikacije, običajno kombinacija nečesa, kar uporabnik ve (geslo), ter nečesa, kar uporabnik ima (fizični ključ ali pametni telefon). V nadaljevanju prikaz in navodila za vzpostavitev dveh možnosti varne prijave. **eA prijava** in **YubiKey**.

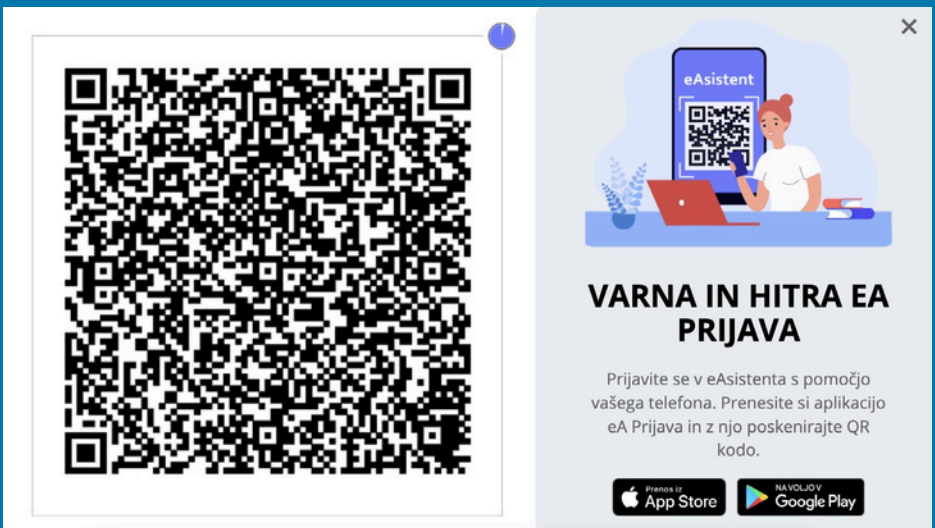
eA Prijava

YubiKey

Navodila za vzpostavitev

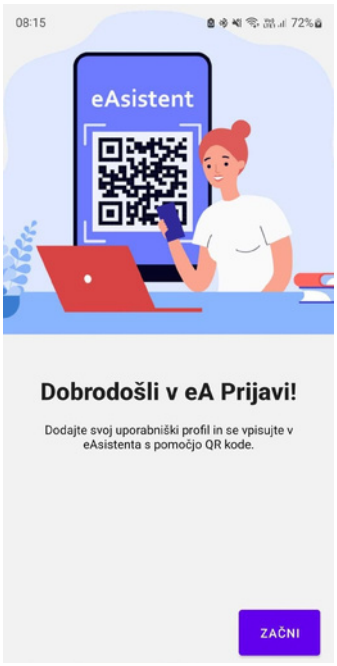
NAVODILA ZA UPORABO eA PRIJAVA

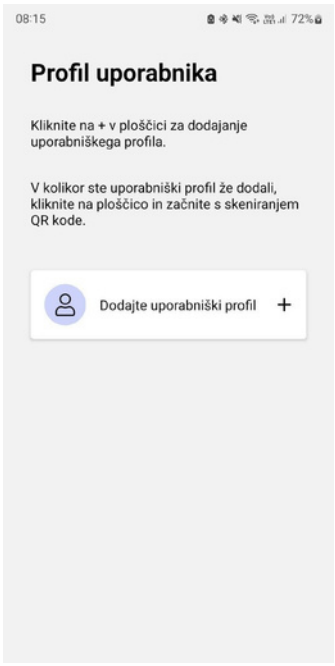
Aplikacija uporabnikom omogoča hitro in varno prijavo preko QR kode. Preko aplikacije se lahko prijavijo vsi uporabniki.
QR koda se nahaja na prijavni strani eAsistenta (slika levo).

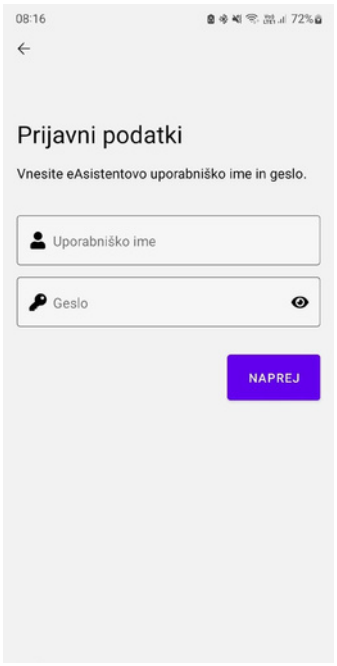


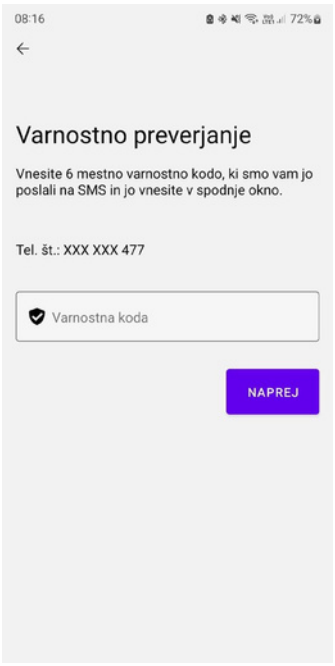
Na naslednji strani si lahko ogledate podrobnejša navodila po korakih.
Na voljo pa tudi video navodila na **TEJ POVEZAVI.**

V aplikaciji ima uporabnik možnost dodati nov profil ali izbere že obstoječ profil. V kolikor uporabnik dodaja nov profil se mu, s klikom na “+”, odpre forma za vnos uporabniškega imena in gesla. Po vnosu uporabniškega imena in gesla s klikom “NAPREJ” preide na varnostno preverjanje kjer, na svojo telefonsko številko (vneseno v svoj eA profil), prejme varnostno 6-mestno kodo. Po vneseni varnostni kodi s klikom “NAPREJ” uspešno doda nov uporabniški profil v aplikacijo.

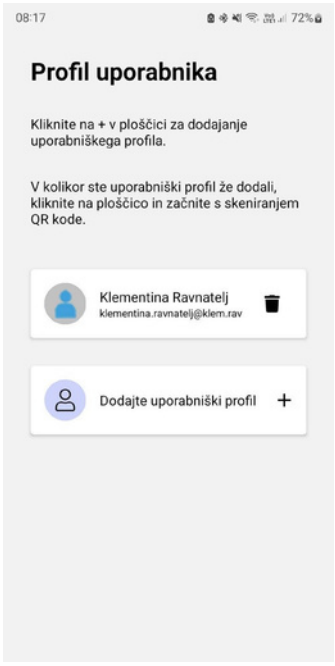


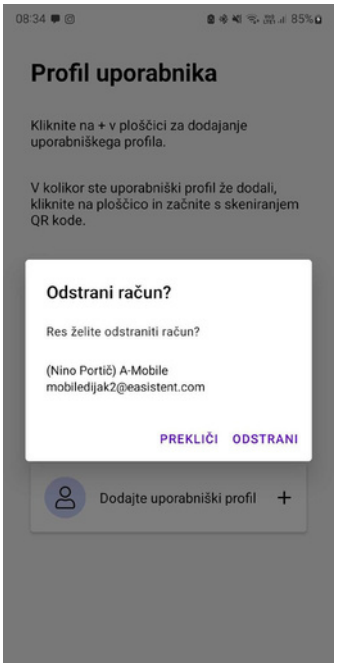






V aplikaciji ima lahko uporabnik dodanih več profilov za prijavo, npr. profil učitelja, profil starša,... Za prijavo v enega izmed profilov mora uporabnik izbrati želeni profil za prijavo. Po izbiri profila se mu odpre možnost skeniranja QR kode. QR kodo poskenira iz prijavne strani eA, po uspešnem skeniranju pa se zgodi avtomatska prijava v eAsistenta. Uporabnik lahko račun v aplikaciji tudi izbriše, s klikom na ikono “smetnjak”, ki se nahaja desno na profilni ploščici.





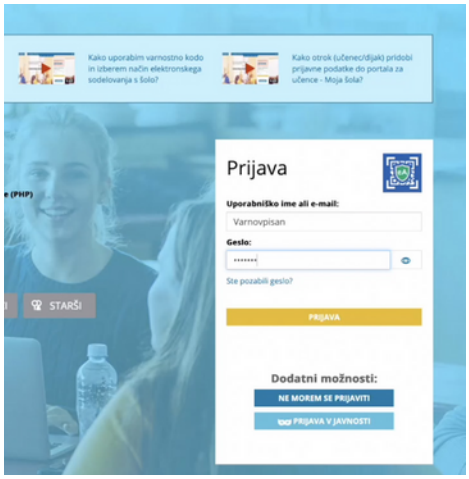
Navodila

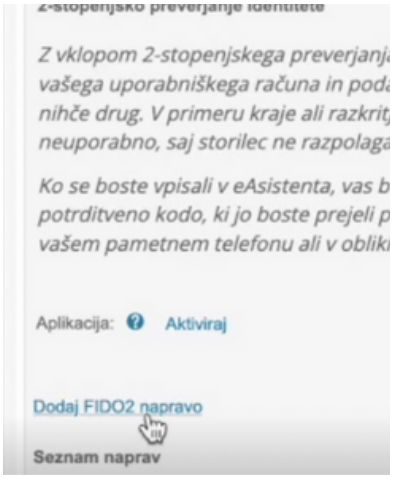
NAVODILA ZA VZPOSTAVITEV IN UPORABO YubiKey

YubiKey, ki je USB ključek, ki uporablja standardne protokole za avtentikacijo, kot so U2F (Universal 2nd Factor), FIDO2 (Fast Identity Online) in OTP (One-Time Password). YubiKey omogoča uporabnikom, da varno in enostavno potrjujejo svojo identiteto pri spletnih storitvah, računalnikih in mobilnih napravah.

Na naslednji strani si lahko ogledate podrobnejša navodila po korakih. Na voljo pa tudi video navodila na **TEJ POVEZAVI.**

1. Vpišite se v svoj račun v eAsistentu.
2. Desno zgoraj pri imenu uporabnika kliknite gumb **Nastavitve uporabnika**.
3. Spodaj levo kjer piše “dvostopenjsko preverjanje identitete” kliknite gumb **Dodaj FIDO2 napravo.**
4. Ko začne **Yubikey**, ki je nameščen v vašo napravo, utripati, pomeni, da ga **z dotikom nanj** lahko dodate, na kar vas opozarja tudi brskalnik.
5. Ko je naprava najdena, je dodana pod seznamom naprav. **Shranimo spremembo**.





Test delovanja: Odjavimo se iz računa, zopet vpišemo uporabniško ime in geslo. Ob prijavi nas prosi, da se dotaknemo svoje FIDO2 naprave. Z dotikom naprave s tem potrdimo svojo identiteto in dostopamo do računa.

PRIPOROČILA:
Hranite YubiKey na varnem mestu, da preprečite morebitno njegovo nepooblaščeno uporabo. V primeru da do vašega uporabniškega računa dostopate preko različnih naprav nosite YubiKey s seboj.

Skrbni in informacijsko ozaveščeni učitelj imajo ključno vlogo pri zagotavljanju visoke ravni informacijske varnosti na šolah. S svojim zavedanjem o tveganjih, doslednim upoštevanjem varnostnih smernic lahko učitelji in vodstvo šole vzpostavijo varno in zaupno okolje, ki varuje podatke ter spodbuja varno uporabo tehnologije v izobraževalnem procesu.