# Privatnost i anonimnost na Internetu

1

00:00:00,000 --> 00:00:11,400

Dobrodošli. U ovoj lekciji ćemo naučiti kako zaštititi privatnost na Internetu uz pravilno podešavanje postavki kolačića.

2

00:00:11,400 --> 00:00:22,966

Pri pretraživanju weba svaki korisnik neprimjetno

ostavlja digitalni trag te se osobne informacije ne

mogu se sakriti. Napravljen je kompromis u kojem

3

00:00:22,966 --> 00:00:33,199

su privatnost i anonimnost zamijenjene za

sigurnost i udobnost. Bez obzira na to, nekim je

ljudima njihova privatnost vrlo važna. Na kraju

4

00:00:33,200 --> 00:00:46,300

krajeva, svaki bi korisnik trebao imati pravo sam

izabrati kojim organizacijama i pojedincima želi

dati vlastite podatke na raspolaganje.

5

00:00:46,300 --> 00:00:55,666

Nažalost, to je danas rijetko slučaj. Osim što

gotovo svatko može saznati ponešto o drugome

bez velikog truda, te se informacije često i

6

00:00:55,666 --> 00:00:59,966

zloupotrebljavaju.

7

00:00:59,966 --> 00:01:09,499

Web-mjesta sakupljaju podatke o korisnicima na

razne načine. Osnovna sredstva kojima se koriste

jesu opće informacije koje dobiju od preglednika,

8

00:01:09,500 --> 00:01:15,266

podaci koje korisnici unose u web forme te

kolačići (cookie).

9

00:01:15,266 --> 00:01:27,599

U osnovi, kolačić (cookie) jest obična tekstualna

datoteka kakve rabe web-poslužitelji da bi

pohranili informacije o korisniku i njegovim

10

00:01:27,600 --> 00:01:37,200

aktivnostima na nekom web-mjestu. Kompanija, vlasnik poslužitelja se zatim koristi tim podacima u različite svrhe.

11

00:01:37,200 --> 00:01:47,266

Primarna namjena jest prilagodba sadržaja korisniku i predmemoriranje nekih postavki koje je korisnik ranije odabrao. Rabe se i za pohranu

12

00:01:47,266 --> 00:01:57,032

lozinke za pristup poštanskom sandučiću, kako je

korisnik ne bi svaki put morao ponovno upisivati.

Osnovna ideja nije loša jer olakšava

13

00:01:57,033 --> 00:02:08,366

pregledavanje Interneta te kolačići, osim

pohranjivanja nekih osobnih podataka, omogućuju

web-mjestima da prate i navike posjetitelja.

14

00:02:08,366 --> 00:02:17,132

Kolačić ne može sadržavati štetni kod s obzirom na to da se nalazi u tekstualnoj, a ne izvršnoj datoteci.

15

00:02:17,133 --> 00:02:25,199

Ne može pristupiti disku. U osnovi ne predstavlja

neki sigurnosni rizik osim narušavanja privatnosti.

16

00:02:25,200 --> 00:02:37,700

Jedan od primjera zlouporabe, jest otimanje

kolačića (cookie hijacking). U pravilu kolačiću

mogu pristupiti samo domene od kojih su stvoreni.

17

00:02:37,700 --> 00:02:44,966

Nekoliko je slučajeva poznato u kojima su web-

mjesta mogla pristupiti svim kolačićima na

računalu.

18

00:02:44,966 --> 00:02:55,366

Ako bi podacima u kolačićima mogla pristupiti

neka zlonamjerna osoba, mogla bi ih iskoristiti za

imitiranje korisnika, mogla bi stvoriti kopiju,

19

00:02:55,366 --> 00:03:04,499

imitaciju originalnog kolačića i pristupiti nekom

web-mjestu predstavljajući se kao netko drugi.

Opasnost je najočitija kod kolačića koji omogućuju

20

00:03:04,500 --> 00:03:09,633

automatski pristup korisničkom računu.

21

00:03:09,633 --> 00:03:19,433

Postavke vezane za privatnost i postupanje s

kolačićima dostupne su unutar kartice „Privatnost“

(Privacy). Šest mogućnosti upravljanja kolačićima

22

00:03:19,433 --> 00:03:34,766

uključuju blokiranje ili dopuštanje svih kolačića te

četiri dodatne razine privatnosti.

23

00:03:34,766 --> 00:03:44,799

Visoka razina ne dopušta stvaranje kolačića koji

uključuju osobne podatke, bez suglasnosti

korisnika računala. Web-mjesta koja nemaju

24

00:03:44,800 --> 00:03:57,766

definiranu kompaktnu izjavu o privatnosti ne mogu

postavljati kolačiće. (Compact Privacy statement –

tekst koji navodi točno kako će kolačići biti

25

00:03:57,766 --> 00:04:01,099

korišteni te njihovo vrijeme trajanja.)

26

00:04:01,100 --> 00:04:11,766

Srednja do visoka razina blokira kolačiće treće

strane s web-mjesta koja nemaju kompaktnu izjavu

o privatnosti. Blokiraju se i kolačići treće strane

27

00:04:11,766 --> 00:04:21,999

koji rabe osobne informacije bez eksplicitne

suglasnosti te kolačići prve strane (first-party) koji

se koriste osobnim informacijama bez implicitne

28

00:04:22,000 --> 00:04:24,966

suglasnosti korisnika.

29

00:04:24,966 --> 00:04:35,999

Srednja razina odobrava kolačiće prve strane koji

se koriste osobnim informacijama bez implicitne

suglasnosti, ali takvi kolačići bivaju izbrisani pri

30

00:04:36,000 --> 00:04:47,966

zatvaranju Internet Explorera. Blokirani su kolačići

treće strane kao i kod prethodne razine. Srednja je

razina standardno postavljena.

31

00:04:47,966 --> 00:04:58,732

Niska razina prihvaća sve kolačiće prve strane.

Kolačići treće strane s web-mjesta bez kompaktne

izjave o privatnosti blokirani su, a kolačići treće

32

00:04:58,733 --> 00:05:11,333

strane koji rabe osobne informacije bez implicitne

suglasnosti dopušteni su, no brišu se pri izlasku iz

Internet Explorera.

33

00:05:11,333 --> 00:05:24,299

Vrlo često želimo blokirati kolačiće koje naše informacije mogu prenijeti tzv. trećim stranama. To radimo na sljedeći način: Unutar web preglednika

34

00:05:24,300 --> 00:05:37,100

otvorimo Internetske mogućnosti --> Privatnost pa odaberemo "Dodatno" nakon čega se otvara sljedeći dijaloški okvir u kojem podesimo

35

00:05:37,100 --> 00:05:48,300

postavke na način kako je prikazano na slici u

nastavku. Označimo "Odbaci automatsku obradu

kolačića", "Prihvatimo kolačiće od prve strane",

36

00:05:48,300 --> 00:05:55,866

međutim blokiramo "Kolačiće treće strane".

Potvrdimo sa "U redu".

37

00:05:55,866 --> 00:05:59,599

Lekcija je završena.

# Prilagodba Internet Explorera

1

00:00:00,000 --> 00:00:07,833

Dobrodošli. U sljedećem videu ćemo vidjeti kako obrisati povijest pregledavanja.

2

00:00:07,833 --> 00:00:18,733

U prethodnoj smo lekciji rekli kako svaki korisnik

Interneta ostavlja na njemu digitalni trag. Također

smo pokazali načine kako taj trag možemo

3

00:00:18,733 --> 00:00:22,166

kontrolirati.

4

00:00:22,166 --> 00:00:33,166

Međutim, moramo biti svjesni da i na našim

računalima ostavljamo tragove o posjećenim web

mjestima kao i sve podatke vezane uz njih, poput

5

00:00:33,166 --> 00:00:43,766

spremljenih lozinki i sl. Tijekom pregledavanja web-stranica Windows Internet Explorer pohranjuje sljedeće vrste podataka: Privremene internetske

6

00:00:43,766 --> 00:00:56,732

datoteke; Kolačiće; Povijest web-mjesta koja ste

posjetili; Podatke koje ste upisali u web-mjesta ili

adresnu traku, kao što su vaše ime i adresa, te

7

00:00:56,733 --> 00:01:06,533

adrese web-mjesta koja ste ranije posjetili;

Spremljene web-lozinke; Privremene podatke koje

pohranjuju dodaci preglednika.

8

00:01:06,533 --> 00:01:19,499

Ovo može biti posebno važno, ako su ti „tragovi“ ostavljeni na računalima kojima se služe i drugi korisnici poput raznih Internet kafića i sl. Vrlo je

9

00:01:19,500 --> 00:01:29,300

bitno nakon završetka pregledavanja web mjesta, znati i obrisati podatke o njima. To ćemo napraviti na sljedeći način.

10

00:01:29,300 --> 00:01:48,500

Unutar Internet Explorera otvorit ćemo "Internetske mogućnosti" te odabrati karticu "Općenito". Nakon toga kliknemo na "Obriši".

11

00:01:48,500 --> 00:01:58,966

nakon čega se pojavljuje sljedeći dijaloški okvir unutar kojega moramo označiti što želimo obrisati. Ovdje je označeno brisanje privremenih

12

00:01:58,966 --> 00:02:10,899

internetskih datoteka, kolačića i podataka s web

mjesta te povijesti pregledavanja. Nakon što smo

označili ono što želimo obirsati, kliknemo na

13

00:02:10,900 --> 00:02:13,133

"Izbriši".

14

00:02:13,133 --> 00:02:21,166

Lekcija je završena.

# Automatsko popunjavanje web obrazaca

1

00:00:00,000 --> 00:00:11,966

Dobrodošli. U slijedećem videu naučit ćemo što je to opcija automatskog popunjavanja web obrazaca unutar Internet Explorera.

2

00:00:11,966 --> 00:00:23,032

Opcija automatskog popunjavanja (AutoComplete) omogućuje da Internet Explorer pamti sve ono što je upisano, kao web adrese, pojmove kod

3

00:00:23,033 --> 00:00:33,699

pretraživanja Interneta, podatke upisivane u razne web obrasce poput imena i prezimena, datuma i godine rođenja i sl. Kada korisnik krene ponovno

4

00:00:33,700 --> 00:00:43,966

unositi te podatke, Internet Explorer ih pokuša sam dovršiti. Ako je ponuđeni završetak točan, nije potrebno podatak unijeti to do kraja, već samo

5

00:00:43,966 --> 00:00:46,732

pritisnuti tipku Enter.

6

00:00:46,733 --> 00:00:55,299

Većina će tu mogućnost smatrati veoma korisnom. I ovo su postavke koje će nam to omogućiti.

7

00:00:55,300 --> 00:01:14,233

U Internet pregledniku kliknite u gornjem desnom uglu "Postavke", zatim "Internetske mogućnosti", unutar toga odaberite karticu "Sadržaj" te

8

00:01:14,233 --> 00:01:18,099

"Postavke".

9

00:01:18,100 --> 00:01:31,233

Nakon čega se otvara sljedeći dijaloški okvir u kojem odabiremo za što želimo koristiti automatske postavke pohranjivanja.

10

00:01:31,233 --> 00:01:40,599

Koliko nam to god bilo (ne)simpatično, vodite računa da je ta opcija sigurnosni rizik, jer se svi ti podaci koji se koriste za automatsko popunjavanje

11

00:01:40,600 --> 00:01:50,133

pohranjuju na našem računalu. Najveći rizik predstavlja mogućnost pamćenja lozinki i korisničkih imena. Iako korisno i olakšava proces

12

00:01:50,133 --> 00:01:59,766

pristupa korisničkim računima, ostaje činjenica da su sve te lozinke onda pohranjene na računalu i bilo koji napadač može lako doći do njih i

13

00:01:59,766 --> 00:02:10,666

iskoristiti ih. Zbog toga je najbolje isključiti sve ponuđene opcije automatskog popunjavanja, te obrisati one podatke koji su već spremljeni.

14

00:02:10,666 --> 00:02:20,499

Za to je potrebno odabrati "Izbriši povijest samodovršetaka...".

15

00:02:20,500 --> 00:02:22,700

Lekcija je završena.

# Filtiranje sadržaja

1

00:00:00,000 --> 00:00:10,800

Dobrodošli. U ovoj lekciji ćemo naučiti kakospriječiti otvaranje pojedinih stranica uz filtriranje web sadržaja.

2

00:00:10,800 --> 00:00:22,333

World Wide Web je vrijedan izvor sadržaja kojimogu biti korisni, obrazovni, zabavni i sl. Sadržavai mnogo web stranica upitnog sadržaja, npr.

3

00:00:22,333 --> 00:00:31,566

pornografske stranice, stranice koje namećunasilje ili mržnju u nekom obliku i zlonamjernestranice koje pokušavaju inficirati računalo

4

00:00:31,566 --> 00:00:41,699

virusom ili kompromitirati sigurnost instalacijomtrojanskog konja ili neke druge vrste štetnog koda.Posebice kad su djeca u pitanju, a i u drugim

5

00:00:41,700 --> 00:00:52,200

situacijama, postoje sredstva s pomoću kojih semogu blokirati takva web-mjesta tako da ihpreglednik uopće neće prikazati.

6

00:00:52,200 --> 00:01:02,100

Dostupan je cijeli niz aplikacija koje filtriraju web-

sadržaj prije nego što se prikaže u prozoru

preglednika. Osim filtriranja sadržaja, nude i razne

7

00:01:02,100 --> 00:01:09,900

druge opcije „roditeljske kontrole“ kao nadzor

aktivnosti, vremensko ograničavanje,

ograničavanje obavijesnih skupina (newsgroup) i

8

00:01:09,900 --> 00:01:19,700

razgovora (chat), filtriranje elektroničke pošte i

slično. Najpoznatiji alati jesu: NetNanny,

CyberSitter, CyberPatrol. Osim komercijalnih,

9

00:01:19,700 --> 00:01:29,200

postoje i besplatni poput Microsoftovog

FamilySafety-a. Filtriranje sadržaja uglavnom

funkcionira na dva načina. Neki alati održavaju

10

00:01:29,200 --> 00:01:39,100

bazu podataka web mjesta za koje je poznato da

ulaze u jednu od kategorija koje bi bilo dobro

blokirati. Oni zatim blokiraju pristup bilo kojem

11

00:01:39,100 --> 00:01:48,833

web mjestu koje se nalazi u bazi podataka –

ovisno o načinu na koji je filtar sadržaja

konfiguriran. Druga metoda jest procjena sadržaja

12

00:01:48,833 --> 00:01:59,866

u realnom vremenu i potraga za ključnim riječima i

frazama ili nekim drugim elementima koji

naznačuju nepodoban sadržaj

13

00:01:59,866 --> 00:02:01,232

Lekcija je završena.

# Web-kupnja i financijske transakcije

1

00:00:00,000 --> 00:00:12,466

Dobrodošli. U sljedećem videu, naučit ćemo na što trebamo obratiti pozornost kod provođenja financijskih transakcija na Internetu.

2

00:00:12,466 --> 00:00:24,566

Kupnja putem Interneta vrlo je sklizak teren. Uza

sve prednosti koje pruža razgledanje i kupnja iz udobnosti vlastitog doma, takav pristup krije

3

00:00:24,566 --> 00:00:34,132

mnoge rizike. Mnogi su rizici, no postoji i mnogo

metoda pokušaja zaštite takvih oblika transakcija.

4

00:00:34,133 --> 00:00:47,399

Glavni web-preglednici danas imaju mogućnost

korištenja SSL-om (Secure Socket Layer). SSL je

protokol koji pruža način dokazivanja autentičnosti

5

00:00:47,400 --> 00:00:58,366

web-poslužitelja te šifrira podatke koji se prenose

između preglednika i poslužitelja te osim toga

provjerava promet da bi osigurao da podaci nisu

6

00:00:58,366 --> 00:01:10,699

modificirani pri putovanju Internetom. SSL u kombinaciji s HTTPS-om (Secure Hypertext

Transfer Protocol) pruža najpopularniji oblik

7

00:01:10,700 --> 00:01:26,133

šifriranja veze, sjednice (session). HTTPS obično

radi preko TCP/IP priključne točke 443, za razliku

od uobičajenog HTTP protokola koji radi preko

8

00:01:26,133 --> 00:01:30,033

priključne točke 80.

9

00:01:30,033 --> 00:01:45,199

URL (Uniform Resource Locator) nekog HTTPS web-mjesta obično započinje s https:// umjesto http://, gdje to dodatno slovo „s“ upravo označuje

10

00:01:45,200 --> 00:01:57,100

sigurnu vezu. SSL rabi digitalne certifikate za

autentikaciju jedne ili obje strane u komunikaciji i

šifriranje podataka koje razmjenjuju. Pri posjetu

11

00:01:57,100 --> 00:02:06,833

sigurnom web-mjestu poslužitelj predoči certifikat,

a preglednik ga na korisničkom računalu

procjenjuje. Ako web-poslužitelj ima valjan digitalni

12

00:02:06,833 --> 00:02:17,733

certifikat, web-preglednik će automatski

uspostaviti vezu s pomoću SSL-a. Ako je veza

osigurana SSL-om, unutar prozora preglednika

13

00:02:17,733 --> 00:02:27,166

obično se negdje nalazi sličica zaključanog lokota (mjesto ovisi o pregledniku kojim se koristimo).

14

00:02:27,166 --> 00:02:38,599

No ako web-preglednik ima certifikat koji je

istekao ili nije valjan; ako je certifikat izdao izvor

koji u pregledniku nije definiran kao pouzdan ili

15

00:02:38,600 --> 00:02:49,300

ako certifikat nije vezan na isti poslužitelj s kojim je

preglednik u tom trenutku spojen, obično se

prikaže neka vrsta obavijesti ili upozorenja i

16

00:02:49,300 --> 00:03:00,166

korisnik treba sam izabrati hoće li prihvatiti taj

certifikat ili ne. U takvim slučajevima je uputno

dobro razmisliti o tome je li tvrtka koja je vlasnik

17

00:03:00,166 --> 00:03:10,499

web-mjesta ugledna i je li to uistinu ispravan

poslužitelj, a ne podvala odnosno zlonamjerna

kopija.Certifikat ne bi trebalo prihvatiti ako

18

00:03:10,500 --> 00:03:21,100

korisnik nije potpuno siguran u valjanost certifikata i legitimnost web-mjesta odnosno trebalo bi takvo web-mjesto napustiti.

19

00:03:21,100 --> 00:03:31,900

Za razliku o stranice koju smo vidjeli, s nevažećim certifikatom, stranica s ispravnim certifikatom izgleda upravo ovako. Ima sve

20

00:03:31,900 --> 00:03:40,700

potrebne i ključne elemente, a to je: počinje s https i ima znak lokotića.

21

00:03:40,700 --> 00:03:51,000

Na prethodnim dvjema slikama smo vidjeli kako izgleda stranica s valjanim i isteklim certifikatom. U web kupnju (online purchase) smijemo se

22

00:03:51,000 --> 00:04:02,166

upuštati samo ukoliko se cijeli proces obavlja preko sigurnih stranica s valjanim certifikatima. To je jedini način da izbjegnemo neki od oblika

23

00:04:02,166 --> 00:04:15,899

prevara koje vrebaju na Internetu. Sigurna stranica je, kako je prikazano na prethodnoj slici, obilježena s lokotićem u desnom uglu i u većini

24

00:04:15,900 --> 00:04:20,600

slučajeva bi prije samog naziva stranice trebalo stajati https.

25

00:04:20,600 --> 00:04:23,366

Lekcija je završena.

# Neovlašteno traženje informacija (phishing i pharming)

1

00:00:00,000 --> 00:00:08,933

Dobrodošli. U ovom videu naučit ćemo koje su metode neovlaštenog pridobivanja osobnih podataka.

2

00:00:08,933 --> 00:00:18,299

Neovlašteno traženje informacija (phishing i pharming) i mnoge druge tehnike varanja korisnika temelje se na socijalnom inženjeringu.

3

00:00:18,300 --> 00:00:29,633

Prijevarom, manipulacijom se natjera korisnika da samostalno izvrši neku radnju (instaliranje nekog programa, otkrivanje osobnih podataka i sl.).

4

00:00:29,633 --> 00:00:39,899

Takva je radnja najčešće njemu samom na štetu, ali je prijevara obično dovoljno dobro izvedena da toga nije svjestan. Barem ne na vrijeme.

5

00:00:39,900 --> 00:00:47,700

Neovlašteno traženje informacija (phishing) uključuje kontaktiranje žrtve preko elektroničke pošte, soba za razgovor (chat rooms) ili usluga

6

00:00:47,700 --> 00:00:53,833

trenutačnih poruka (instant messaging) i jedan je od oblika kibernetičkog kriminala.

7

00:00:53,833 --> 00:01:05,266

Najčešće se šalje neka vrsta obavijesti kako je potrebno unijeti određene osobne podatke sa svrhom potvrde ili ažuriranja korisničkog računa,

8

00:01:05,266 --> 00:01:16,966

radi poziva za darivanje novca u lažne dobrotvorne svrhe, obavijesti o nekom novčanom dobitku, lažne obavijesti od administratora i slično.

9

00:01:16,966 --> 00:01:30,066

Mnogi korisnici nasjednu na takve prijevare, pogotovo zato što je obično riječ o naizgled legitimnim tvrtkama ili uslugama kao što su banke,

10

00:01:30,066 --> 00:01:40,066

pružatelji internetskih usluga (ISP), tvrtke za internetsku trgovinu i slično. Prijevare često uključuju poznata imena kao PayPal, eBay ili

11

00:01:40,066 --> 00:01:42,932

poznate banke.

12

00:01:42,933 --> 00:01:53,566

Unutar te obavijesti (najčešće e-poruke) nalazi se poveznica (link) na neko web-odredište gdje je potrebno unijeti podatke. Klikom na poveznicu,

13

00:01:53,566 --> 00:02:04,432

web preglednik otvara stranicu koja izgleda vrlo stvarno i uvjerljivo. To je obično lažna stranica i sve unesene podatke preuzima autor prijevare.

14

00:02:04,433 --> 00:02:15,633

Podaci koji se traže jesu osobni podaci, lozinke, brojevi kreditnih kartica, brojevi bankovnih računa i slično, a cilj je vrlo očit – krađa identiteta i

15

00:02:15,633 --> 00:02:24,399

financijska prijevara. Klikom na takve poveznice, osim krađe osobnih podataka, velika je vjerojatnost i da se inicira

16

00:02:24,400 --> 00:02:34,433

instalacija i nekakvoga štetnog koda poput špijunskih programa (spyware), crva ili trojanskih konja.

17

00:02:34,433 --> 00:02:44,133

Takva prijevara (phishing) uključuje integraciju više elemenata, moguće špijunskog koda (spyware) koji sakuplja informacije o korisniku koje poslije

18

00:02:44,133 --> 00:02:54,533

služe za slanje prave vrste obavijesti na koju će konkretan korisnik nasjesti. Jednako tako, da bi se cijela zamka uspješno izvršila, primjenjuju se

19

00:02:54,533 --> 00:02:59,166

tehnike zavaravanja (spoofing).

20

00:02:59,166 --> 00:03:10,166

Činjenica je da poznate tvrtke ili financijske organizacije od korisnika nikada ne traže osobne podatke na takve načine, već obično šalju

21

00:03:10,166 --> 00:03:20,632

formalna pisma. Specifično je da su takvi tipovi elektroničkih poruka često puni gramatičkih grešaka i pogrešno napisanih riječi. Razlog takve

22

00:03:20,633 --> 00:03:30,633

nečitljivosti jest korištenje računalnih prevoditelja poput Google Translate-a koji nisu dovoljno dobri kako bi stranicu preveli pravopisno i gramatički

23

00:03:30,633 --> 00:03:37,533

ispravno.

24

00:03:37,533 --> 00:03:46,499

Neovlašteno traženje informacija prijevarom (pharming) također je vrsta prijevare s istim ciljem kao i prethodna, no s nešto opskurnijim

25

00:03:46,500 --> 00:03:56,266

metodama. Čak je i stručnjacima mnogo teže otkriti takvu prijevaru jer je gotovo nevidljiva. Zastrašujuća je pomisao takve prijevare koja je

26

00:03:56,266 --> 00:04:06,032

vrlo suptilna, dakle ne pokušava namamiti korisnika i izmanipulirati ga na neke radnje, a opet, riječ je o ozbiljnom narušavanju sigurnosti.

27

00:04:06,033 --> 00:04:15,666

Izraz „pharming“ prilagođeni je oblik engleske riječi „farming“ – uzgoj na farmi. Riječ je o otmici prave adrese i postavljanju imitacije tražene web-

28

00:04:15,666 --> 00:04:25,266

stranice. U osnovi, „pharming“ se zasniva na preusmjeravanju korisnika na lažna web mjesta koja izgledom podsjećaju ili su identična web

29

00:04:25,266 --> 00:04:29,832

mjestima koja smo u stvari željeli posjetiti.

30

00:04:29,833 --> 00:04:40,433

Neovlašteno traženje informacija prijevarom (pharming) zasniva se na tehnikama kompromitiranja DNS (Domain Name Server)

31

00:04:40,433 --> 00:04:47,566

poslužitelja, i to mijenjanjem njihove priručne memorije (cache) tako da pohranjuje pogrešne IP adrese. Kada korisnik, primjerice, želi posjetiti

32

00:04:47,566 --> 00:04:57,799

web mjesto svoje banke, biva preusmjeren na lažnu stranicu jer će DNS poslužitelj vratiti pogrešnu IP adresu. Stranica koja će se prikazati

33

00:04:57,800 --> 00:05:07,933

nalikovat će na pravu stranicu banke, ali riječ je o imitaciji, lažnoj stranici koja izgleda realno i uvjerljivo, ali kojom upravlja autor prijevare (

34

00:05:07,933 --> 00:05:10,199

pharmer).

35

00:05:10,200 --> 00:05:21,266

Donekle je utješno to što se takva vrsta prijevare događa rjeđe od ostalih (npr. phishing), međutim, alarmantno je što je golem broj nevinih ljudi biva

36

00:05:21,266 --> 00:05:30,632

prevaren i opljačkan iako takvi napadi traju vrlo kratko. Još je strašnija činjenica da tijekom tog procesa web preglednik uredno prikazuje da se

37

00:05:30,633 --> 00:05:40,966

nalazi na ispravnom web mjestu iako je ono lažno. Vrlo je malo toga što pojedinac može poduzeti u obrani od takve prijevare. To je problem koji

38

00:05:40,966 --> 00:05:51,066

rješavaju pružatelji internetskih usluga (ISP) te telekomunikacijske tvrtke i organizacije koje posjeduju DNS opremu na Internetu.

39

00:05:51,066 --> 00:06:02,299

Lekcija je završena.

# Prijevara (hoax)

1

00:00:00,000 --> 00:00:08,700

Dobrodošli. U ovom videu naučit ćemo nešto o

lažnim obavijestima koje se šire Internetom.

2

00:00:08,700 --> 00:00:20,233

„Hoax“ u prijevodu znači prijevara, obmana i to je

upravo ono što jest – lažna obavijest koja se širi

preko e-pošte (spam). Ne sadržava nikakav,

3

00:00:20,233 --> 00:00:28,599

uobičajeno, nikakav zlonamjerni kod i osnovni je

cilj prosljeđivanje poruke što većem broju

korisnika nakon primitka.

4

00:00:28,600 --> 00:00:38,900

Takve se prijevare dijele u dvije osnovne

skupine:lažna obavijest o virusima (virus hoax) i

lančana pisma.

5

00:00:38,900 --> 00:00:49,300

Lažna obavijest o virusima (virus hoax) obično je

e-poruka koja sadržava informacije o nekom

užasnom virusu (fiktivnom) koji se širi velikom

6

00:00:49,300 --> 00:00:58,933

brzinom, inficira goleme količine računala i nijedan

ga zaštitni program zasad ne može otkriti. To su

obavijesti dramatičnih naslova koje većinom

7

00:00:58,933 --> 00:01:07,633

sadržavaju mnoštvo kompliciranih tehničkih izraza

(nerijetko izmišljenih) i pozivaju se na poznata

imena poput IBM-a, Microsofta ili nekih

8

00:01:07,633 --> 00:01:12,199

organizacija koje se bave sigurnošću.

9

00:01:12,200 --> 00:01:21,733

Jednako tako, neke takve prijevare mogu

uzrokovati i konkretnu štetu. U obavijesti o novom

virusu primatelju se detaljno objašnjava način na

10

00:01:21,733 --> 00:01:31,566

koji se sam može riješiti konkretne opasnosti,

poduzimanjem neke radnje koja najčešće uključuje

brisanje neke datoteke uz detaljne upute kako je

11

00:01:31,566 --> 00:01:40,432

pronaći. Korisnici koji nasjednu na takvu zamku mogu ne znajući obrisati neku valjanu sistemsku datoteku što može i ne mora uzrokovati probleme

12

00:01:40,433 --> 00:01:44,699

u radu računala.

13

00:01:44,700 --> 00:01:55,833

Drugu pak skupinu čine lančana pisma (chain letters) ili „pisma sreće“ poznata još od ranije kada su se širila poštom, kao prava pisma. Ta skupina

14

00:01:55,833 --> 00:02:05,866

uključuje sve ostale vrste prijevara koje ne

sadržavaju obavijesti o virusima. Tu su molbe za

novčanu pomoć za bolesne, obitelji otetih i slično,

15

00:02:05,866 --> 00:02:15,799

koje apeliraju na suosjećanje, zatim prilike za

zaradu samo prosljeđivanjem primljene poruke na

što više adresa, prijetnje o gubitku novca ili lošoj

16

00:02:15,800 --> 00:02:26,600

sreći ako se poruka ne proslijedi, lažna obećanja

o darovima, peticije, obavijesti o terorističkim

napadima ili čak obične šale.

17

00:02:26,600 --> 00:02:38,100

Većina ljudi koja se služi elektroničkom poštom

navikla je na primanje spama i ovakvih obavijesti

pa ih je prilično lako otkriti. Dovoljno je promotriti

18

00:02:38,100 --> 00:02:50,666

naslov te nepredviđene i neželje e-poruke koji

obično dramatično ističe opasnost, nešto važno,

nešto besplatno ili neku zaradu da bismo

19

00:02:50,666 --> 00:03:00,732

znali da je riječ o prijevari i da takve poruke ne

treba niti otvarati. Jednako tako, većina spam

filtara (antispam) danas relativno dobro

20

00:03:00,733 --> 00:03:02,899

prepoznaje takve poruke i rješava ih se.

21

00:03:02,900 --> 00:03:09,900

Lekcija je završena.

# Spam

1

00:00:00,000 --> 00:00:09,400

Dobrodošli. U ovoj lekciji ćemo naučiti što je to

SPAM i koje su opasnosti vezane uz njega.

2

00:00:09,400 --> 00:00:20,100

Spam se najčešće kratko definira kao neželjena

elektronička pošta koja se masovno šalje velikoj

količini korisnika, nešto nalik na velike količine

3

00:00:20,100 --> 00:00:26,900

reklamnih letaka koje vidimo svaki dan utrpane u

naše poštanske sandučiće.

4

00:00:26,900 --> 00:00:35,900

Ljudi koji šire spam – spammeri koriste se raznim

načinima pribavljanja e-adresa.

5

00:00:35,900 --> 00:00:48,433

Najvažnija je valjanost adresa, a ugledniji izvor na

neki način samim imenom jamči valjane adrese,

zato je i cijena veća. Oni koji ne kupuju e-adrese

6

00:00:48,433 --> 00:00:59,999

na takve načine koriste se raznim programima za

ekstrakciju adresa i sastavljaju vlastite liste. Rabe

programe koji izvlače e-adrese s raznih foruma i

7

00:01:00,000 --> 00:01:09,000

obavijesnih skupina (newsgroup).Nakon što sakupe određenu količinu adresa,

počinju slati spam na njih. Koriste se raznim

8

00:01:09,000 --> 00:01:18,766

metodama, kao što je otvaranje privremenih

korisničkih računa kod raznih pružatelja usluga s

kojih masovno šalju beskorisnu elektroničku poštu

9

00:01:18,766 --> 00:01:22,699

i zatim ih zatvaraju prije nego što ih netko uhvati.

10

00:01:22,700 --> 00:01:34,366

U spam porukama također se često na kraju

nalazi poveznica (link) na koju treba kliknuti da bi

korisnik navodno bio skinut s liste za slanje

11

00:01:34,366 --> 00:01:43,466

(mailing list). Klikom na takvu poveznicu u svakom

ste slučaju spammeru potvrdili da je poruka

primljena i da je vaša e-adresa valjana. S tom vam

12

00:01:43,466 --> 00:01:54,599

potvrdom može nastaviti slati spam ili vašu adresu

prodati drugim spammerima. Ili se, u najgorem

slučaju, klikom može inicirati preuzimanje ili

13

00:01:54,600 --> 00:01:58,433

instalacija nekoga zlonamjernog programa.

14

00:01:58,433 --> 00:02:10,199

Spam je problem na koji treba obratiti posebnu

pozornost. To je pojam koji u sebi na neki način

spaja gotovo sve ostale nametnike koji vrebaju

15

00:02:10,200 --> 00:02:21,800

Internetom – od zlonamjernog koda (virusi, crvi,

trojanski konji, špijunski programi) koji se skriva u

privitcima, zatim prijevara (hoax) koje obično

16

00:02:21,800 --> 00:02:32,233

dolaze u obliku e-poruke pa do neovlaštenog

traženja informacija (phishing) i zavaravanja

(spoofing) koji su usko povezani sa spamom

17

00:02:32,233 --> 00:02:38,099

(zavaravanje poveznicama, web-zavaravanje, e-

mail zavaravanje...). Spam integrira sve oblike zlonamjernog koda i

18

00:02:38,100 --> 00:02:43,066

socijalnog inženjeringa u jedan sveobuhvatan

problem za koji za sada nema kvalitetnog rješenja.

19

00:02:43,066 --> 00:02:47,099

Lekcija je završena.

# E-mail zavaravanje (e-mail spoofing) i Web-zavaravanje (web-spoffing)

1

00:00:00,000 --> 00:00:07,733

Dobrodošli. U ovom videu učiti ćemo o zavaravanju na Internetu.

2

00:00:07,733 --> 00:00:17,333

Postoje dva glavna načina zavaravanja ljudi

tijekom boravka na Internetu, pa tako razlikujemo

zavaravanje elektroničkim porukama i Web-

3

00:00:17,333 --> 00:00:20,899

zavaravanje.

4

00:00:20,900 --> 00:00:31,800

Kod zavaravanja e-porukama posrijedi je tehnika

krivotvorenja informacija u zaglavlju elektroničke

poruke tako da se čini kao da stiže s nekog

5

00:00:31,800 --> 00:00:45,400

drugog odredišta, najčešće, nekog korisniku

poznatog. Protokol koji se rabi za e-poruke, SMTP

(Simple Mail Transfer Protocol), ne obuhvaća

6

00:00:45,400 --> 00:00:57,166

nikakvu autentikaciju za provjeru izvorišta odnosno

pošiljatelja. Zamjenom adrese pošiljatelja, e-

poruka naizgled stiže od nekog drugog, nekog tko

7

00:00:57,166 --> 00:01:05,866

je nije poslao i, bez implementacije nekih

sigurnosnih mjera, gotovo je nemoguće utvrditi

pravog pošiljatelja. Tehnikom elektroničkog

8

00:01:05,866 --> 00:01:17,632

zavaravanja najčešće se koriste autori virusa.

Širenje virusa preko e-pošte uz krivotvorenje

adrese pošiljatelja korisnicima koji prime virus, u

9

00:01:17,633 --> 00:01:21,066

mnogome, otežava pronalazak izvora.

10

00:01:21,066 --> 00:01:31,932

Kod web-zavaravanje riječ je o tehnici prikrivanja

web-adresa presretanjem zahtjeva za pregled

nekog web-mjesta i zatim preusmjeravanjem na

11

00:01:31,933 --> 00:01:41,699

neku drugu web-adresu. Na toj se adresi može

nalaziti lažno, nepostojeće web-mjesto koje

izgleda legitimno ili web-mjesto koje „glumi“ neko

12

00:01:41,700 --> 00:01:49,766

već postojeće. Takva lažna web-mjesta koja imitiraju neka već

poznata, najčešće imaju adrese (URL) vrlo slične

13

00:01:49,766 --> 00:01:56,799

onima koje predstavljaju (npr. www.micrsoft.com)

pa žrtve misle da doista pristupaju tim stranicama.

14

00:01:56,800 --> 00:02:06,833

Web-zavaravanje najčešće se koristi za

zloupotrebu stranica koje pružaju neke usluge kao

što je internetska kupnja, odnosno stranice koje

15

00:02:06,833 --> 00:02:18,099

traže unošenje nekih osobnih podataka, kao

brojeve kreditnih kartica ili podatke o korisničkim

računima, koji se na taj način kradu. Primjer

16

00:02:18,100 --> 00:02:28,400

zavaravanja su i web-mjesta koja nude različite

optimizacije računala s tekstovima oglasa koji

nalikuju na „Vaše je računalo sporo? Web-stranice

17

00:02:28,400 --> 00:02:33,866

se otvaraju sporo? itd.

18

00:02:33,866 --> 00:02:40,699

Lekcija je završena.

# Važnost ne otkrivanja povjerljivih informacija na društvenim mrežama

1

00:00:00,000 --> 00:00:10,800

Dobrodošli. U ovom videu naučit ćemo zašto je bitno ne otkrivati povjerljive, osobne informacije na društvenim mrežama.

2

00:00:10,800 --> 00:00:21,400

Čovjek je društveno biće. U trenucima sve većihotuđenja sasvim je razumljiva činjenica da ljudiimaju potrebu biti prisutni na društvenim mrežama.

3

00:00:21,400 --> 00:00:27,833

Jedna od najpopularnijih društvenih mrežatrenutačno je Facebook, s više od pola milijardekorisnika.

4

00:00:27,833 --> 00:00:37,633

Pri podjeli informacija moramo biti svjesni drugihljudi „oko sebe“ te vrlo oprezno voditi brigu oinformacijama koje želimo podijeliti s drugima.

5

00:00:37,633 --> 00:00:48,599

Ono o čemu treba voditi brigu jest da dioinformacija koje ostavljamo na nekoj od mrežazlonamjerni ljudi mogu vrlo lako iskoristiti i

6

00:00:48,600 --> 00:00:59,133

time: uzrokovati štetu za ugled osobe; dovesti dozastrašivanja (cyber-bullying) pa i ucjenjivanja;dovesti do krađe identiteta uz pomoć prikupljenih

7

00:00:59,133 --> 00:01:06,299

informacija, dovesti do lažnog predstavljanja teuhođenja.

8

00:01:06,300 --> 00:01:19,800

No, ipak je glavna namjera nanošenje financijskeštete, a uglavnom se izvodi prikupljanjem odnosnoobradom povjerljivih podataka. Između ostalog, ti

9

00:01:19,800 --> 00:01:29,833

podaci mogu izravno ili neizravno dovesti i dokrađe identiteta. Obično je pritom riječ o stjecanjuinformacija o bankarskim transakcijama i sl.

10

00:01:29,833 --> 00:01:40,533

Podaci poput adrese stanovanja i statusa oodlascima na godišnji mogu dovesti do provale isl. Kontaktne se informacije, obvezno, ne bi

11

00:01:40,533 --> 00:01:49,766

trebale ostavljati s obzirom na to da ih zlonamjerneosobe i štetni softver poput trojanskog konja moguzloupotrijebiti.

12

00:01:49,766 --> 00:01:58,732

U velikoj mjeri sami možemo kontrolirati privatnost svojih podataka s pomoću postavki kojima se koristimo.

13

00:01:58,733 --> 00:02:07,733

Pravila privatnosti koje definira Facebook, pa i druge mreže, određuju da su ime, prezime i fotografija uz profil (engl. Profile picture) uvijek

14

00:02:07,733 --> 00:02:16,666

javno dostupni. Jednako je tako trećim stranama zabranjeno koristiti se prikupljenim podacima u neku njihovu svrhu.

15

00:02:16,666 --> 00:02:24,199

Iako su u posljednje vrijeme uvedena mnoga poboljšanja i dodaci namijenjeni očuvanju privatnosti, Facebook teško može imati potpunu

16

00:02:24,200 --> 00:02:34,600

kontrolu nad svojim podacima, stoga je na nama da kroz postavke privatnosti na bilo kojoj društvenoj mreži, pažljivo definiramo što želimo da

17

00:02:34,600 --> 00:02:37,666

se prikazuje, a što ne.

18

00:02:37,666 --> 00:02:47,732

Ono na što moramo paziti je i tzv. iskopavanje informacija. Na primjer, na Facebooku je poznat alat „Graph Search“ čija je inicijalna namjena

19

00:02:47,733 --> 00:02:57,499

„Pronalaženje novih prijatelja i starog sadržaja“. Ono o čemu trebamo voditi računa je upravo taj stari sadržaj koji nam jednoga dana kada bude

20

00:02:57,500 --> 00:03:08,166

iskopan može nanijeti popriličnu štetu, a uz odgovarajuće postavke privatnosti možemo ga kontrolirati i spriječiti.

21

00:03:08,166 --> 00:03:20,366

Također, vodite brigu o tzv. povezanim profilima sobzirom na činjenicu da više od 51% korisnikaInterneta posjeduje više profila na različitim

22

00:03:20,366 --> 00:03:22,766

mrežama.

23

00:03:22,766 --> 00:03:30,799

Primjer situacije koju ne bismo željelijest da na našem Facebook profilu objavimo nešto„šaljivo“. Kako nam je Facebook profil povezan s

24

00:03:30,800 --> 00:03:40,900

našim Linkedin (profesionalna društvena mreža)profilom, ovakva bi nam situacija mogla zadatidosta glavobolje. Primjerice, rukovoditelj nam je

25

00:03:40,900 --> 00:03:50,800

prijatelj na LinkedIn profilu, ali ne i na Facebookute je tako neizravno saznao „zanimljive“ detalje iznašega privatnog života.

26

00:03:50,800 --> 00:04:03,433

Na društvenim mrežama, nikako ne objavljujte:aluzije na lozinke i lozinke, financijske podatke,adresu i telefonski broj, fotografije djece, nikakvu

27

00:04:03,433 --> 00:04:12,333

poslovnu informaciju, društvene planove (ako jeriječ o društvenoj mreži) te osobne razgovore (zato postoje drugačiji načini komunikacije).

28

00:04:12,333 --> 00:04:20,899

Iako nije direktno povezano s društvenim mrežama, kada govorimo o bankarskim transakcijama, posebno treba biti oprezan kod

29

00:04:20,900 --> 00:04:29,333

situacija neovlaštenog kopiranja (skimming). Podefiniciji je skimming proces kopiranja kreditneodnosno bilo koje platne kartice i korištenja

30

00:04:29,333 --> 00:04:39,099

duplikata, a bez znanja samog korisnika.Odnosno, kada korisnik sazna da mu je karticakopirana, već je uglavnom kasno. Oprezan treba

31

00:04:39,100 --> 00:04:48,400

biti, uglavnom prilikom podizanja novca nabankomatima, kada sam bankomat moženeovlašteno biti prerađen da kopiju kartice šalje

32

00:04:48,400 --> 00:04:50,200

kriminalcima.

33

00:04:50,200 --> 00:04:57,500

No, bez obzira što je danas najčešćioblik kopiranja platnih kartica onaj nabankomatima, posebno moramo biti oprezni kod

34

00:04:57,500 --> 00:05:02,366

bilo kakvog plaćanja putem Interneta.

35

00:05:02,366 --> 00:05:14,732

Uz društvene mreže, često se veže i pojam njege(Grooming). Njegovanje odnosno njega se koristiza opisivanje ljudi i njihovih postupaka kada žele

36

00:05:14,733 --> 00:05:24,299

seksualno naškoditi djeci i mladima i to na načinda im se putem Interneta pokušavaju približiti tezadobiti njihovo povjerenje.

37

00:05:24,300 --> 00:05:34,533

U stvarnom svijetu, na takve osobe možemo naići u školama, susjedstvu, sportskim klubovima…U online svijetu, takva osoba kroz njegu

38

00:05:34,533 --> 00:05:39,299

(njegovanje) pokušava uspostaviti odnos s djecom ili mladima pretvarajući se da im je prijatelj.

39

00:05:39,300 --> 00:05:48,500

Pokušaje približavanja i stjecanja povjerenja grade na informacijama koje su o djeci saznali putem društvenih mreža. Kada skupe dovoljno

40

00:05:48,500 --> 00:05:56,733

informacija o određenoj mladoj osobi,pokušat će joj se „približiti“. Obično započinju razgovore s djecom na način da pokušavaju

41

00:05:56,733 --> 00:06:08,266

pogoditi teme koje su djeci interesantne, a čestodaju lažne fizičke opise i navode krive godine. Nemali je broj slučajeva i da šalju lažne fotografije,

42

00:06:08,266 --> 00:06:17,266

uglavnom višestruko mlađih osoba predstavljajućise da su to oni. S obzirom da je u današnjevrijeme kada se ljudi polagano otuđuju, daleko

43

00:06:17,266 --> 00:06:26,132

lakše uspostaviti odnos povjerenja u virtualnomsvijetu nego „oči u oči“, višestruko iskorištavajutakve načine ponašanja maloljetnika.

44

00:06:26,133 --> 00:06:36,166

Da bi zaštitili svoju djecu, potrebno se držatijednostavnog pravila, SMART, koji će biti opisan u nastavku:

45

00:06:36,166 --> 00:06:46,966

S – SAFE (Sigurnost): Neka djeca čuvaju svojusigurnost ne dajući svoje osobne podatke ikomena Internetu.

46

00:06:46,966 --> 00:06:57,399

M – MEETING (Sastanak): Neka djeca budu svjesna činjenice da nalaženje u stvarnom svijetu s osobom iz online svijeta nosi potencijalne

47

00:06:57,400 --> 00:06:59,433

opasnosti.

48

00:06:59,433 --> 00:07:11,299

A – ACCEPTING (Prihvaćanje): Neka djeca budusvjesna da primanje elektroničkih poruka,istovremenih poruka i sl od osoba koje ne poznaju

49

00:07:11,300 --> 00:07:18,833

može biti opasno. Poruke mogu sadržavati viruse ili biti neprimjerenog sadržaja.

50

00:07:18,833 --> 00:07:30,299

R – RELIABLE (Pouzdano): Neka djeca budusvjesna činjenice da im na Internetu netko moželagati o sebi te da informacije koje nađu o toj

51

00:07:30,300 --> 00:07:34,800

osobi, također, na Internetu ne moraju biti točne.

52

00:07:34,800 --> 00:07:47,033

T – TELL (Izreći): Djeca moraju imati povjerenja usvoje roditelje odnosno skrbnike i moraju im semoći obratiti ukoliko se zbog bilo kojeg događaja

53

00:07:47,033 --> 00:07:53,699

koji se dogodio u online svijetu osjećaju neugodnoili zabrinuto.

54

00:07:53,700 --> 00:07:57,166

Lekcija je završena.