# E-pošta

1

00:00:00,000 --> 00:00:11,066

Dobrodošli. U ovom videu proći ćemo osnovne

sigurnosne naputke koji se odnose na

komunikaciju elektroničkom poštom.

2

00:00:11,066 --> 00:00:21,299

Slanje i primanje elektroničke pošte jedna je od

najčešćih radnji koje se izvode na računalu. Zbog

mogućnosti dostavljanja poruka gotovo odmah,

3

00:00:21,300 --> 00:00:30,233

bilo gdje na svijetu, elektronička pošta pruža

brzinu i učinkovitost s kojom se klasična

poštanska usluga ne može niti mjeriti. No jednako

4

00:00:30,233 --> 00:00:40,433

učinkovito kako dostavlja legitimne poruke, tako je

efikasna i u distribuiranju zlonamjernih programa i

neželjenih spam poruka.

5

00:00:40,433 --> 00:00:51,466

Danas je e-pošta primarno sredstvo poslovne i

privatne komunikacije za milijune ljudi. Milijarde

poruka dnevno šalju se preko Interneta. Danas,

6

00:00:51,466 --> 00:01:02,299

prema statistikama oko 70 – 80 % od čitave

elektroničke pošte koja se razmjenjuje čine

neželjene komercijalne poruke, odnosno spam, a

7

00:01:02,300 --> 00:01:12,566

jedna od 36 sadržava neki oblik štetnog koda. Po

pitanju neželjene pošte, to možda i nije toliko

različito od standardnog poštanskog sandučića.

8

00:01:12,566 --> 00:01:23,066

Većina klasične pošte koju danas primamo sastoji

se od kataloga, oglasa i reklama. No sadržaj

elektroničke pošte može biti mnogo štetniji za nas

9

00:01:23,066 --> 00:01:28,999

od reklamnih kataloga koji zatrpavaju naše

sandučiće.

10

00:01:29,000 --> 00:01:40,400

Privici e-poruka mnogim su korisnicima velika

prednost, vrlo su korisna mogućnost brze i

jednostavne razmjene privatnih i poslovnih

11

00:01:40,400 --> 00:01:51,966

informacija, slika, programa i drugih datoteka. Ali

jednako se tako kod većine štetnih poruka onaj

zlonamjerni dio nalazi unutar privitka. Raznim

12

00:01:51,966 --> 00:02:03,199

tehnikama socijalnog inženjeringa, korisnika se

tekstom u tijelu e-poruke pokušava nagovoriti,

uvjeriti da otvori privitak i pokrene datoteku te time

13

00:02:03,200 --> 00:02:13,633

inficira računalo. Osim uvjerljivog nagovora,

uskoro su uslijedile i druge tehnike zavaravanja pa

se elektroničke poruke maskiraju tako da korisnik

14

00:02:13,633 --> 00:02:24,133

misli da stižu od njemu poznate osobe. Veća je

vjerojatnost da će korisnik otvoriti poruku od

nekog rođaka ili radnog kolege pa počinje

15

00:02:24,133 --> 00:02:34,933

stvaranje virusa i zlonamjernih programa koji sami

sebe šalju na sve adrese iz adresara e-mail

klijenta na zaraženom računalu. Stoga je potrebno

16

00:02:34,933 --> 00:02:44,933

imati na umu da bi čak i e-poruka s poznate

adrese mogla biti sumnjiva te da opreza nikad

dosta, pogotovo s obzirom na činjenicu da je u

17

00:02:44,933 --> 00:02:55,833

nekim situacijama dovoljno i samo otvoriti e-

poruku da bi se računalo inficiralo, dakle,

opasnosti se ne kriju samo u privicima.

18

00:02:55,833 --> 00:03:06,866

Budući da je danas većina korisnika svjesna da je

velika vjerojatnost da se u privitku koji sadržava

neku izvršnu datoteku skriva štetni program, stekli

19

00:03:06,866 --> 00:03:17,566

su naviku ne otvarati takve privitke, osim ako

točno znaju o čemu je riječ ili očekuju primitak

takve datoteke. No, zlonamjerni se programi često

20

00:03:17,566 --> 00:03:26,366

maskiraju tako da im se maskira ekstenzija,

odnosno stavlja se dvostruka ekstenzija.

21

00:03:26,366 --> 00:03:37,599

Većina e-mail klijenata danas nudi mogućnost

filtriranja e-poruka po raznim pravilima, što je vrlo

korisno. No kako liste blokiranih vrsta datoteka

22

00:03:37,600 --> 00:03:48,333

rastu, pisci štetnih programa pronalaze nove vrste

izvršnih datoteka i nove načine skrivanja. U

svakom bi slučaju privitke trebalo otvarati samo

23

00:03:48,333 --> 00:03:58,599

ako korisnik potpuno vjeruje pošiljatelju i upoznat

je s onim što se nalazi u privitku te ako je potpuno

siguran da konkretna e-poruka stiže upravo s

24

00:03:58,600 --> 00:04:12,266

adrese s koje piše da stiže. U protivnom, privitke

e-poruka s nepoznatih adresa ili privitke sumnjivim

e-porukama nipošto ne bi trebalo otvarati. Što se

25

00:04:12,266 --> 00:04:22,532

tiče spama, ni na kakve spam e-poruke ne bi

trebalo odgovarati te ih zapravo ne bi trebalo niti

otvarati. Takve poruke obično imaju naslove koji

26

00:04:22,533 --> 00:04:32,499

odmah naznačuju da je riječ o spamu te bi ih

trebalo odmah izbrisati jer nikad ne možemo znati

nalaze li se u njima samo iritantna reklama ili neka

27

00:04:32,500 --> 00:04:46,500

prijevara i štetni programi. Jednako tako, vlastitu

e-adresu nikad ne bi trebalo objavljivati na web-

stranicama ili ih unositi u razne web-formulare.

28

00:04:46,500 --> 00:04:59,400

Korištenje e-mail klijentom, koji zapravo služi kao

posrednik između e-mail poslužitelja i korisnika,

omogućuje razne pogodnosti i sigurnosne mjere

29

00:04:59,400 --> 00:05:08,466

koje takvi programi pružaju. Jedan od

najkorištenijih programa za elektroničku poštu jest

Microsoft Outlook.

30

00:05:08,466 --> 00:05:20,732

Web e-mail sustavi kao što su Hotmail, Yahoo!

mail i slični pružaju pogodnost pristupanja e-mail

sandučićima i slanje i primanje elektroničke pošte

31

00:05:20,733 --> 00:05:27,466

na bilo kojem računalu koje je povezano s

Internetom. U slučaju odabira web e-mail usluge, najbolje je

32

00:05:27,466 --> 00:05:37,899

odabrati pružatelje usluga koji nude i razne

sigurnosne opcije, kao što su skeniranje privitaka

programima za otkrivanje virusa, spam filtriranje,

33

00:05:37,900 --> 00:05:46,766

mogućnost šifriranja e-poruka i pristup e-mail

računu preko sigurne veze (SSL). Pri odabiru besplatnih pružatelja elektroničke

34

00:05:46,766 --> 00:05:58,499

pošte nije na odmet provjeriti obavljaju li tzv.

kontekstualno pretraživanje. Naime, da bi mogli

platiti sve troškove davanja usluge besplatne

35

00:05:58,500 --> 00:06:08,800

elektroničke pošte, najčešće rabe sadržaj e-

poruka za prikaz oglasa te time kompenziraju

financijsku stranu priče, ali na taj način

36

00:06:08,800 --> 00:06:20,133

kompromitiraju našu privatnost.Pri pristupanju web sandučiću s nekoga javnog

računala također treba paziti da se privatni podaci

37

00:06:20,133 --> 00:06:27,933

ne spremaju na računalu (u priručnoj memoriji,

cache)

38

00:06:27,933 --> 00:06:40,766

Otvaranjem priloga koji sadržavaju makronaredbe ili izvršne datoteke izlažemo se opasnosti od inficiranja našeg računala.

39

00:06:40,766 --> 00:06:47,599

Lekcija je završena.

# Razumijevanje svrhe šifriranja, dešifriranja e-pošte i digitalnog potpisa

1

00:00:00,000 --> 00:00:08,833

Dobrodošli. Nakon ovog videa razumjet ćemo svrhu šifriranja elektroničke pošte.

2

00:00:08,833 --> 00:00:20,666

Šifriranje e-poruke u programu Microsoft Outlook štiti povjerljivost poruke tako da se pretvara iz običnog teksta u šifrirani. Osnovni princip šifriranja

3

00:00:20,666 --> 00:00:30,966

je kroz Cezarov kod objašnjen u poglavlju o Mjerama zaštite. Samo primatelj poruke koji ima privatni ključ koji odgovara javnom ključu,

4

00:00:30,966 --> 00:00:41,966

korištenom za šifriranje može dešifrirati poruku te ju potom pročitati. Svi ostali primatelji koji nemaju odgovarajući privatni ključ vide besmisleni tekst.

5

00:00:41,966 --> 00:00:56,466

Dakle, šifriranje jednoznačno možemo opisati kao akciju čija je namjera osigurati da jedino osoba kojoj je elektronička poruka namijenjena može tu

6

00:00:56,466 --> 00:00:59,566

poruku i pročitati.

7

00:00:59,566 --> 00:01:10,332

Digitalni potpis označuje matematičku shemu koja omogućuje provjeru autentičnosti poruke ili dokumenta. Na ovaj se način može sa sigurnošću

8

00:01:10,333 --> 00:01:20,499

provjeriti i potvrditi autor poruke, i to s većom sigurnošću nego što je to slučaj u normalnom svijetu, gdje se autentičnost poruke obično

9

00:01:20,500 --> 00:01:30,733

provjerava običnim potpisom. Razlog ovome jesu obilježja digitalnog potpisa koja osiguravaju nemogućnost krivotvorenja digitalnog potpisa

10

00:01:30,733 --> 00:01:34,466

primjenom današnjih tehnologija.

11

00:01:34,466 --> 00:01:46,132

Da biste kreirali vlastiti digitalni potpis, morate imati certifikat za potpisivanje koji dokazuje vaš identitet. Prilikom slanja digitalno potpisane

12

00:01:46,133 --> 00:01:57,666

elektroničke poruke ili dokumenta šaljete i svoj certifikat te javni ključ. Certifikate izdaje ustanova za izdavanje certifikata, a moguće ih je opozvati.

13

00:01:57,666 --> 00:02:08,832

Valjanost certifikata najčešće traje godinu dana, te ga nakon isteka valjanosti potpisnik mora obnoviti ili pribaviti novi certifikat za potpisivanje, a da bi

14

00:02:08,833 --> 00:02:17,933

potvrdio svoj identitet.Da bi naručili svoj certifikat, morate se obratiti ustanovi za izdavanje certifikata. Kod nas tu ulogu

15

00:02:17,933 --> 00:02:28,899

izdavatelja certifikata ima Financijska agencija. Ona izdaje digitalne certifikate, potpisuje certifikate da bi se potvrdila njihova valjanost te

16

00:02:28,900 --> 00:02:35,633

bilježi opozvane certifikate i one čija je valjanost istekla.

17

00:02:35,633 --> 00:02:44,099

Lekcija je završena.

# Istovremene poruke

1

00:00:00,000 --> 00:00:11,200

Dobrodošli. U ovom videu naučit ćemo što su to aplikacije za razmjenjivanje istovremenih poruka te koje nas opasnosti vrebaju dok ih koristimo.

2

00:00:11,200 --> 00:00:19,733

Korištenje izravnom porukom način jekomuniciranja s drugim korisnicima na LAN iliWAN mreži, i to u realnom vremenu.

3

00:00:19,733 --> 00:00:29,066

Riječ je o zbirci komunikacijskih tehnologija koje se koriste tekstualno/audio/vizualnom komunikacijom između dvoje ili više sudionika.

4

00:00:29,066 --> 00:00:38,232

U naravi, trenutna razmjena poruka jekomunikacijski servis na Internetu koji omogućavakorisnicima razmjenu poruka u stvarnom vremenu.

5

00:00:38,233 --> 00:00:48,199

To je vrsta komunikacijskog servisa putem kojegkorisnici mogu stvoriti privatnu „sobu“ za čavrljanje(chat room) u kojoj s nekom drugom osobom ili

6

00:00:48,200 --> 00:00:54,533

više njih mogu komunicirati u stvarnom vremenu,kao u razgovoru putem telefona.

7

00:00:54,533 --> 00:01:00,966

Primjeri programa za istodobne poruke: Skype,Google Talk, ICQ.

8

00:01:00,966 --> 00:01:08,099

Danas većina sustava za istovremene poruke postoji i za mobilne uređaje.

9

00:01:08,100 --> 00:01:16,200

Iako je riječ o komunikaciji koja je vrlo brza iefikasna, ona sa sobom nosi i određenesigurnosne rizike s obzirom na to da ranije

10

00:01:16,200 --> 00:01:25,466

spomenuti „Black Hat hakeri“ stalno rabe mrežuistovremenih poruka te elektroničkih poruka (e-mail) za phishing pokušaje u želji da se dokopaju

11

00:01:25,466 --> 00:01:30,766

korisničkog imena, lozinke, podataka o kreditnimkarticama i sl.

12

00:01:30,766 --> 00:01:40,032

Hakeri primjenjuju dvije metode kako bi isporučili zlonamjerni kod. Jedna od njih jest pokušaj zaraze računala virusima, trojanskim konjima ili

13

00:01:40,033 --> 00:01:43,199

špijunskim programima preko zaraženih datoteka.

14

00:01:43,200 --> 00:01:53,166

Drugi način, također koristeći se socijalniminženjeringom, jesu pokušaji slanja određenogteksta koji sadržava putanju k web-mjestu sa

15

00:01:53,166 --> 00:01:57,266

štetnim kodom putem sustava za istovremen poruke.

16

00:01:57,266 --> 00:02:07,099

Za korištenje programom za istovremene porukevrijede ista pravila kao i za bilo koju prisutnost nadruštvenim mrežama, a isključivo se zabranjuje

17

00:02:07,100 --> 00:02:16,566

odavanje lozinki ili bilo kojih osobnih podataka. Također je vrlo bitno ograničiti dijeljenje datoteka komunicirajući istodobnim porukama.

18

00:02:16,566 --> 00:02:25,366

S obzirom na mogućnost dijeljenja datoteka,posebno ih oprezno treba prihvaćati, a pogotovood nepoznatih činitelja, kako računalo ne bismo

19

00:02:25,366 --> 00:02:29,799

inficirali nekim zlonamjernim kodom.

20

00:02:29,800 --> 00:02:57,866

Lekcija je završena.