CYBER SECURITY

osnovni pojmovi

ŠTO JE SIGURNOST?

"Kvaliteta ili stanje sigurnosti - biti bez opasnosti"

Uspješna organizacija treba imati voditi računa o više razina sigurnosti:

- **Fizičko osiguranje**
- **Osobna sigurnost**
- **Osiguranje sigurnosti**
- **Sigurnost komunikacija**
- **Sigurnost mreže**
- **Sigurnost informacija**

Cyber security

znači biti slobodan od opasnosti ili štete uzrokovane prekidom, ometanjem ili padom informatičk o-komunikacijskih tehnologija (ICT) ili zlouporabom ICT-a

Cyber sigurnost

Skup alata, politika, sigurnosnih koncepata, sigurnosnih mjera, smjernica, pristupa upravljanju rizicima, radnji, obuke, najboljih praksi, osiguranja i tehnologija koje se mogu koristiti za zaštitu cyber okruženja i organizacije i imovine korisnika.

Organizacijska i korisnička imovina uključuju povezane računalne uređaje, osoblje, infrastrukturu, aplikacije, usluge, telekomunikacijske sustave i cjelokupnost prenesenih i / ili pohranjenih podataka u cyber okruženju.

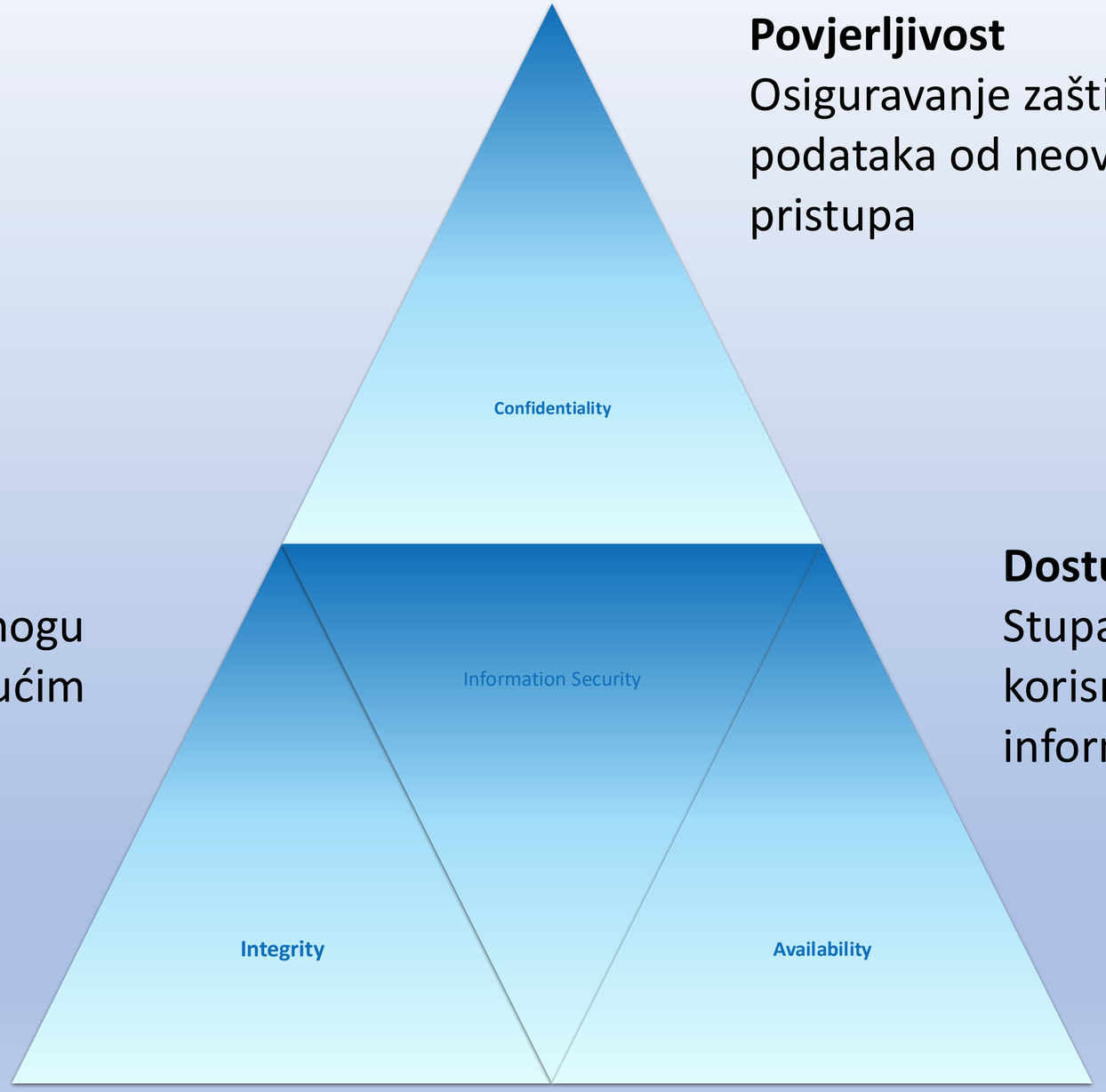
Cyber security nastoji osigurati ostvarenje i održavanje sigurnosnih svojstava organizacije i imovine korisnika protiv relevantnih sigurnosnih rizika u cyber okruženju.

PODRUČJA INFORMACIJSKE SIGURNOSTI

- Sigurnost aplikacija
- Kontrola pristupa
- Nastavak poslovanja i planiranje oporavka od katastrofe
- Kriptografija
- Sigurnost operacija
- Fizička sigurnost
- Telekomunikacije i mrežna sigurnost
- Informacijska sigurnost i upravljanje rizicima
- Pravo, regulativa, usklađenost i istrage
- Sigurnosna arhitektura i dizajn

CIA trijada

Povjerljivost
Osiguravanje zaštite podataka od neovlaštenog pristupa



Integritet
Osiguranje da se podaci mogu mijenjati samo odgovarajućim mehanizmima

Dostupnost
Stupanj do kojeg ovlašteni korisnici mogu pristupiti informacijama u legitimne svrhe

ULOGA INFORMACIJSKE SIGURNOSTI

Uloga informacijske sigurnosti je zaštita informacijske imovine

- Kako postići informacijsku sigurnost?
- Politika
- Tehnologija
- Programi osposobljavanja i osvješćivanja

DIGITAL LIFE

FIZIČKI IDENTITET

S nama nosimo svoj osobni, fizički identitet kamo god idemo. To uključuje informacije kao što su visina i težina, boja očiju, spol, ton kože, itd. Neke od tih detalja možemo promijeniti, ali u cjelini naš fizički identitet je ono što svatko od nas naziva "ja".

DIGITALNI IDENTITET

Digitalni identitet je informacija o entitetu koju računalni sustavi koriste za predstavljanje vanjskog agenta. Taj agent može biti osoba, organizacija, aplikacija ili uređaj.

KARAKTERISTIKE DIGITALNOG IDENTITETA

- proteže se izvan fizičkih značajki
- omiljena hrana, vrsta automobila koji vozite, trenutna adresa pošte
- korisnička imena i zaporke za sve vaše online račune,
- povijest pretraživanja,
- postove društvenih medija,
- digitalne fotografije,
- skenirane slike putovnice
- digitalni identiteti lako se iskorištavaju i vrlo su profitabilni.
- cijela je industrija izrasla s jedinom svrhom da smislimo tragove podataka koje ostavljamo na mreži
- sve ove informacije zauvijek su povezane s našim internetskim identitetom, a nemamo pravo glasa što će se dogoditi s tim podacima nakon što odu iz naše ruke.

GDPR

UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA

od 27. travnja 2016.

o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)

Zašto GDPR?

Zaštita pojedinaca s obzirom na obradu osobnih podataka temeljno je pravo.

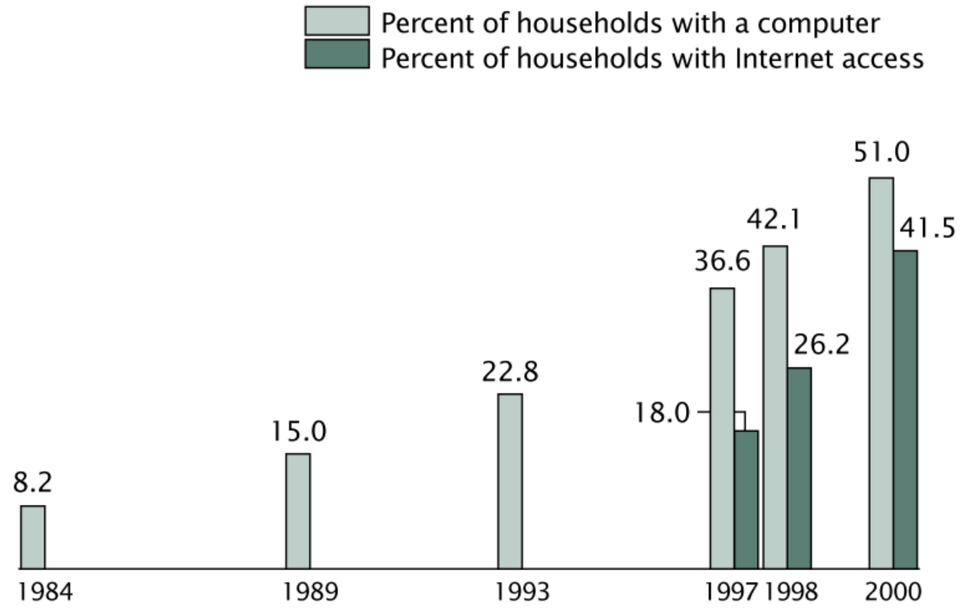
Člankom 8. stavkom 1. Povelje Europske unije o temeljnim pravima („Povelja”) te člankom 16. stavkom 1. Ugovora o funkcioniranju Europske unije (UFEU) utvrđuje se da *svatko ima pravo na zaštitu svojih osobnih podataka*.

Zašto GDPR?

Figure 1.

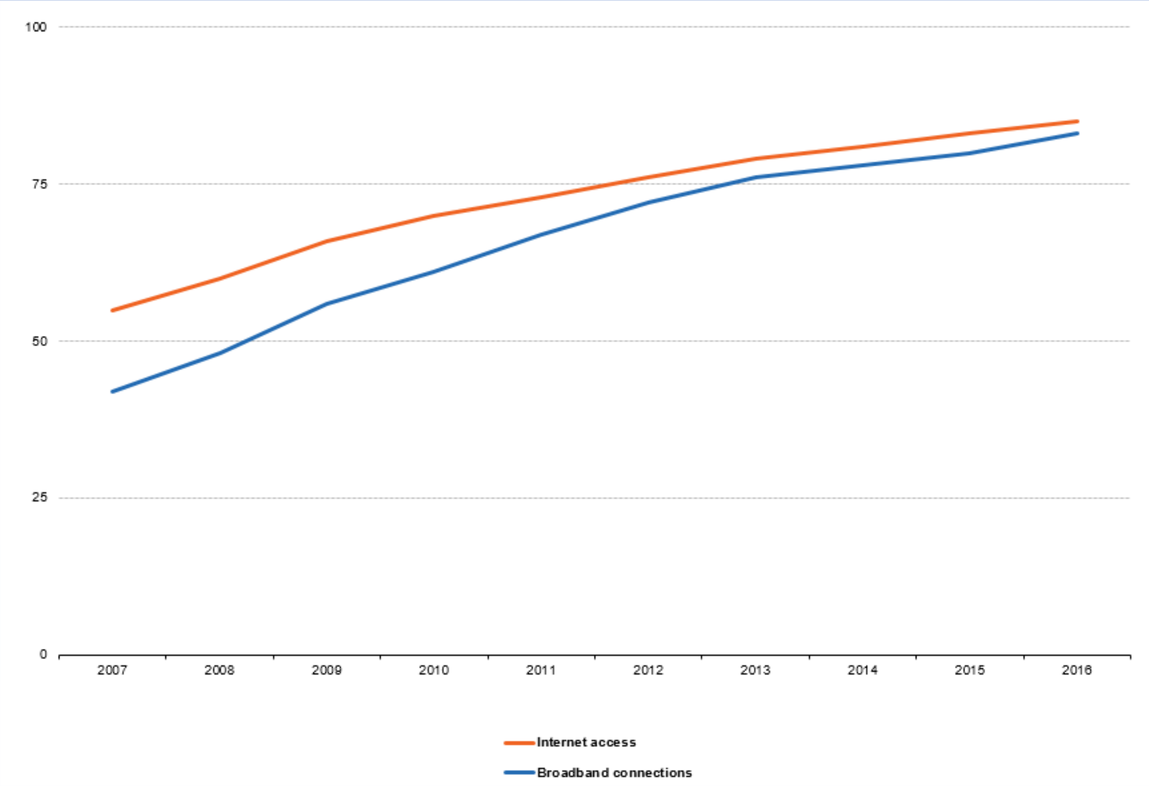
Computers and Internet Access in the Home: 1984 to 2000

(Civilian noninstitutional population)



Note: Data on Internet access were not collected before 1997.
Source: U.S. Census Bureau, Current Population Survey, various years.

Zašto GDPR?



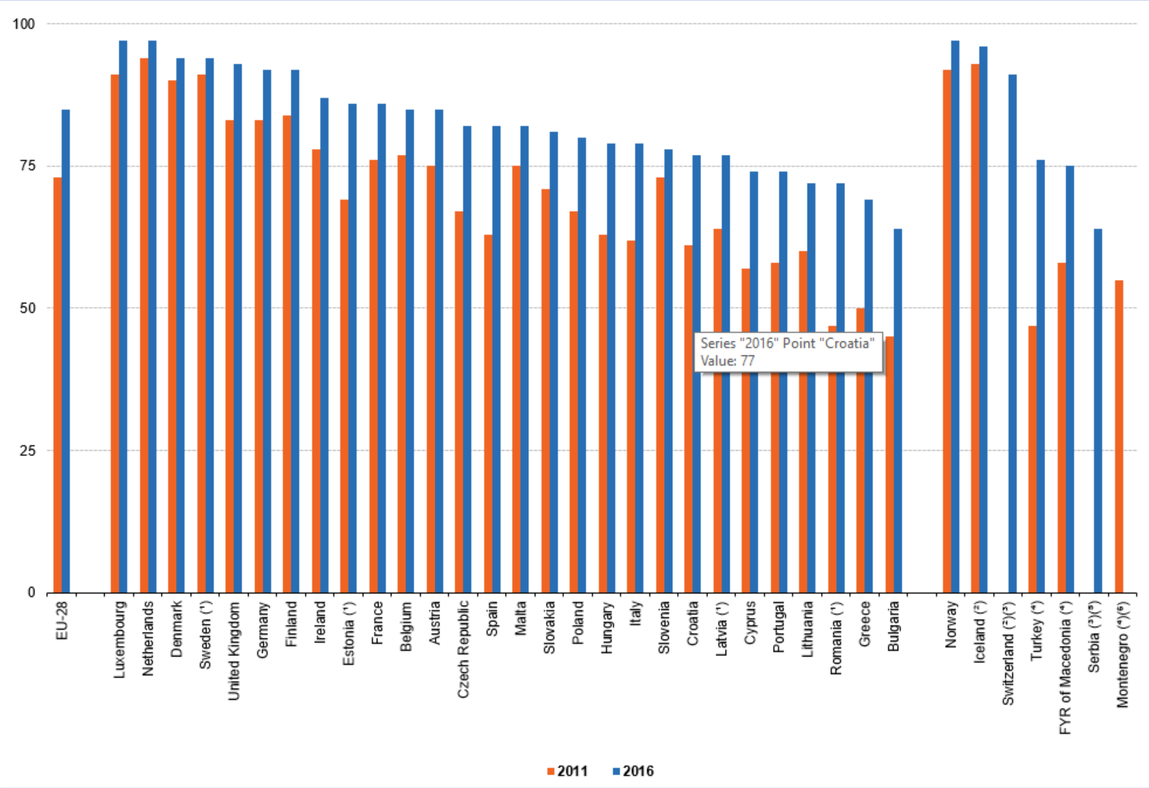
Science, technology and digital society
Digital economy and society statistics — households and individuals

Figure 1: Internet access and broadband internet connections of households, EU-28, 2007–2016
(% of all households)

	Internet access	Broadband connections
2007	55	42
2008	60	48
2009	66	56
2010	70	61
2011	73	67
2012	76	72
2013	79	76
2014	81	78
2015	83	80
2016	85	83

Source: Eurostat (online data codes: isoc_ci_in_h and isoc_ci_it_h)

Zašto GDPR?



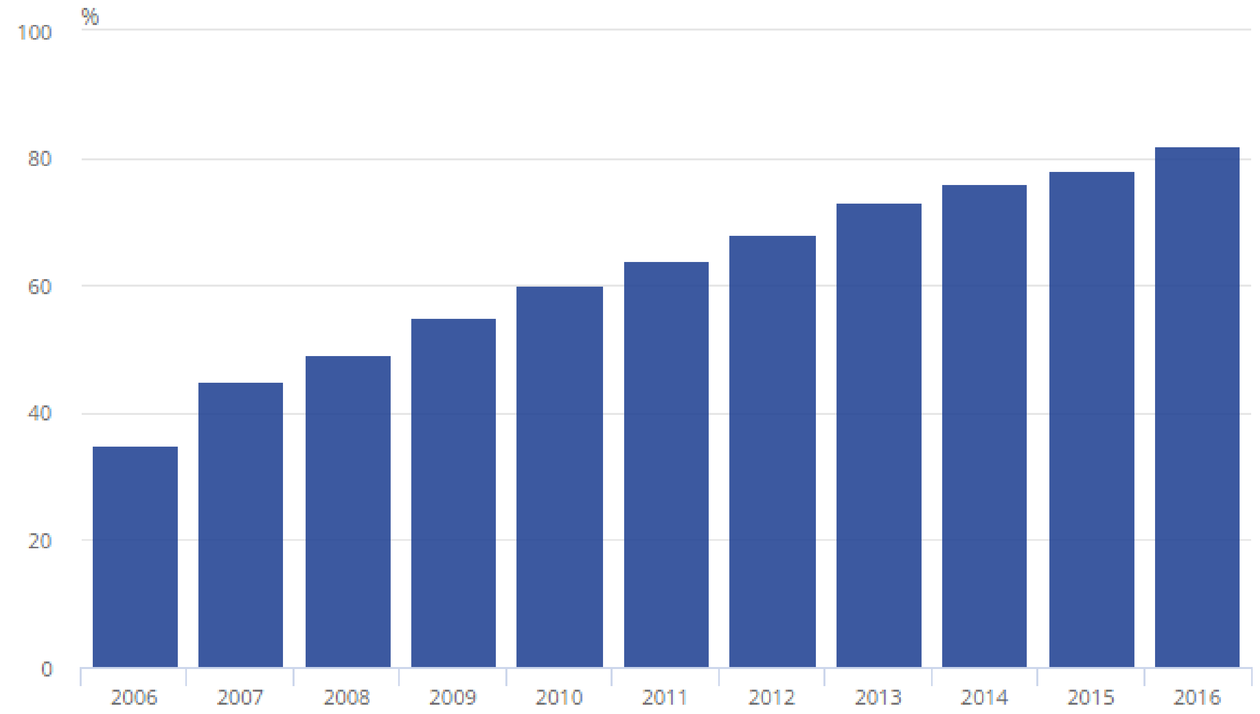
Science, technology and digital society
Digital economy and society statistics — households and individuals

Figure 2: Internet access of households, 2011 and 2016
(% of all households)

	2011	2016
EU-28	73	85

Zašto GDPR?

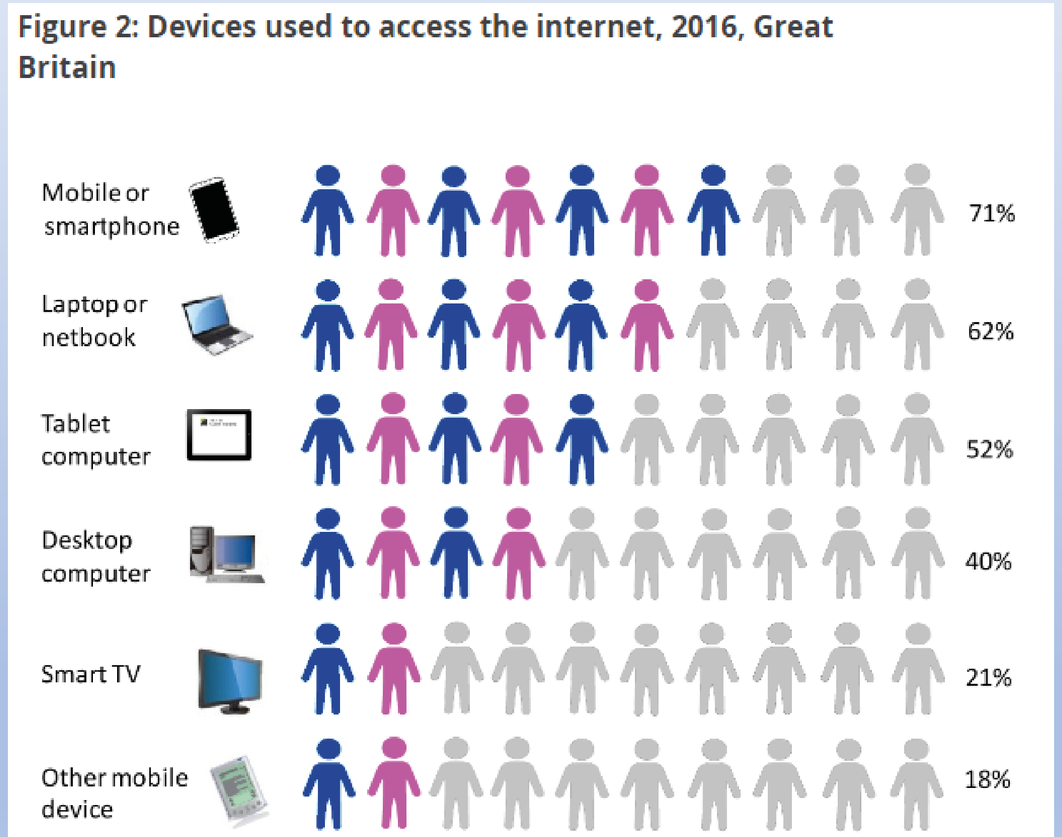
Figure 1: Daily internet use by adults, 2006 to 2016, Great Britain



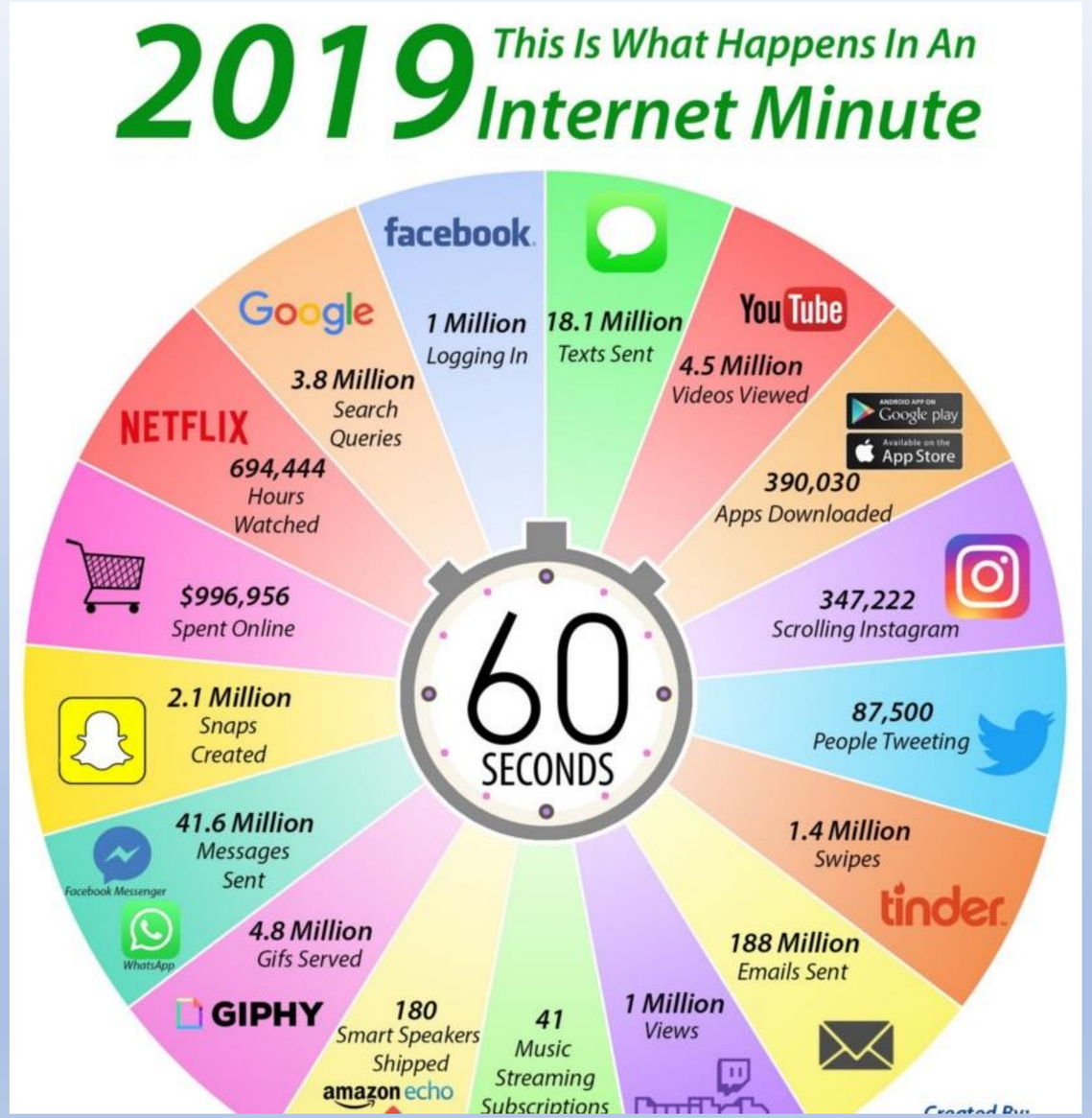
Source: Office for National Statistics

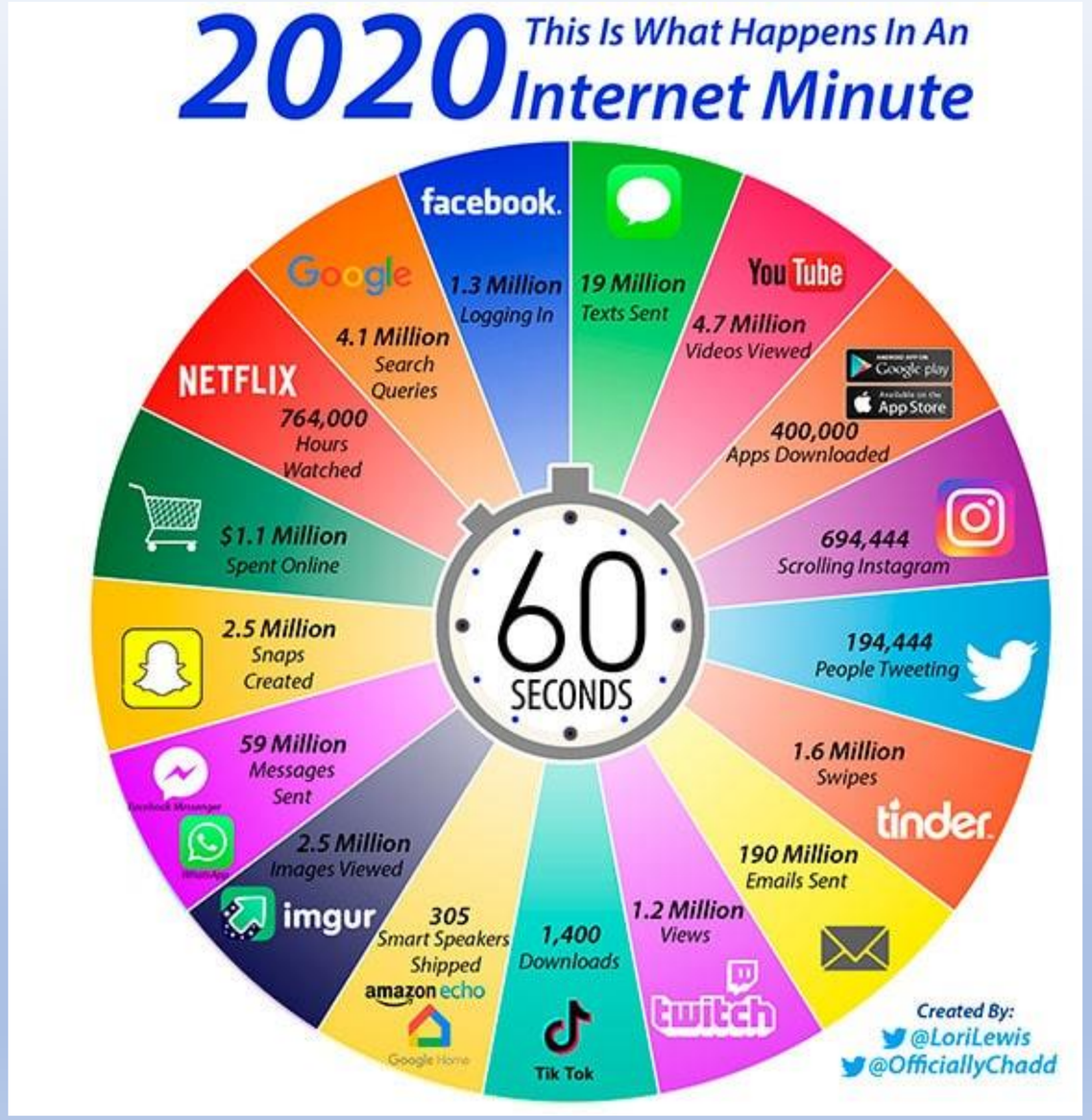
Zašto GDPR?

Figure 2: Devices used to access the internet, 2016, Great Britain



Source: Office for National Statistics


2019 This Is What Happens In An Internet Minute
facebook
1 Million
Logging In
18.1 Million
Texts Sent
YouTube
4.5 Million
Videos Viewed
390,030
Apps Downloaded
347,222
Scrolling Instagram
87,500
People Tweeting
1.4 Million
Swipes
tinder
188 Million
Emails Sent
1 Million
Views
41
Music
Streaming
Subscriptions
180
Smart Speakers
Shipped
amazon echo
4.8 Million
Gifs Served
GIPHY
41.6 Million
Messages
Sent
Facebook Messenger
WhatsApp
2.1 Million
Snaps
Created
$996,956
Spent Online
NETFLIX
694,444
Hours
Watched
Google
3.8 Million
Search
Queries
60
SECONDS


2020 This Is What Happens In An Internet Minute
facebook
1.3 Million
Logging In
19 Million
Texts Sent
YouTube
4.7 Million
Videos Viewed
400,000
Apps Downloaded
694,444
Scrolling Instagram
194,444
People Tweeting
1.6 Million
Swipes
tinder
190 Million
Emails Sent
1.2 Million
Views
twitch
1,400
Downloads
Tik Tok
305
Smart Speakers
Shipped
amazon echo
2.5 Million
Images Viewed
imgur
59 Million
Messages
Sent
2.5 Million
Snaps
Created
$1.1 Million
Spent Online
NETFLIX
764,000
Hours
Watched
Google
4.1 Million
Search
Queries
60
SECONDS
Created By:
@LoriLewis
@OfficiallyChadd

ZAŠTO GDPR?

17.05.2017.

ZAŠTO GDPR?

18.06.2018.

ZAŠTO GDPR?

8.1.2019.

ŠTO JE TO GDPR?

- Potpuna revizija regulacije zaštite podataka s opsežnim ažuriranjima onoga što se može smatrati identificirajućim informacijama **EU građana i njihovih osobnih podataka**
- Primjena u svim državama članicama EU
- Na sve organizacije koje obrađuju podatke u EU – bez obzira na to gdje je ta organizacija geografski utemeljena
- Specifična i značajna prava za pojedince vlasnike osobnih podataka da traže naknadu, pravo na brisanje i točnu reprezentaciju

Što je to GDPR?

- Uvođenje novčanih kazni u iznosu do max. 20 mil eura ili 4% godišnjeg prometa
- Naknada se može tražiti od organizacija i pojedinaca zaposlenih kod njih
- Značajno smanjenje tog iznosa temeljeno na provođenju tehničkih ili organizacijskih kontrola.

Što od nas traži GDPR

GDPR traži: odgovorno postupanje s osobnim informacijama, u svom najširem smislu

Obveza prema GDPR-u zahtijeva

- **Razumijevanje** podataka, da bi ih
- **Zaštitili** i
- **Upravljali** njima
- Gdje god se nalazili (baze podataka, datoteke, e-mail sustavi, storage)
- U bilo kojem formatu (strukturirani, nestrukturirani, audio, itd)

Osobni podatak

EU GDPR

…osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca;

Osobni podatak

- *pseudonimizacija - obrada osobnih podataka na način da se osobni podaci više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi;*

- *Genetski podaci (npr. individualna genetska sekvenca)*
- *Biometrijski podaci (otisak prsta, prepoznavanje lica, prepoznavanje očne retine, itd.)*
- *Papirnati podaci*

Ekstrateritorijalnost

EU GDPR

Primjenjuje se u slučaju AKO

*a) je organizacija **osnovana** u EU*

*b) organizacija **nudi robu i usluge** EU rezidentima*

*c) **nadzire ponašanje** EU rezidenata*

proširuje se nadzor nad organizacijama koje nisu u EU moraju se uskladiti

Primjena na izvršitelje obrade

***Izvršitelj obrade**: fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade;*

***Voditelj obrade:** fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka; kada su svrhe i sredstva takve obrade utvrđeni pravom Unije ili pravom države članice, voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom Unije ili pravom države članice;*

EU GDPR

- **Izravna obavezna odgovornost**
- dodatno i **obavezni uvjeti** za izvršitelje, podizvršitelje i kontrolore

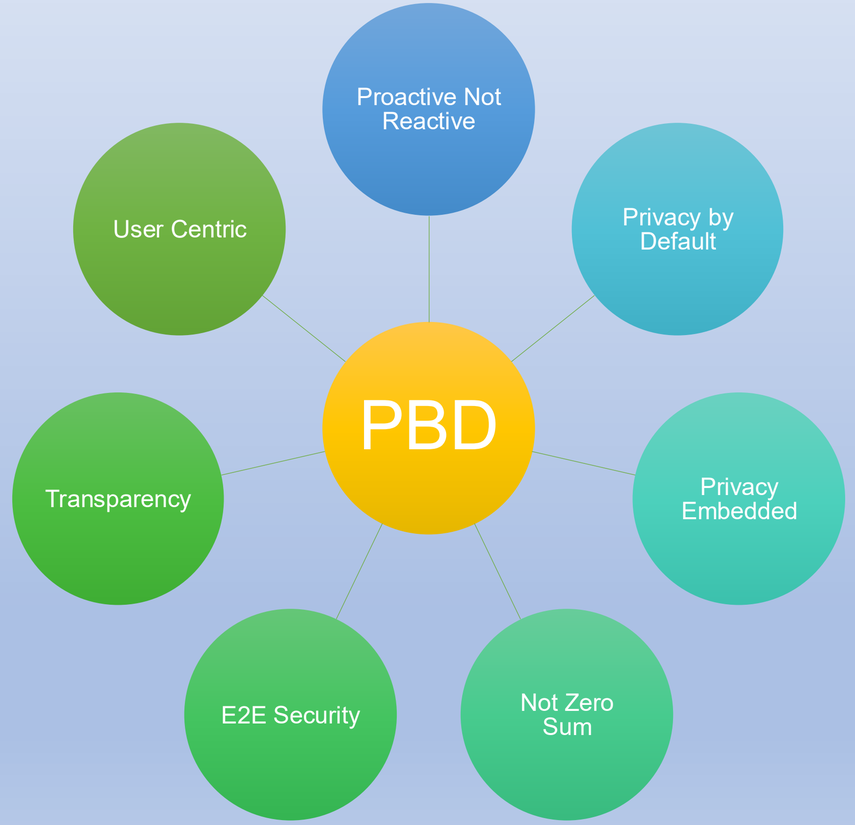
Odgovornost

Odgovarajuće mjere za utvrđivanje sukladnosti

- *usvajanje detaljnih zapisa vezanih uz obradu podataka*
- *primjena sigurnosnih mjera*
- *Procjena utjecaja na privatnost (PIA - Privacy Impact Assesment)*
- *Integrirana zaštita privatnosti (Privacy by Design)*
- *Imenovanje Službenika za zaštitu osobnih podataka (DPO - Data Protection Officer)*

Privacy by Design

Koncept integrirane zaštite privatnosti (Privacy by Design) odnosi se na neophodnost integriranja privatnosti i zaštite osobnih podataka u informacijsko komunikacijskoj tehnologiji od početka do kraja njihovog životnog ciklusa: od faze koncepcije (dizajna) do izlaska iz upotrebe.



Načela obrade osobnih podataka (zakonitost)

Privole

Opt-Out metode

prikupljanja neopozive privole

nedovoljno jasne privole

nepotpune privole

Registar “NE ZOVI”

1. stvaranje preduvjeta
2. **revizija postojećih procedura i dokumentacije**
3. čišćenje zbirki osobnih podataka i revizija prava
4. definiranje novih pravila
5. **implementacija novih rješenja i nadogradnja postojećih**
6. **dizanje svijesti**

Privola sadržava:

Svrha

Vrste podataka

Rok čuvanja

Prava ispitanika

Kome se obratiti u slučaju pritužbe

Načela obrade osobnih podataka (točnost)

Čišćenje baza podataka

Uspostava procedure ažuriranja točnosti podataka

1. stvaranje preduvjeta
2. revizija postojećih procedura i dokumentacije
3. **čišćenje postojećih baza osobnih podataka i revizija prava**
4. definiranje novih pravila
5. implementacija novih rješenja i nadogradnja postojećih
6. dizanje svijesti

Osobni podaci koji se prikupljaju i dalje obrađuju moraju biti **točni, potpuni, ažurni** te prikupljeni i obrađeni na pošten način.

Načela obrade osobnih podataka (svrhovitost)

Revizija procedura za prikupljanje podataka

1. stvaranje preduvjeta
2. **revizija postojećih procedura i dokumentacije**
3. Čišćenje postojećih baza osobnih podataka i revizija prava
4. definiranje novih pravila
5. implementacija novih rješenja i nadogradnja postojećih
6. dizanje svijesti

Načelo svrhovitosti i opsega obrade osobnih podataka govori da se osobnih podaci mogu **prikupljati u svrhu s kojom je ispitanik upoznat**, **koja je izričito navedena** i

u skladu s Zakonom i

mogu se dalje **obrađivati** samo u **svrhu u koju su prikupljeni** te da **moraju biti primjereni, relevantni i**

ne smiju biti prekomjerni

Načela obrade osobnih podataka (trajnost)

Definiranje pravila za rok čuvanja osobnih podataka

1. stvaranje preduvjeta
2. revizija postojećih procedura i dokumentacije
3. čišćenje postojećih baza osobnih podataka i revizija prava
4. **definiranje novih pravila**
5. implementacija novih rješenja i nadogradnja postojećih
6. dizanje svijesti

osobni podaci moraju biti pohranjeni u obliku koji omogućava identifikaciju osobe **samo onoliko vremena koliko je potrebno da se zadovolji svrha** zbog koje su podaci prikupljeni

Načela obrade osobnih podataka (sigurnost)

Enkripcija

Evidencija obrade

Upravljanje privolama

Pravo na zaborav

Pravo na prijenos

Osobni podaci moraju biti **zaštićeni od**

neovlaštenog pristupa i uporabe te se čuvaju u obliku koji omogućava identifikaciju fizičke osobe onoliko vremena koje je potrebno za ostvarenje svrhe prikupljanja podataka.

1. stvaranje preduvjeta
2. revizija postojećih procedura i dokumentacije
3. čišćenje postojećih baza zbirki osobnih podataka i revizija prava
4. **definiranje novih pravila**
5. implementacija novih rješenja i nadogradnja postojećih
6. dizanje svijesti

Individualna prava

I prije GDPR-a postoje prava na pristup, ispravak, brisanje ili blokiranje osobnih podataka

Također i pravo na odjavljivanje iz marketinških akcija

- *Novi zakon uključuje:*
  - *nedvosmislen pristanak na upotrebu osobnog datka*
  - *povećavanje prava pristupa i prigovora*
  - ***pravo na zaborav** (Right to be Forgotten)*
  - ***pravo na prenosivost podataka** (Right to Data Portability)*
  - ***izrada profila** - svaki oblik automatizirane obrade osobnih podataka koji se sastoji od uporabe osobnih podataka za ocjenu određenih osobnih aspekata povezanih s pojedincem, posebno za analizu ili predviđanje aspekata u vezi s radnim učinkom, ekonomskim stanjem, zdravljem, osobnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog pojedinca;*

Prijava povrede osobnih podataka

GDOR uključuje prijavu povrede osobnih podataka:

- *voditelju obrade (ukoliko ste izvršitelj obrade podataka)*
- *nadzornom tijelu*
- *pogođenim pojedincima - vlasnicima osobnih podataka*

Trenutno ne postoje pravila na razini EU (osim telco i ISP)

- izvještaj se očekuje u roku 72 sata

Imenovanje DPO

Postavljanje Službenika za zaštitu osobnih podataka – DPO (Data Protection Officer)

- kako za izvršitelje obrade tako i za voditelje obrade
- *Može biti zaposlen ili eksternaliziran*

- *Prag za imenovanje:*
  - *obavezno za tvrtke s javnim ovlastima*
  - *sistematski nadzor pojedinaca i osobnih podataka na **velikoj skali***
  - *obrada osjetljivih podataka na **velikoj skal***
  - *obaveza za tvrtke iznad 250 zaposlenih*

Poslovi:

- *podrška, informiranje i savjetovanje*
- *nadzire usklađenost*
- *svijest/edukacija*
- *obavlja PIA, PII Data Discovery*
- *točka kontakta*
- *uključen u sve slučajeve*
- *odgovoran Upravi*

Dizanje svijesti

Edukacija vanjskih partnera, izvršitelja, dobavljača i djelatnika

1. stvaranje preduvjeta
2. revizija postojećih procedura i dokumentacije
3. čišćenje postojećih baza osobnih podataka i revizija prava
4. definiranje novih pravila
5. implementacija novih rješenja i nadogradnja postojećih
6. **dizanje svijesti**

Prva kazna za kršenje GDPR-a u Hrvatskoj bit će veća od 100.000 kn

U objavi o donošenju rješenja AZOP je tad naveo da je od jedne banke čak 34 puta tražio da se uskladi s GDPR regulativom.

Prva novčana kazna za kršenje GDPR regulative u Hrvatskoj bit će veća od 100.000 kuna, doznaje Poslovni dnevnik.

Sredinom ožujka Agencija za zaštitu osobnih podataka (AZOP) objavila je da je donijela prvo takvo rješenje, ali i oko njega stvorila misteriju jer nije navela iznos kazne, ime subjekta koji je kaznila kao ni da nije objavila samo rješenje.

Kazne

azop Agencija za zaštitu osobnih podataka

O AZOP-U | DOKUMENTI | GRAĐANI | VODITELJI I IZVRŠITELJI OBRADE | SLUŽBENIK ZA ZAŠTITU PODATAKA

Rješenje kojim se izriče upravno novčana kazna zbog odbijanja dostave osobnih podataka ispitanicima

ZAHT

azop Agencija za zaštitu osobnih podataka

O AZOP-U | DOKUMENTI | GRAĐANI | VODITELJI I IZVRŠITELJI OBRADE | SLUŽBENIK ZA ZAŠTITU PODATAK

Izdana nova upravna novčana kazna

22. 2. 2021.

ZAH

Zaštitarskoj tvrtki 500.000 kuna kazne za video muškarca koji se križao nakon dezinficiranja ruku

To je prvenstveno poruka voditeljima i izvršiteljima obrade da se Opća uredba o zaštiti podataka mora shvatiti ozbiljno, govore iz Agencije

Pravilnik videonadzora

1. Svrha i područje pravilnika video nadzora
2. Kako osiguravamo da je naš sustav postavljen i da se njime upravlja vodeći računa o privatnosti i zaštiti podataka i to sukladno Općoj uredbi o zaštiti podataka?
3. Koje područje se nadzire?
4. Koje osobne podatke prikupljamo i u koju svrhu?
5. Koja je pravna osnova i zakonitost prikupljanja podataka?
6. Tko ima dostup do informacija i kome su one dostupne?
7. Kako štitimo i čuvamo podatke?
8. Kako dugo čuvamo podatke?
9. Na koji način informiramo javnost?
10. Na koji način pojedinac može provjeriti, ispraviti ili izbrisati svoje podatke?
11. Pravo na prigovor

Utjecaj Covid-19 pandemije

Porast *phishing*, *malspam* i *ransomware* napada

- Porast *phishing*, *malspam* (zlonamjerni spam) i *ransomware* napada u kojima napadači koriste COVID-19 kao mamac za predstavljanje brandova čime obmanjuje zaposlenike i kupce.
- Ovo rezultira porastom broja zaraženih osobnih računala i telefona.
- **Ne ciljaju se samo tvrtke, već i krajnji korisnici koji preuzimaju aplikacije koje se odnose na COVID-19 također su meta prevara u kojima preuzimaju ransomware prerušen u legitimne programe.**
- Potrebno je poduzeti proaktivne korake podižući svijest svojih djelatnika
- Kupci trebaju biti oprezniji pogotovo kada otvaraju linkove, e-mail ili dokumente povezane s COVID-19 temom.

Povećani sigurnosni rizik od rada na daljinu

- S porastom broja zaposlenika koji rade od kuće (školaraca i studenata koji imaju virtaulnu edukaciju) virtualna privatna mreža poduzeća (VPN) postaje spas, a njihova sigurnost i dostupnost bit će glavni fokus sigurnosti.
- U želji da se to postigne, postoji mogućnost pogrešne konfiguracije sigurnosti u VPN-ovima, izlaganje osjetljivih podataka na internetu i također izlaganje napadima uskraćivanja usluge (DoS).
- Uz to, pojedini korisnici (ili više njih istodobno) mogu koristiti osobna računala za obavljanje službenih dužnosti koje bi također mogle predstavljaju veliku količinu rizika.
- Potrebno je osigurati da su VPN usluge sigurne i pouzdane jer je izgledno da će biti puno više nadzora protiv ovih usluga.
- Nadalje, zaposlenici se ne bi trebali koristiti privatnim računalima u službene svrhe.

Potencijalna kašnjenja u otkrivanju i odgovoru na cyber-napad

- Funkcionirati sigurnosnih timova je narušeno zbog pandemije COVID-19 a time se
- otežava otkrivanje zlonamjernih aktivnosti i odgovaranje na ove aktivnosti postaje još složenije.
- Ažuriranje zakrpa na sustavima također može biti izazov ako sigurnosni timovi nisu operativni.
- Potrebno je napraviti procijeniti sigurnosne zaštite i istražiti upotrebu zajedničkog rada s vanjskim konzultanata, posebno za područja u kojima ključni faktori ljudskog rizika identificirani.

Priljev cyber kriminalaca

- Globalno, tvrtke smanjuju svoju radnu snagu kako bi se nosile s učincima COVID-19.
- Neki ljudi su također izgubili sredstva za život zbog različitih ograničenja kretanja od strane vlada širom Europske unije i svijeta.
- Ovaj potez je potaknuo rast cyber kriminalaca kao nezaposlenih s pristupom internetu koji su izgubili posao zbog posljedica COVID-19 i na ovaj način vide priliku za život od pandemije.
- Organizacije koje razmišljaju o otpuštanju trebaju provoditi pravilne planove izlaska.
- Također, potrebno je poticati sve koji su izgubili posao ili ne mogu raditi zbog izolacije na razmatranje uzimanja tog razdoblja za učenje novih profitabilnih vještina i pohađanje internet tečajeva.

Ažuriranje BCP planova

- Mnoge organizacije imaju planove nastavka poslovanja (BCP), ali je evidentno da utjecaj globalne pandemije COVID-19 u njima nije razmatran.
- S povećanim utjecajem COVID-19, organizacije trebaju ažurirati postojeće BCP i planove odgovora na incidente posebno za slučaj pandemije koje pogađaju mnoge zemlje i kritične elemente opskrbnih lanaca istovremeno.
- Treba napraviti reviziju procjene rizika na kritični procesi za prepoznavanje različitih mogućnosti u sustavu Windows i osigurati da se ti procesi i dalje mogu odvijati na prihvatljivoj razini

Cyber sigurnost nakon COVID-19

- Pandemija COVID-19 izazvala je veliko opterećenje na globalno gospodarstvo a stručnjaci predviđaju recesiju kao dio posljedica pandemije.
- Post COVID-19 strategija može uključit smanjenje poslovnih linija koje se ne smatraju kritičnim što može uključivati operacije cyber sigurnosne.
- Ovaj kratkoročni plan mogao bi se pokazalo kao „ubijanje krave zbog šnicle„ na duge staze jer to može dodatno povećati utjecaj napada.
- Savjet je ažuriranje BCP i politika / praksi rada na daljinu radeći uz određivanje prioriteta kibernetičke sigurnosti nakon COVID-19 pandemije.

Cyber prijetnje

Osobni podaci klijenata

- Izazovom prikupljanja i rukovanja podacima klijenata (i potencijalnih) zbog same količine podataka i činjenice da su pohranjene informacije često izuzetno osjetljive i osobne prirode.
- Stoga su posljedice povrede podataka vrlo teške, a podatke čini i vrlo atraktivnom metom za lopove.
- Stoga je potrebna velika doza opreza prilikom provođenja procjene rizika na vlastitim sigurnosnim sustavima.
- Sigurnost se svodi na dizajniranje i učinkovitu primjenu robusnih sustava kako bi se smanjila površina napada.
- To uključuje strogo ograničavanje pristupa zaposlenika osjetljivim zapisima i primjenu robusnih sigurnosnih mjera poput biometrijske dvofaktorske provjere autentičnosti za osoblje ovlašteno za pristup osjetljivim zapisima.
- Također uključuje postavljanje temeljitog sustava revizije za praćenje datoteka kojima se pristupa i koji temeljito istražuje sve otkrivene anomalije ili kršenja.
- Kad se otkrije da su zaposlenici prekršili sigurnosne protokole, moraju se provesti značajne sankcije kako bi se osiguralo da se protokoli pravilno slijede.

GDPR kazne

- Ukoliko dođe do povrede podataka moguće je očekivati i tužbe klijenata na ime naknade štete zbog ranjivosti njihovih podataka.
- Tužbe od klijenata mogu uslijediti jer postoji zakonska odgovornost (GDPR) zaštitite svih osobnih podatke koji se prikupljaju i pohranjuju za potrebe poslovanja.
- Kako bi se izbjegla potencijalna poslovna i financijska katastrofu, uvijek je u najboljem interesu osigurati da su svi podaci klijenata zaštićeni, ne samo iza vatrozida, već s detaljnom sigurnosnom politikom koju provode svi zaposlenici, partneri i dionici.

Sigurnost web stranica

- S obzirom na to da distributeri veliku većinu svog poslovanja obavljaju na mreži, neophodno je da se njihovi internetski portali redovito ispituju na sigurnost i prije i nakon što postanu aktivni.
- To znači pregled koda i sigurnosno testiranje prije puštanja u rad kako bi se osiguralo da nisu prisutne softverske pogreške koje bi mogle dovesti portal u opasnost.
- Testiranje pomaže osigurati da se s otkrivanjem novih ranjivosti osigura da je portal siguran i zaštićen od ranjivosti, bilo krpanjem ili ublažavanjem kontrola poput vatrozida web aplikacija koje mogu "*virtualno zakrpati*" portal dok razvojni tim ne nađe "pravi" zakrpu za rješavanje problema.

Edukacija korisnika

- Iako se tehnički timovi bave problemima koji se mogu pojaviti na internetskom portalu, potrebno je osigurati da interni krajnji korisnici (koji se često nazivaju najslabijom karikom u sigurnosnom lancu), budu pravilno educirani te da nehotice ne izlažu organizaciju klikom na *link* ili otvaranjem zlonamjernog privitka.
- Bez ove sigurnosne obuke, interni krajnji korisnici riskiraju nanijeti potencijalno veću štetu.
- Mogu zaraziti mrežu trojanskim virusima s daljinskim upravljačem ili čak *ransomware*-om, što bi moglo dovesti do toga da se moraju isključiti neke ili sve operacije tvrtke, ovisno o tome koliko je zaraza zlonamjernim softverom loša.
- Trening o sigurnosti trebao bi se baviti snažnom konstrukcijom lozinki, načinom prepoznavanja *phishing* napada, kao i pokušajima *socijalnog inženjeringa*.

Višeslojna strategija sigurnosti

- Većina današnjih organizacija suočava se sa sličnim sigurnosnim izazovima sličnim većini
- Posjedovanje višeslojne sigurnosne strategije pomaže smanjivanju rizika od povreda podataka koje rezultiraju krađom intelektualnog vlasništva, podataka o klijentima, partnerima, poslovnih podataka i / ili drugih osjetljivih podataka.
- Holistički pristup osiguranju sustava započinje usvajanjem Cyber okvira.
- Potrebno je identificirati i napraviti inventar IT imovine radi boljeg upravljanja i održavanja, a zatim je zaštititi tako dajući prioritete kritičnim sustavima i primjenjujući najbolje moguće sigurnosne proizvode i usluge.
- Neke zaštite mogu uključivati kontrolu pristupa, mrežnu sigurnost, zaštitu krajnje točke, šifriranje podataka i nadzor događaja.
- Također je dobro otkriti sustave koji su ugroženi ili osjetljivi na eksploataciju i stvoriti plan odgovora koji je usmjeren na proces kako bi se smanjilo vrijeme oporavka sve pogođene imovine u cijeloj organizaciji.
- Najbolji sigurnosni planovi su oni koji su iterativni, orijentirani na procese i okretni prema dinamičnom krajoliku prijetnji gdje novi vektori napada i tehnike zahtijevaju konstantan oprez.

Ransomware

- Danas najveću zabrinutost za svaku organizaciju predstavljaju ransomware napadi
- Ključni razlog su ogromne količine podataka koje imaju sve tvrtke koje se bave poslovima osiguranja
- Ransomware napadi nisu novi; taktika koju koriste cyber kriminalci je jednostavna: upotreba zlonamjernog softvera koji blokira pristup računalnom sustavu ili podacima, obično šifriranjem, sve dok žrtva ne plati značajnu naknadu napadaču.
- Osiguravajuće i zdravstvene ustanove prioritet su broj jedan za cyber kriminalce zbog velikog broja podataka koje pohranjuju o pacijentima i kupcima.
- Najbolji način za ublažavanje takvog rizika je spriječiti situaciju i zaštititi se prije nego što se dogodi. Vrlo je teško dešifrirati hakirane datoteke, a može biti još zamršenije kretati u pregovore s cyber kriminalcima.
- Na primjer, provođenje pen-testova

Trojanski konji, crvi, virusi

Uz ransomware najveće prijetnje s kojima se suočavaju današnje organizacije su trojanski konji, crvi, virusi, profesionalni hakeri i cyber-iznuđivači, nezadovoljni sadašnji i bivši zaposlenici te korisničke pogreške i nepažnja.

Kako bi se ublažili ovi rizici potrebno je:

- Koristite VPN, virtualnu privatnu mrežu.
- Osigurajte svoje uređaje. Imajte na umu svaku aplikaciju koju instalirate te dozvole i pristup koji im date. Ako je aplikacija besplatna, obično plaćate podacima. Uklonite unaprijed instalirane aplikacije koje ne upotrebljavate - takozvani bloatware. Razmislite o isključivanju kolačića i praćenju.
- Zaštitite svoje poruke. Uzmite u obzir **Signal**, Telegram ili Whatsapp (ako vjerujete Facebooku).
- Ne upotrebljavajte javni Wi-Fi.
- Budite svjesni prijetnji. Potencijalne povrede podataka vrebaju iza svakog ugla. Možete biti svjesni promjena okruženja prijetnje i zaštititi se sustavom kao što je Trend Micro.
- Kontrolirajte svoja korisnička dopuštenja. Budući da zaposlenici dolaze i odlaze, ljudi koji rade na daljinu te sve više pametnih telefona pristupa mrežama tvrtki, važnije je nego ikad strogo kontrolirati korisnička dopuštenja unutar vašeg poslovanja. Ograničite pristup zaposlenima izvan mjesta i pobrinite se za opoziv nepotrebnih dozvola kad zaposlenici odu ili promijene položaj.
- Redovito i često ažurirajte lozinke. Jedan od najlakših načina da haker provali vaš sustav je probijanjem lozinke - što je sve lakše učiniti kada najpopularnije lozinke uključuju lozinku i 123456. Obavezno promijenite lozinku nekoliko puta godišnje.
- Ostanite sigurni u oblaku. Brokeri se sve više oslanjaju na rješenja za pohranu podataka zasnovana na oblaku, ali nije svaki oblak jednak. Provjerite imaju li oblaci koje upotrebljavate značajke poput šifriranja kada se datoteke prenose, kao i kada nisu.
- Stvorite akcijski plan nakon povrede podataka. Nitko od nas nikada ne namjerava biti prekršen, ali čak i ako učinimo sve što možemo kako bismo to izbjegli, i dalje bismo mogli postati žrtve. Ako to učinimo, moramo brzo djelovati. Zbog toga je dobro imati akcijski plan nakon probijanja kao dio vašeg općeg planiranja u slučaju katastrofe.
- Odaberite pravi suradnički softver. Bez obzira imate li zaposlenike koji rade na daljinu ili imate mrežne sastanke i webinare, morate odabrati zajednički softver koji smanjuje rizik od povrede podataka. Odaberite alate koji šifriraju poruke i imaju dvofaktorsku provjeru autentičnosti prilikom prijave.

Zastarjeli softver

- U usporedbi s drugim financijskim industrijama, sektor osiguranja još uvijek zaostaje u usvajanju cyber sigurnosti
- Cyber kriminalci više su usmjereni na banke i druge financijske institucije, ali sada su te institucije dobro osigurane u smislu cyber sigurnosti.
- Kkao im to više nije laka meta, cyber kriminalci ciljaju osiguravatelje, osiguravajuće tvrtke sadrže znatne količine podataka o osobnim, financijskim, imovinskim i drugim osobnim podacima.
- Glavni kibernetički rizici:
  - Korištenje zastarjelog sigurnosnog softvera omogućuje hakerima jednostavan napad na sustav.
  - Prijetnje poput pucanja vjerodajnica i skeniranja ranjivosti mogu virtualno isključiti cijeli sustav preko noći. Kako bi se prevladale ove prijetnje, prvo je potrebno educirati djelatnike i partnere da prepoznaju zlonamjerne ili sumnjive aktivnosti. Također je potrebno implementirati sigurnosne protokole, softver i uređaje koji mogu zaštititi podatke od prijetnji.
  - Ransomware: jednostavno rješenje je korištenje pohrane u oblaku i sigurnosna kopija sa širokim rasponom značajki kibernetske sigurnosti koja mogu zaštititi sustav od zlonamjernog koda.

Primjeri i zaštita

Procjena rizika

Procjena rizika određuje koje podatke i sustave treba zaštititi i prijetnju izloženosti. Procjena rizika trebala bi obuhvatiti:

- Gdje i kako se čuvaju osjetljivi podaci, tko ih koristi i kako se koriste
- Kako se koristi e-pošta
- Kako se podacima pristupa na daljinu
- Koji se pristupi koriste za zaštitu podataka
- Kada i gdje se koriste mobilni uređaji

Sveobuhvatni sigurnosni plan

- Stvaranje sveobuhvatnog sigurnosnog plana.
- Sveobuhvatan sigurnosni plan trebao bi se baviti sigurnosnim ranjivostima i navesti pristupe za zaštitu od sigurnosnih propusta i oporavka od njih.
- Ne bi trebao zaštititi samo vitalne podatke od hakera i cyber kriminalaca, već i zaštititi od nenamjerne izloženosti podataka upućenih osoba.
- Plan treba testirati kako bi se provjerilo radi li dobro.

Dubinska obrana

- Snažna obrana od prijetnji kibernetske sigurnosti može se stvoriti primjenom rješenja koje provodi kombinaciju proaktivnih i reaktivnih tehnologija. Jedan od takvih pristupa je otkrivanje i odgovor krajnje točke (*Endpoint Detection & Response* - EDR), koji kontinuirano nadgleda i brzo reagira na prijetnju kibernetske sigurnosti.
- Međutim, EDR rješenje može biti pretjerano složeno, proizvodeći velike količine podataka i upozorenja. Uz to, mnoga EDR rješenja oslanjaju se na umjetnu inteligenciju koja ponekad propušta hvatanje ključnih informacija.
- Boljim pristupom upravlja se EDR-om, koji kombinira praćenje prijetnji 24 sata dnevno, odgovor na incidente i filtriranje upozorenja.
- Upravljani EDR pruža dublje istraživanje, analizu i provjeru valjanosti prijetnji od EDR-a kombinacijom napredne analitike, obavještajnih podataka o prijetnjama, forenzičkog prikupljanja podataka i ljudske stručnosti.

Sigurnosna kultura

- Dobar sigurnosni program mora uključivati politike obuke koje educiraju osoblje o sigurnosnim politikama i planovima i povećava njihovu sigurnosnu svijest.
- Zaposlenici koji budno i motivirano štite osjetljive podatke najcjenjeniji su oklop u obrani od prijetnji cyber sigurnosti.
- Važna su strana obuke o osvješćivanju o sigurnosti simulacije koje oponašaju zlonamjeran pristup socijalnom inženjeringu, poput krađe identiteta i krađe koplja, namijenjene zavaravanju zaposlenika u otkrivanju osjetljivih podataka.

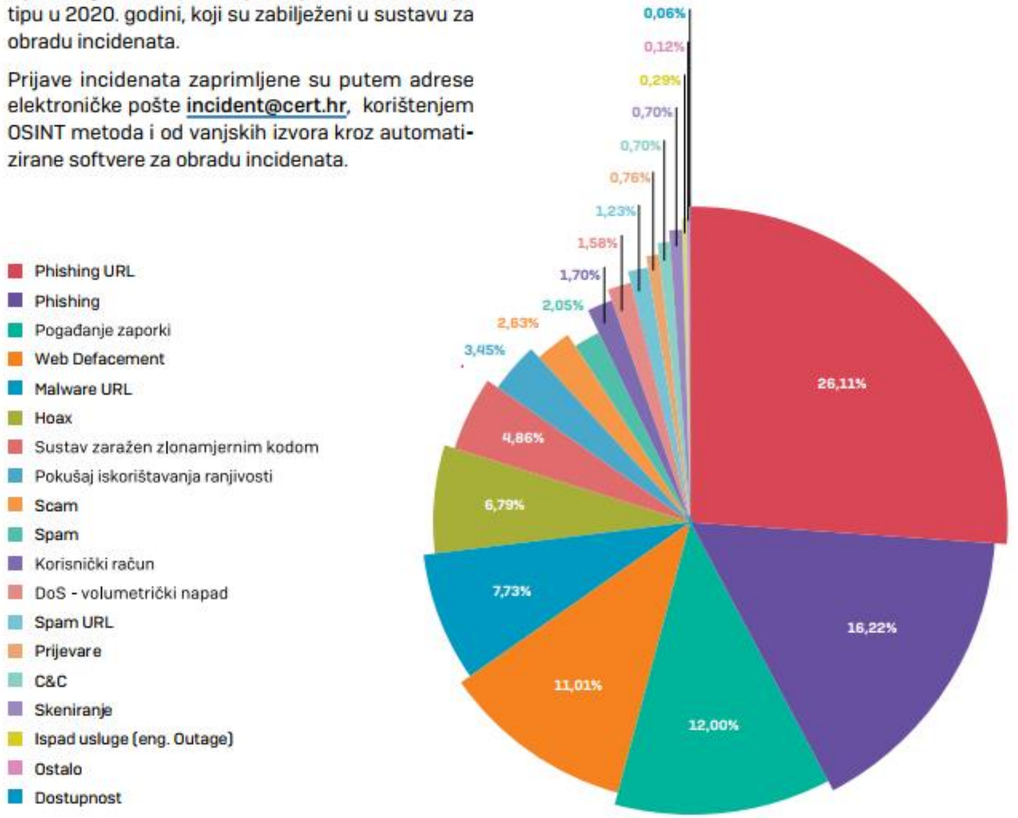
Sigurnosne usluge

- Rastući obujam i sofisticiranost cyber napada otežavaju tvrtkama a i njihovim IT odjelima posvećivanje vremena i pažnje potrebnog za suzbijanje tih prijetnji.
- Kao odgovor na to, važno je iskoristiti pružatelje usluga koji imaju stručnost za razvoj i provedbu sigurnosnih planova.

2.2. RASPODJELA INCIDENATA PO TIPU

Sljedeći grafikoni prikazuju omjere incidenata po tipu u 2020. godini, koji su zabilježeni u sustavu za obradu incidenata.

Prijave incidenata zaprimljene su putem adrese elektroničke pošte incident@cert.hr, korištenjem OSINT metoda i od vanjskih izvora kroz automatizirane softvere za obradu incidenata.



Raspodjela incidenata po tipu u 2020. godini

TIP INCIDENTA	BROJ	TREND
PHISHING URL	446	▲
PHISHING	277	▲
POGAĐANJE ZAPORKI	205	▲
WEB DEFACEMENT	188	▲
MALWARE URL	132	▲
HOAX	116	▲
SUSTAV ZARAŽEN ZLONAMJERNIM KODOM	83	▲
POKUŠAJ ISKORIŠTAVANJA RANJIVOSTI	59	▲
SCAM	45	▲
SPAM	35	▼
KORISNIČKI RAČUN	29	▲
DOS - VOLUMETRIČKI NAPAD	27	▲
SPAM URL	21	▲
PRIJEVARE	13	▼
C&C	12	▲
SKENIRANJE	12	▲
ISPAD USLUGE (ENG. OUTAGE)	5	–
OSTALO	2	▼
DOSTUPNOST	1	–
DOS - NAPAD NA APLIKACIJSKOM SLOJU	1	–
ZLONAMJERNO RUDARENJE KRIPTOVALUTE (ENG. CRYPTOJACKING)	1	–
UKUPNO	**1710**	▲

Prikaz incidenata po tipu u 2020. godini

Prikaz popularnih vrsta zlonamjernih sadržaja

Zlonamjerni *ransomware* sadržaj

- Naziv za skup zlonamjernih programa koji korisniku onemogućuju korištenje raounala
- Nakon zaraze zlonamjerni ransomware sadržaj može šifrirati datoteke iii onemogućiti njihovo korištenje tako da se pojavi početni ekran s određenom porukom koju nije moguće maknuti
- Od korisnika čije je računalo zaračeno traži se otkupnina u zamjenu za daljnje normalno korištenje računala

Cryptominer

- Zlonamjerni sadržaj za neovlašteno rudarenje elektroničkih kriptovaluta je relativno nova vrsta zlonamjernog sadržaja čiji je glavni zadatak preuzimanje resursa računala te trošenje istih na rudarenje elektroničkih kriptovaluta bez odobrenja vlasnika računala
- Ova je vrsta zlonamjernog sadržaja veoma popularna jer napadači korištenjem resursa mnogih računala stječu novčanu dobit

WannaCry (2017.)

1

Napad s početka priče zahvatio je poznate kompanije kao što su španjolska Telefonica, FedEx, Deutsche Bahn, Renault i Sberbank,

Cryptolocker (2013.)

2

Smatra se prvim modernim ransomwareom, a autor mu je jedan od najpoznatijih i najtraženijih cyber kriminalaca u

Locky (2016.)

3

Postao je svjetski poznat nakon što je Holivudski prezbiterijanski medicinski centar uplatio 17 000 dolara otkupnine kako bi nakon više

Cerber (2016.)

4

Predstavlja novu generaciju ransomwarea, specifičnu po tome što funkcioniraju kao ransomware usluga; u praksi to znači da cyber kriminal

TeslaCrypt (2015.)

5

Isprva se pojavio kao malware koji se veže uz određene računalne igre da bi nakon nekog vremena postao najzastupljeniji ransomware koji je

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be **arrested**.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press

OK


Payment will be raised on
5/15/2017 15:58:08
Time Left
02:23:58:59
Your files will be lost on
5/19/2017 15:58:08
Time Left
06:23:58:59
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Prikaz popularnih vrsta zlonamjernih sadržaja

Zlonamjerni *wiper* sadržaj

- Ovoj vrsti zlonamjernog sadržaja primarni je zadatak uništavanje sustava i/ili podataka te ih zbog toga možemo nazivati i brisačima
- Napadi ovom vrstom zlonamjernog sadržaja obično uzrokuju velike financijske i reputacijske štete tvrtkama žrtvama
- Akteri koji stoje iza ove vrste napada su najčešće motivirani slanjem političke poruke, sabotiranjem ili jednostavno prikrivanjem vlastitih tragova nakon uspješnog prikupljanja podataka

Zlonamjerni kod bez datoteke

- Zlonamjerni kod bez datoteke ne ostavlja artefakte/dokaze na lokalnom tvrdom disku prilikom zaraze ciljanog računala zbog čega lako zaobilazi tradicionalne sigurnosne i forenzičke alate temeljene na sigurnosnom potpisu
- Tipični napadi iskorištavaju ranjivosti u preglednicima i povezanim programima (Java, Flash ili PDF čitači) ili ih napadači isporučuju koristeći *phishing*

Prikaz popularnih vrsta zlonamjernih sadržaja

Trojanski konj

- Trojanski konj oblik je zlonamjernog sadržaja koji se lažno predstavlja kao neki koristan program kako bi ga korisnik izvršio, odnosno dozvolio mu instalaciju
- Termin je, zbog analogije, preuzet iz grčke mitologije
- Trojanski konj može izmijeniti operacijski sustav na zaraženom računalu kako bi on prikazivao oglase iii skočne prozore u svrhu ostvarivanja novčane koristi od strane napadača
- Opasniji je slučaj kada trojanski konj omogući napadaču potpunu kontrolu nad zaraženim računalom

Botnet

- Jedna od najvećih prijetnji internetu je prisutnost velike količine kompromitiranih računala
- Mreže takvih računala često se nazivaju *botnet* mreže iii "zombi vojske", a računala koja su njihov dio prisutna su u kućanstvima, školama, poslovnim zgradama i vladama diljem svijeta
- Uglavnom se nalaze pod kontrolom jednog (iii nekolicine) hakera, a koriste se za izvođenje raznih oblika napada - od distribuiranih napada uskraćivanja usluga (eng. Distributed Denial-of-Service, DDoS), slanja neželjenih poruka elektroničke pošte, iskorištavanja alata za praćenje pritisaka tipki (eng. keylogger) do širenja tzv. malware programa i sl.

Prikaz popularnih vrsta zlonamjernih sadržaja

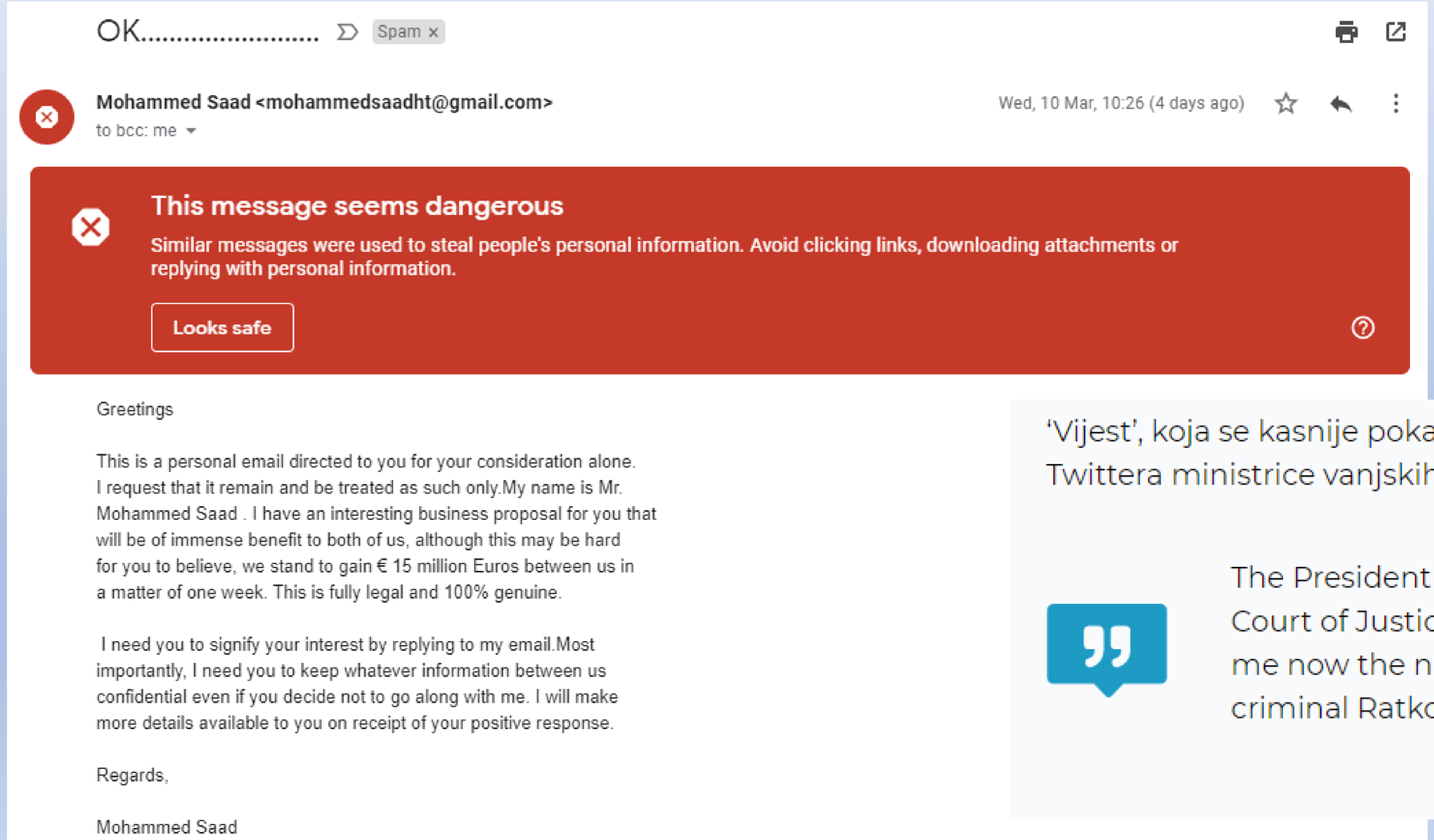
Neželjena pošta (eng. *Spam*)

- Spam je neželjena elektronička poruka poslana s namjerom oglašavanja raznog reklamnog sadržaja, u svrhu *phishing* napada ili kao sredstvo distribucije zlonamjernih poveznica
- Najčešće se šalje putem elektroničke poste
- Osim u slučaju e-poste, spam se koristi još i kod elektroničkih foruma, blogova, socijalnih mreža, servisa za izravnu komunikaciju i drugih sustava za razmjenu poruka ili drugih podataka
- Širitelji spama nazivaju se spameri (eng. spammers).

Hoax

- Hoax je poruka elektroničke poste neistinitog sadržaja, poslana s ciljem zastrašivanja ili dezinformiranja primatelja
- Želja osobe koja je poslala hoax je njegovo prosljeđivanje na što veći broj adresa
- Pri tome ih primatelji doista i prosljeđuju internetom jer su uvjereni da time pomažu drugima
- Hoax ne može uzrokovati oštećenja računalnih programa i operacijskih sustava, ali zabilježeni su brojni slučajevi gdje je hoax svojim sadržajem i vještom psihologijom naveo korisnike da sami oštete svoje programe i sustave
- Drugi oblik štete koju hoax može nanijeti je zavaravanje korisnika to narušavanje njihovog ugleda, kao i ugleda određenih organizacija, tvrtki i poznatih osoba.

Primjeri hoaxa



OK..... Spam ×

Mohammed Saad <mohammedsaadht@gmail.com>
to bcc: me

Wed, 10 Mar, 10:26 (4 days ago)

This message seems dangerous

Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments or replying with personal information.

Looks safe

Greetings

This is a personal email directed to you for your consideration alone. I request that it remain and be treated as such only.My name is Mr. Mohammed Saad . I have an interesting business proposal for you that will be of immense benefit to both of us, although this may be hard for you to believe, we stand to gain € 15 million Euros between us in a matter of one week. This is fully legal and 100% genuine.

I need you to signify your interest by replying to my email.Most importantly, I need you to keep whatever information between us confidential even if you decide not to go along with me. I will make more details available to you on receipt of your positive response.

Regards,

Mohammed Saad

‘Vijest’, koja se kasnije pokazala lažnom, prenijeli su ‘s Twittera ministrice vanjskih poslova BiH **Bisere Turković’.**

> The President of the International Court of Justice A.A.Yusuf confirms me now the news of the death of war criminal Ratko Mladić.
>
> — Bisera Turković (@BTurkovicBH) February 11, 2020

Phishing

- Phishing (varijanta engleske riječi za pecanje, fishing) je vrsta socijalnog inženjeringa koja se odnosi na prijevare, kojima se služe zlonamjerni korisnici šaljući lažne poruke koristeći pritom postojeće internet servise. Riječ je o kriminalnoj aktivnosti.
- Koristeći razne načine manipulacije, kriminalci od korisnika pokušavaju prikupiti povjerljive podatke (korisnička imena, lozinke, podaci s kreditnih kartica i sl.) kako bi ostvarili financijsku korist.
- U pravilu, phishing poruke prenose se putem elektroničke pošte koja navodi korisnika da klikne na određeni link koji ga dalje vodi na stranice zloćudnog web poslužitelja.
- Takve zloćudne Web stranice obično se lažno predstavljaju kao Web stranice banaka, servisa za elektroničko plaćanje (PayPal i dr.) i sl. krivotvoreći, odnosno imitirajući njihov izgled.
- U svrhu phishing-a, osim elektroničke pošte, mogu poslužiti i drugi servisi poput foruma, servisa za izravnu komunikaciju (Whatsapp, Skype, i dr.) te društvene mreže (Facebook, Instagram).
- Društvene mreže posebno su opasne jer podaci prikupljeni sa njih mogu poslužiti za krađu identiteta, ali i zbog činjenice da poruke dobivene od prijatelja, kojima su kompromitirani računi, imaju određeni kredibilitet.

Krađa identiteta

Krađa identiteta daleko je najčešća vrsta *phishinga*. Prevaranti se predstavljaju kao legitimna tvrtka u pokušaju krađe osobnih podataka ili vjerodajnica za prijavu. E-pošta često koristi prijetnje i osjećaj hitnosti kako bi uplašila korisnike da rade ono što napadači žele.

Tehnike korištene u krađi identiteta

- **Legitimni linkovi**: Mnogi napadači pokušavaju izbjeći otkrivanje preko filtara e-pošte ugrađujući legitimne linkove u svoje lažne phishing e-adrese. To rade na način da uključuju legitimne kontakt podataka s organizacijom koje lažiraju.
- **Spajanje zlonamjernog i bezopasnog kôda**: odgovorni za stvaranje *phishing* odredišnih stranica obično kombiniraju zlonamjerni i bezopasni kôd da bi zavarali Exchange Online Protection (EOP).
- **Preusmjeravanja i skraćene veze**: Zlonamjerni napadači ne žele alarmirati svoje žrtve. Stoga izrađuju svoje phishing kampanje kako bi koristili skraćene URL-ove kao sredstvo zavaravanja sigurnih pristupnika e-pošte (SEG), preusmjeravanjem korisnika na *phishing* odredišnu stranicu tek nakon isporuke e-pošte i preusmjeravanja na legitimne web stranice nakon što su žrtve izgubile vjerodajnice.
- **Izmjena logotipa robne marke**: Neki filtri e-pošte mogu uočiti kada zlonamjerni napadači ukradu logotipe organizacija i ugrade ih u svoju e-poštu o napadu ili na svoje odredišne stranice za krađu identiteta. To čine tražeći HTML atribute logotipa. Da bi zavarali ove alate za otkrivanje, zlonamjerni napadači mijenjaju HTML atribut logotipa, poput njegove boje.
- **Minimalni sadržaj e-pošte**: Digitalni napadači pokušavaju izbjeći otkrivanje uključivanjem minimalnog sadržaja u svoje e-poruke o napadima.

Spear Phishing

- U ovoj vrsti prevare, napadači prilagođavaju svoje e-adrese napada ciljnim imenom, položajem, tvrtkom, radnim brojem telefona i ostalim informacijama, pokušavajući prevariti primatelja da vjeruje da imaju vezu s pošiljateljem.
- Ipak je cilj isti kao i krađa identiteta: prevariti žrtvu da klikne na zlonamjerni URL ili privitak e-pošte kako bi predala svoje osobne podatke.
- S obzirom na količinu informacija potrebnih za stvaranje uvjerljivog pokušaja napada, ne čudi da je krađa identiteta uobičajena na web lokacijama društvenih medija poput *LinkedIn-a* gdje napadači mogu koristiti više izvora podataka za izradu ciljane e-pošte napada.

Tehnike korištene u spear phishing

- **Smještanje zlonamjernih dokumenata na usluge u oblaku:** Digitalni napadači sve više smještaju svoje zlonamjerne dokumente na Dropbox, OneDrive, Google Drive i druge usluge u oblaku. Prema zadanim postavkama, IT vjerojatno neće blokirati ove usluge, što znači da filtri e-pošte organizacije neće označavati napadnute dokumente.
- **Kompromitirani tokeni:** Digitalni kriminalci pokušavaju ugroziti API tokene ili tokene sesija. Uspjeh u tom pogledu omogućio bi im krađu pristupa računu e-pošte, web mjestu SharePoint ili drugom resursu**.**
- **Prikupite obavijesti o odsutnosti ureda:** Napadačima je potrebno puno podataka kako bi poslali uvjerljivu kampanju *spear phishinga*. Jedan od načina na koji to mogu učiniti je masovnim slanjem e-pošte zaposlenicima i prikupljanjem obavijesti o odsutnosti kako bi se naučio format adresa e-pošte koje koriste interni zaposlenici.
- **Istraživanje društvenih medija:** Zlonamjerni napadači moraju naučiti tko radi u ciljanoj tvrtki. To mogu učiniti pomoću društvenih mreža kako bi istražili strukturu organizacije i odlučili koga bi željeli izdvojiti za svoje ciljane napade.

CEO prevara *Whaling*

- Spear phishing napadači mogu ciljati bilo koga u organizaciji, čak i rukovoditelje. To je logika iza napada "*kitolov*". U tim prijevarama prevaranti pokušavaju napasti rukovoditelje i ukrasti njihove podatke za prijavu.
- U slučaju da se njihov napad pokaže uspješnim, prevaranti mogu odabrati provođenje CEO prevare. Kao druga faza prijevare s poslovnim e-poštom (BEC), CEO prevara je kada napadači zloupotrijebe ugroženi račun e-pošte izvršnog direktora ili drugog visokog rukovodstva kako bi odobrili lažne bankovne prijenose financijskoj instituciji po njihovom izboru.

Tehnike korištene u whaling

- **Infiltriranje u mrežu:** Ugroženi račun rukovoditelja učinkovitiji je od lažnog računa e-pošte. Digitalni napadači koriste zlonamjerni softver i root-kitove za infiltriranje u mrežu svoje mete. *Rootkit je zlonamjerni softver koji neovlaštenom korisniku omogućuje privilegirani pristup računalu i ograničenim dijelovima softvera. Rootkit može sadržavati brojne zlonamjerne alate kao što su keyloggeri, kradljivci bankovnih vjerodajnica, kradljivci lozinki, isključenje antivirusa i botovi za DDoS napade*.
- **Praćenje telefonskog poziva: N**apadač prati e-poštu CEO-a telefonskim pozivom koji je potvrdio zahtjev za e-poštom. Ova taktika socijalnog inženjeringa pomogla je ublažiti strahove mete da bi moglo doći do nečeg sumnjivog.
- **Praćenje lanca opskrbe:** Osim toga, zlonamjerni napadači koriste informacije dobavljača kako bi im se e-poruke o CEO-a činile kao da dolaze od pouzdanih partnera**.**

"DIREKTORSKA" PRIJEVARA

"Direktorska" prijevara događa se kada je zaposlenik koji je ovlašten za provođenje plaćanja prevaren na način da plati lažni račun ili provede neovlašteni prijenos s računa tvrtke.

KAKO SE TO RADI?

Prevarant zove ili šalje poruke predstavljajući se kao direktor ili član uprave tvrtke.

Dobro poznaju organizaciju tvrtke.

Traže hitno provođenje plaćanja.

Koriste fraze kao "povjerljivost", "tvrtka ima povjerenje u vas", "trenutno sam nedostupan".

Kažu da se radi o osjetljivoj situaciji (npr. porezna kontrola, preuzimanje i spajanje poduzeća).

Od zaposlenika se traži da ne slijedi redovne autorizacijske postupke.

Upute o tome kako postupiti mogu se dati kasnije, putem treće osobe ili e-pošte.

Zaposlenik prenosi sredstva na račun koji kontrolira prevarant.

Često se zahtjev odnosi na međunarodna plaćanja bankama izvan Europe.

KAKO PREPOZNATI ZNAKOVE?

- Neočekivani poziv/poruka
- Izravni kontakt od visokog dužnosnika u tvrtki s kojim obično niste u kontaktu
- Zahtijeva se apsolutna povjerljivost
- Pritisak i uvjeravanje u hitnost
- Neuobičajen zahtjev u suprotnosti s internim postupcima
- Prijetnje, neobična laskanja ili obećanja nagrade

ŠTO MOŽETE UČINITI?

KAO TVRTKA

Budite svjesni rizika i pobrinite se da **zaposlenici budu informirani i upoznati**.

Potaknite zaposlenike da budu **oprezni sa svim zahtjevima za plaćanje.**

Provoditi interne protokole vezane uz plaćanja.

Propisati postupak provjere legitimnosti zahtjeva za plaćanjem primljenih putem e-pošte.

Uspostaviti **pravila za izvještaje** o prijevarama.

Pregledajte informacije objavljene na stranicama svoje tvrtke, **ograničite informacije i pripazite** na društvene medije.

Nadogradite i ažurirajte tehničku sigurnost.

Uvijek se obratite policiji u slučaju pokušaja prijevare, čak i ako niste postali žrtvom.

KAO ZAPOSLENIK

Strogo poštujte sigurnosne postupke za plaćanja i nabave. **Ne preskačite niti jedan korak i ne popuštajte pritisku**.

Uvijek **pažljivo provjeravajte adrese e-pošte** kada se radi o osjetljivim informacijama ili prijenosu sredstava.

U slučaju sumnje o nalogu za prijenos, **obratite se nadležnom kolegi**.

Nikad ne otvarajte sumnjive poveznice ili privitke primljene putem e-pošte. Budite posebno oprezni kada čitate svoju privatnu e-poštu na računalima tvrtke.

Ograničite informacije i budite oprezni s obzirom na društvene medije.

Izbjegavajte dijeljenje informacija o internoj organizaciji tvrtke, sigurnosti i procedurama.

Ako primite sumnjivu e-poštu ili poziv, uvijek obavijestite IT odjel.

Ostali oblici socijalnog inženjeringa

Vishing

- Vishing se odnosi na krađu identiteta putem telefonskih poziva
- Budući da se glas koristi za ovu vrstu krade identiteta, ona se naziva vishing > voice + phishing = vishing

Smishing

- SMS phishing je jedan od najlakših vrsta phishing napada.
- Korisnik je ciljan pomoću SMS obavijesti koja sadrži izravnu poruku iii detalj iz lažne narudžbe s poveznicom za otkazivanje
- Na poveznici se nalazi lažna stranica dizajnirana za prikupljanje osobnih podataka.

Catphishing

- Catphishing je vrsta online obmane/prevare u kojoj osoba stvara lažni profil na društvenim mrežama odnosno izmišlja postojanje neke osobe s ciljem mamljenja neke stvarne osobe u vezu – obično romantičnu - kako bi izmamila novac, darove ili samo pažnju
- Može poslužiti i kao lažni odnos s ciljem dobivanja informacija ili pristup određenim resursima na koje osoba žrtva ima pravo

Kako izbjeći phishing?

Budite oprezni pri čitanju svih poruka e-pošte - od stranaca i prijatelja.

Budite oprezni pri IKT komunikaciji (e-pošti, oglasima, telefonskim pozivima, itd.) - pa čak i fizičkoj pošti – u kojoj se traže financijske informacije.

Nemojte kliknuti na "omogući sadržaj" (koji omogućuje makronaredbe) u dokumentima sustava Microsoft Office.

Pazite na poruke e-pošte sa službenim pozdravom ("Poštovani klijenti"), lošom gramatikom ili pravopisnim greškama - i budite na oprezu ako primijetite nešto sumnjivo jer su negativci svakom kampanjom sve pametniji.

Budite izuzetno oprezni pri komunikaciji putem društvenih mreža jer lažni identiteti i profili služe kao alat za prijevaru.

Ne otvarajte poveznice u e-pošti, aplikacijama za dopisivanje ili oglasima. Istražite svaku poveznicu svim dostupnim sredstvima.

Razmislite prije klikanja – svaki put za svaku poruku.

Dvostruko provjerite izvor e-pošte kako biste se uvjerili da je legitiman.

Pažljivo **provjerite** prije otvaranja poruke ili priložene datoteke iz vaše banke.

Omogućite i upotrebljavajte multifaktorsku autentifikaciju kada god možete. Multifaktorska autentifikacija može spriječiti preuzimanje računa.

Zaštita

Sigurnosni program

- Program sigurnosti je skup dokumenata (koji određuju sigurnosne mjere), procedura (koje određuju načine primjene tih sigurnosnih mjera) i funkcija (koje primjenjuju procedure programa sigurnosti, te njime upravljaju)
- Sigurnosni program podrazumijeva uspostavu programa sigurnosti:
- Mora biti organiziran u skladu sa zahtjevima kibernetičke sigurnosti
- Mora imati uspostavljenu odgovarajuću funkcionalnu strukturu te delegira ovlasti kako bi se osigurala primjerena uspostava, upravljanje i nadzor provedbe programa sigurnosti
- Svi na koje se odnosi sigurnosna politika moraju pružiti potporu provedbi programa sigurnosti
- Program sigurnosti mora se odnositi na sve aspekte sigurnosti informacijskog sustava
- Program sigurnosti mora se primjenjivati se na cjelokupan informacijski sustav, sve njegove dijelove i informacijsku imovinu
- Osim ako to nije drukčije specificirano zakonskim propisima iii međunarodnim sporazumima
- Program sigurnosti odnosi se na sve djelatnike, suradnike i vanjske partnere koji imaju pristup informacijskoj imovini koju sigurnosni program štiti

Opće metode zaštite

Antivirus/antispyware/antimalware

- Sigurnosna rješenja za prepoznavanje i zaustavljanje aktivnosti zlonamjernog sadržaja koja su obavezan dio programske opreme računala
- Neka rješenja dolaze u paketima s drugim sigurnosnim alatima (npr. vatrozidom), dok su neka samostalna
- Danas je na internetu moguće pronaći niz besplatnih antivirusnih alata koji zadovoljavaju različite kategorije korisnika

Vatrozid

- Aplikacija koja ograničava mrežnu komunikaciju između računala i Interneta
- Vatrozid selektivnim propuštanjem prometa izbjegava neovlaštenu komunikaciju i smanjuje mogućnost iskorištavanja sigurnosnih propusta u aplikacijama koje ne koristite, a koje imaju mogućnost mre2ne komunikacije

Opće metode zaštite

Automatsko ažuriranje operacijskog sustava i aplikacija

- Sigurnosni propusti u programima stalno se otkrivaju
- Kako bi zaštitili računalo, va2no je uključiti automatsko ažuriranje u operacijskom sustavu i svim aplikacijama koje dolaze u kontakt sa sadržajima s interneta (npr. preglednici PDF dokumenata)
- Operacijski sustav Windows promatra je li automatsko ažuriranje operacijskog sustava uključeno te upozorava korisnika ako nije

Složene i različite lozinke

- Današnja su računala dovoljna snažna da mogu iznimno brzo isprobavati različite kombinacije imena i lozinki pa su zato lozinke koje sadrže riječi iz govornog jezika, datume, imena i slično iznimno jednostavne za pogađanje
- Dobra lozinka sastoji se od najmanje 12 znakova, te je kombinacija velikih i malih slova, brojki te specijalnih znakova

Pravila za dobru lozinku

- 1. Neka bude sačinjena od **najmanje 8 znakova**.
- 2. Treba sadržavati: velika i mala slova, brojeve i interpunkcijske znakove koje dozvoljava internet stranica.
- 3. Ne koristite:
  - 123456, ili kombinaciju tih brojeva,
  - kombinaciju imena i prezimena,
  - kombinaciju imena i godine rođenja,
  - "Qwerty" ili drugi slijed slova na tipkovnici,
  - najgori izbor: "lozinka".
- 4. Ne koristite samo jednu lozinku za sve korisničke račune. Napravite različite lozinke za e-mail, Facebook, forume, on-line bankarstvo, itd. S obzirom na opseg našeg digitalnog života to je gotovo nemoguće, jer bi se morali sjetiti puno lozinki. Zato pokušajte napraviti hijerarhiju usluga. Za najvažnije internetske usluge, na primjer on-line bankarstvo, koristite snažne i jedinstvene lozinke, a za manje važne stranice možete "reciklirati" iste lozinke, uz neke manje prilagodbe.
- 5.Nemojte čuvati pisane lozinke pokraj računala
- Za čuvanje lozinaka možete koristiti posebne programe za upravljanje lozinkama (tzv. Password Manager), na primjer KeePass, LastPass itd.
- *Lozinka štiti, štiti i četkica za zube - nemojte ih posuđivati, i mijenjajte ih redovito!*

Kako zapamtiti dobru lozinku

- Već neko vrijeme dobra lozinka nije nužno samo jedna riječ - može se koristiti cijela rečenica koju ćete lakše zapamtiti: DanasJeLijepDan9. Naravno, s obzirom da smo ju napisali ta lozinka više nije pogodna za korištenje.
- Recept: Uzmite samo prva slova neke fraze ili stiha, koja ćete lako zapamtiti, te dodajte brojeve i velika slova. Primjer: Na planini sunce sja - **20Npss13**.
- Možete izmisliti svoj vlastiti algoritam, npr. od korisničkog imena, naziva internetske usluge te dodatnih znakova stvorite jedinstvenu lozinku za svaku uslugu.

TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

Opće metode zaštite

Sigurnosne kopije i njihova pohrana

- Danas je korištenje računala u poslovne svrhe potpuno uobičajena stvar te velika većina korisnika na računalu pohranjuje važne i povjerljive podatke čiji bi gubitak predstavljao značajan udarac na poslovanje ili privatnost
- Ovom je problemu veoma lako doskočiti izradom sigurnosnih kopija i pohranom tih kopija ili na specijalizirane internetske servise ili na vanjske medije koji nisu povezani mrežom

Informiranje o kibernetičkoj sigurnosti

- Kako bi se znali zaštititi, važno je biti upoznat s prijetnjama
- Postoji niz specijaliziranih internetskih portala koji svakodnevno pišu o zanimljivostima iz svijeta kibernetičke sigurnosti

Rukovanje podacima

- Internet omogućuje kupovinu roba i usluga iz udobnosti doma korištenjem kreditne kartice ili nekog drugog servisa za internetsko plaćanje
- Takve su stranice posebno atraktivna meta za napadače i moramo biti na posebno oprezni kada upisujemo svoje povjerljive podatke na internetskim stranicama jer ih vješt napadač može presresti i iskoristiti ih kako bi stekao novčanu ili neku drugu dobit
- •Stranice na koje upisujemo osobne podatke moraju koristiti HTTPS protokol

Lažne web stranice (phishing)

Kako prepoznati *phishing web* stranice?

Lažnim predstavljanjem putem web stranica koje na prvi pogled izgledaju kao prave stranice prevaranti će te pokušati navesti da upišeš svoje Njuškalo pristupne podatke (korisničko ime i lozinku), osobne podatke ili podatke platnih/bankovnih kartica.

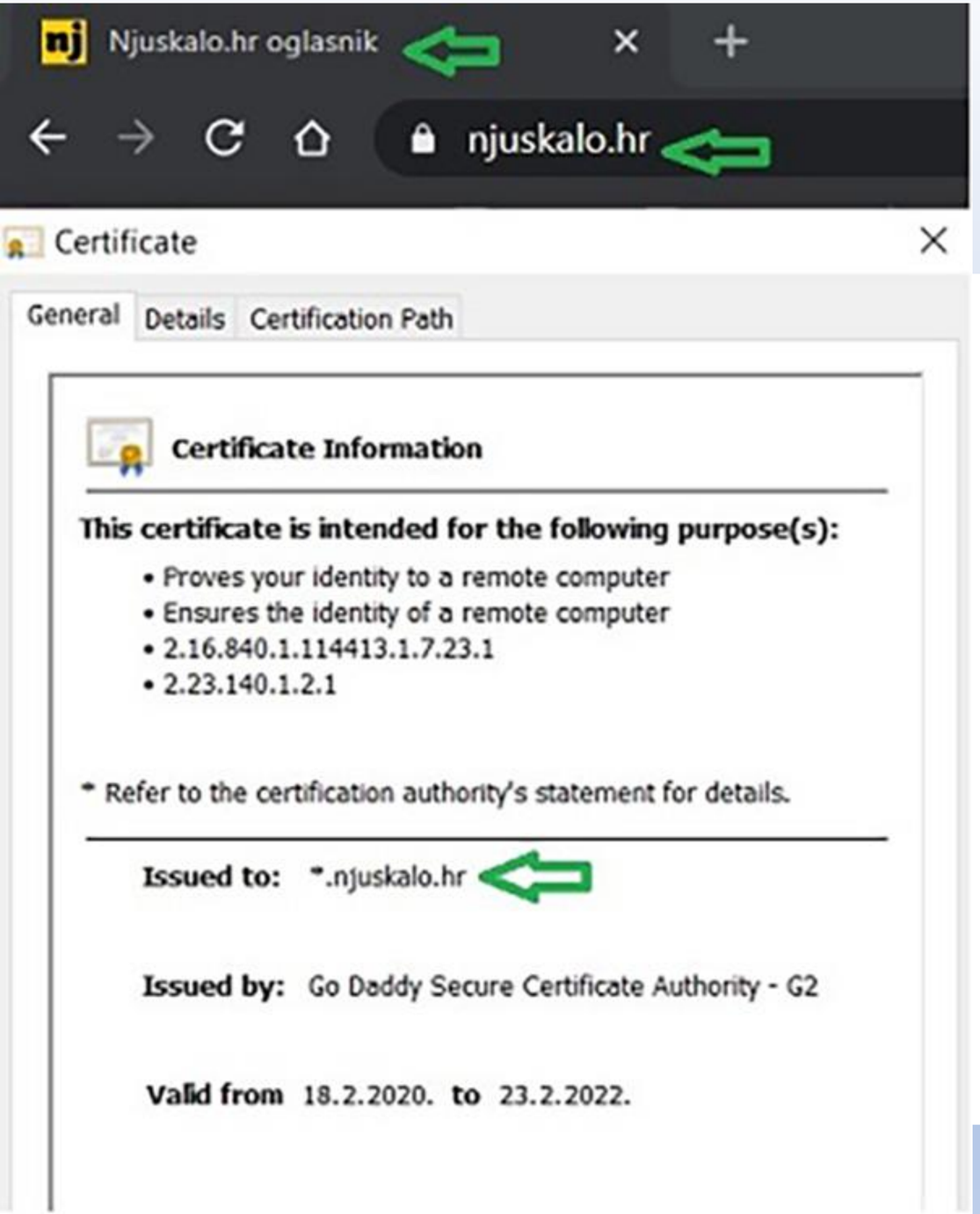
Ovi podaci mogu se iskoristiti dalje za krađu identiteta i razne prijevare, a prevaranti te mogu navesti i da preuzmeš i instaliraš zlonamjerni program koji će iskoristi da kompromitiraju tvoje računalo tebe osobno. Takvim prijevarama mogu te ciljati kroz razne digitalne kanale za komunikaciju (primjerice, Viber, WhatsApp i Facebook poruke), uključujući i e-mail.

Ako ti se poruka čini sumnjivom, na vrijeme prepoznaj nalaziš li se na pravoj stranici.

Kako prepoznati Njuškalove web stranice?

Njuškalo web mjesta i web stranice uvijek u pregledniku imaju sve ove elemente:

- **Njuškalov logo**
- **Ispravnu domenu njuskalo.hr**
- **Ispravan certifikat kojeg možeš vidjeti klikom na lokot**



Certifikat koji se koristi na stranici može biti izdan za Njuškalo domenu *.njuskalo.hr ili za neku Njuškalovu stranicu, primjerice turizam.njuskalo.hr.

Primjeri ispravnih veza/linkova na Njuškalo stranice:

- **https://www.njuskalo.hr**
- **https://turizam.njuskalo.hr**
- **https://popusti.njuskalo.hr/k/drogerija**

Kako prepoznati lažne stranice?

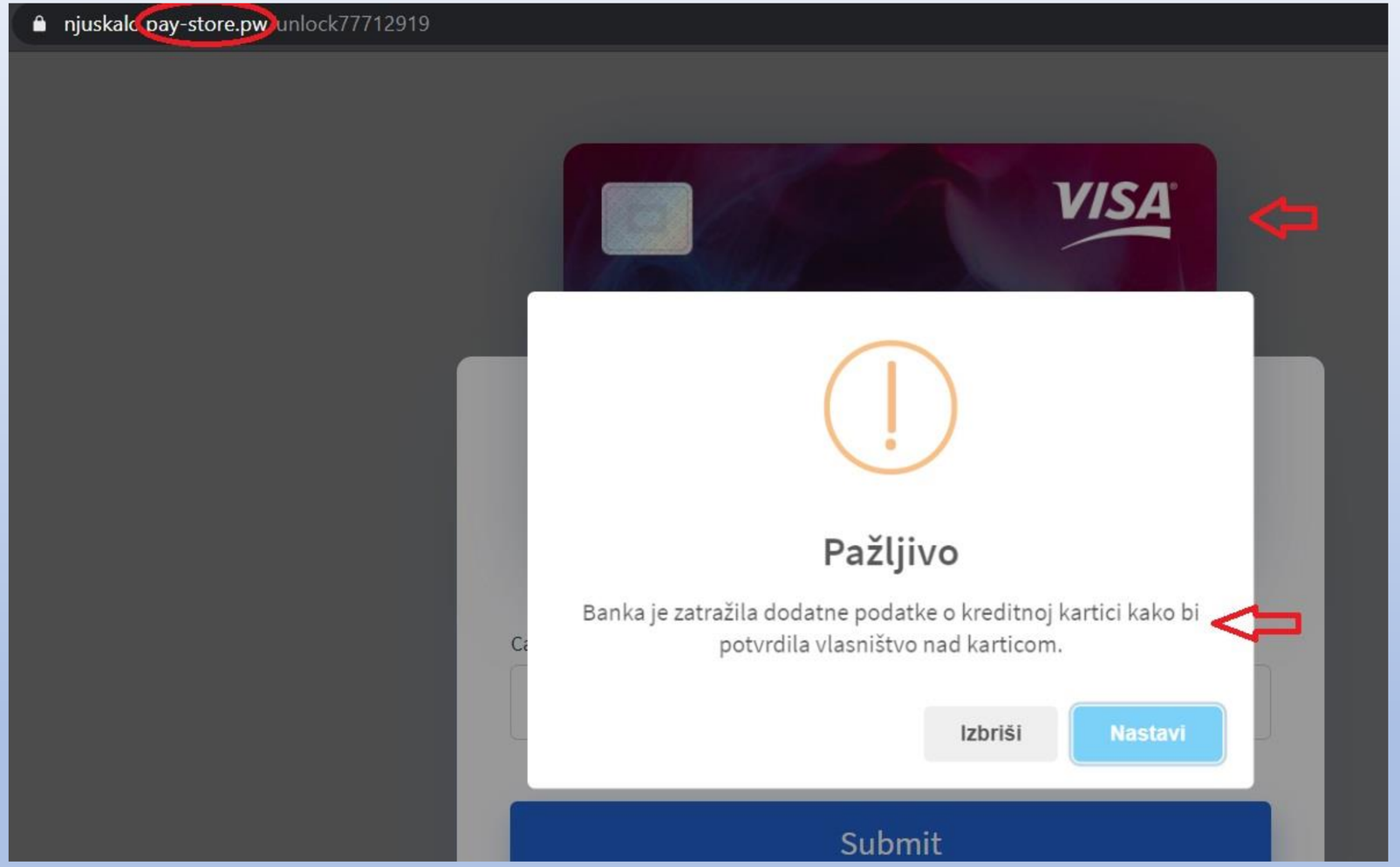
Na lažnoj web stranici prevaranti će te neovlaštenim korištenjem Njuškalo vizuala pokušati uvjeriti da je to prava stranica ili te pokušati uvjeriti da se radi o novoj Njuškalovoj usluzi, primjerice novom načinu plaćanja.

Kako bi te naveli u zabludu, veza (URL) i izgled stranice uvijek su što bolja kopija Njuškalovih pravih stranica, prepoznaj ih i javi nam ako imaš bilo kakvu sumnju u ispravnost stranice koja ti je stigla putem bilo kojeg kanala.

Primjeri veza/linkova na lažne Njuškalo stranice::

- **http://Njuskalo.hr.prijava.pay.info**
- **https://Uplata.Njuskalo-pay.site**
- **https://User.Njuskalo-prijava.com**
- **https://Njuskalo.placanje.com**


12:51
njuskalo.delivery-pay.pw
njuškalo
Primanje sredstava
Bolt
Festina sat
300 HRK
Puno ime
Adresa dostave
Nakon primanja sredstava na vašu karticu, pošaljite robu kupcu u skladu s navedenim podacima, dostupne točke otpreme možete pogledati na službenoj web stranici.


njuskalo.pay-store.pw/unlock77712919
VISA
Pažljivo
Banka je zatražila dodatne podatke o kreditnoj kartici kako bi potvrdila vlasništvo nad karticom.
Izbriši
Nastavi
Submit

Kako prepoznati lažne e-mailove?

U komunikaciji e-mailom pošiljatelj se može lažno predstavljati (*spoofing*) sa ciljem prijevare. Lažnim e-mailom distribuiraju se zlonamjerni programi, prikupljaju se valjane e-mail adrese ili se traže povjerljive informacije primatelja (*phishing*).

Ne postoji jedinstveni način zaštite od ovakvih pokušaja prijevara, ali postoji par znakova koji te mogu na to upozoriti.

Kako prepoznati lažni *e-mail*?

Lažni e-mail može izgledati kao originalni Njuškalov, a uključuje linkove na lažne web stranice ili lažne usluge za koje tvrde da su potvrđene od strane Njuškala. Takve e-mailove često možeš prepoznati po:

- pravopisnim i gramatičkim greškama
- upozorenju o zatvaranju ili brisanju korisničkog računa, kartice ili sl.
- traženju osobnih podataka
- zastrašujućem tonu poruke i naglaskom na hitnu reakciju
- sadržaju e-maila koji sadrži samo privitak

Primjer lažnog *e-maila*:

Iz teksta se razaznaje da se ne radi o legitimnom e-mailu, adresa pošiljatelja je nepoznata, adresa primatelja je vaša ili je prazno. Sadrži privitak, sadržaj i naziv privitka može se mijenjati.

From: Njuskalo [mailto: može biti bilo koja e-mail adresa]
Sent: Tuesday, January 26, 2016 12:00 AM
To: vaša e-mail adresa ili prazno
Subject: Ste dobili vaučer!
Halo!

Ste primili vaučer!
Da biste iskoristili to sada, preuzmite privitak.

Primjer *phishing e-maila*:

Phishing e-mailovi obično ti kažu da je tvoj Njuškalo račun blokiran, zaključan ili ugašen. Može čak sadržavati link koji je identičan Njuškalovom, ali kada klikneš na taj link, odvede te na phishing web stranicu. Radi svoje sigurnosti, uvijek provjeri web adresu nakon što klikneš na bilo kakav link u *e-mailu*.

From: Njuskalo.hr [mailto:info@njuskalo.hr]
Sent: Tuesday, November 04, 2014 2:42 PM
To:
Subject: UPOZORENJE: Pronasli smo e-mail PhishTank. Provjerite pojedinosti svog racuna

Pozdrav ,

Vas racun njuskalo.hr je blokiran iz sigurnosnih razloga.

Otkrili smo neovlašteno prijavu iz druge IP adrese.

Pronasli smo e-mail PhishTank. Provjerite pojedinosti svog racuna.

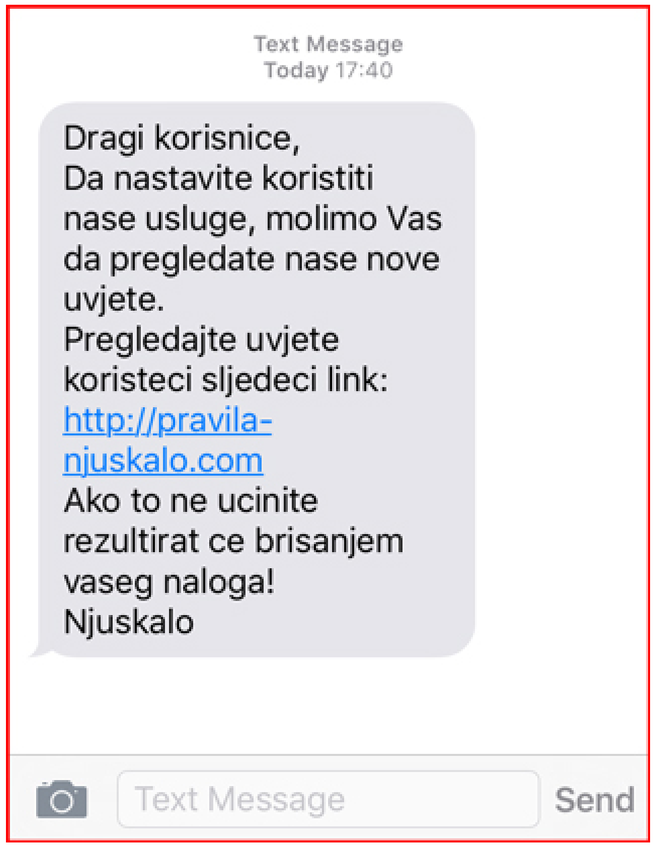
Da bi zastitili svoj racun od PhishTank, molimo Vas da potvrdite pojedinosti svog racuna , molim klikni ovdje

U slucaju da ne potvrdite svoj racun u 24 sata, to ce biti izbrisani.

Zelim ti puno uspjeha.

Njuskalo.hr

Primjer lažnog SMS-a :



Phishing SMS-ovi obično ti kažu da je tvoj Njuškalo račun blokiran, zaključan, ugašen, te traži hitnu potvrdu tvojih podataka ili prihvaćanje pravila i uvjeta oglašavanja. Može sadržavati link koji je identičan Njuškalovom, ali kada klikneš na taj link, odvede te na phishing web stranicu. Radi svoje sigurnosti, uvijek provjeri ispravnost web stranice nakon što klikneš na bilo kakav link u SMS-u ili nazovi našu korisničku podršku ukoliko nisi siguran.

Njuškalo **nikada** neće tražiti potvrdu podataka ili uvjeta oglašavanja putem SMS poruke te prihvaćanje istih uvjetovati brisanjem računa ili deaktivacijom korisnika.

Kako prepoznati lažne SMS poruke?

U komunikaciji SMS-om pošiljatelj se može lažno predstavljati (spoofing) sa ciljem prijevare. Lažnim SMS porukama distribuiraju se zlonamjerni program ili se traže povjerljive informacije primatelja.

Ne postoji jedinstveni način zaštite od ovakvih pokušaja prijevara, ali postoji par znakova koji te mogu na to upozoriti.

Kako prepoznati lažni SMS?

Lažni SMS može izgledati kao poruka koju je poslao Njuškalo, a uključuje linkove na lažne web stranice ili lažne usluge za koje tvrde da su potvrđene od strane Njuškala. Takve SMS-ove često možeš prepoznati po:

- pravopisnim i gramatičkim greškama
- upozorenju o zatvaranju ili brisanju korisničkog računa, kartice ili sl.
- traženju osobnih podataka

08:39

+380 68 968 5069

BLOKIRAJ | DODAJ

DANAS

Poruke i pozivi zaštićeni su potpunom enkripcijom. Nitko izvan ovog razgovora, čak ni WhatsApp, ne može ih pročitati niti poslušati. Dodirnite da biste saznali više.

Zdravo, Jos nije prodano? 07:20

Sto to? 07:21

Bmw e90 prekidaci, zavojnica-spula volana 07:21

Imam 07:21

Ostala mi je jos jedna pa ako ste iz zg mogu vam je dostaviti kad idem ba posao 07:23

Kakvo stanje? Ima li nedostataka? 08:00

Rabljeno. Nema 08:15

Ocuvano i sve radi bez greske 08:15

Napišite poruku

08:39

+380 68 968 5069

Dobro kupujem! 08:25

Sigurna dostava - Kontakt i Pomoć - Njuskalo.hr
www.njuskalo.hr

Možete li poslati kurirsku dostavu putem usluge njuskalo? ja ću platiti po kartici, nakon što je kurir će doći k vama

https://www.njuskalo.hr/index.php?ctl=help&topic_id=1&section_id=1&content_id=231 08:25

Odgovara li vam ova opcija? 08:25

Od kud ste? 08:27

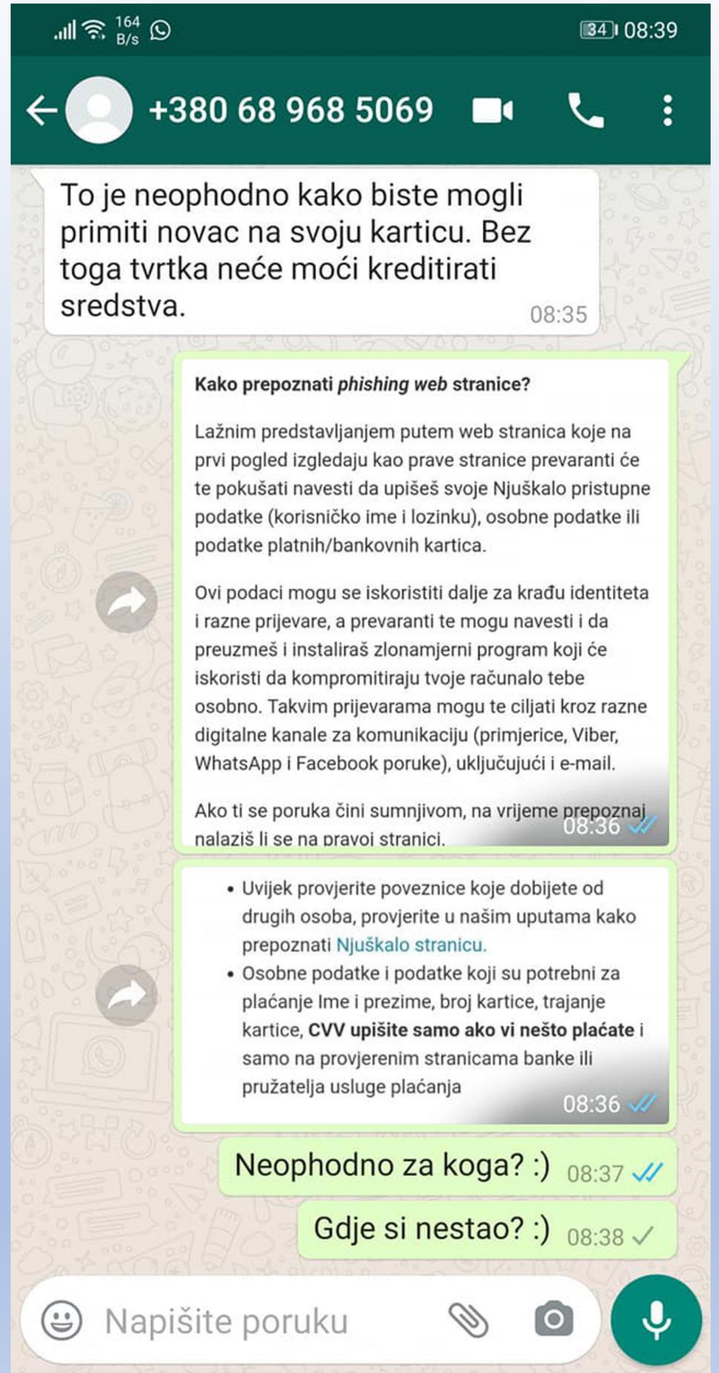
Hercegovačka ul. 23, 21000, Split. 08:27

Meni je svejedno, kak vama odgovara 08:27

Opcija koju sam predložio vrlo mi odgovara. Dogovaram dostavu i plaćam. Plaćate za svoj predmet i brod. Po primitku provjeravam 08:28

Napišite poruku


+380 68 968 5069
Vrlo je jednostavno i sigurno. Mogu organizirati dostavu i poslati vam vezu za primanje sredstava 08:29
Pogledajte kako to izgleda 08:29
No nadam se da je isti princip kao pouzecem 08:29
Moze 08:30
https://njuskalohr-safedeal.shop/tracks/1703235148 08:31
Gotovo 08:31
Hej ali tu me trazi cvv? To ti necu upisati jer se to stavlja samo prilikom placanja. 08:35
Dovoljan je broj racuna ili iban 08:35
To je neophodno kako biste mogli primiti novac na svoju karticu. Bez toga tvrtka neće moći kreditirati sredstva. 08:35
Kako prepoznati phishing web stranice?
Napišite poruku


+380 68 968 5069
To je neophodno kako biste mogli primiti novac na svoju karticu. Bez toga tvrtka neće moći kreditirati sredstva. 08:35
Kako prepoznati phishing web stranice?
Lažnim predstavljanjem putem web stranica koje na prvi pogled izgledaju kao prave stranice prevaranti će te pokušati navesti da upišeš svoje Njuškalo pristupne podatke (korisničko ime i lozinku), osobne podatke ili podatke platnih/bankovnih kartica.
Ovi podaci mogu se iskoristiti dalje za krađu identiteta i razne prijevare, a prevaranti te mogu navesti i da preuzmeš i instaliraš zlonamjerni program koji će iskoristi da kompromitiraju tvoje računalo tebe osobno. Takvim prijevarama mogu te ciljati kroz razne digitalne kanale za komunikaciju (primjerice, Viber, WhatsApp i Facebook poruke), uključujući i e-mail.
Ako ti se poruka čini sumnjivom, na vrijeme prepoznaj nalaziš li se na pravoj stranici. 08:36
Uvijek provjerite poveznice koje dobijete od drugih osoba, provjerite u našim uputama kako prepoznati Njuškalo stranicu.
Osobne podatke i podatke koji su potrebni za plaćanje Ime i prezime, broj kartice, trajanje kartice, CVV upišite samo ako vi nešto plaćate i samo na provjerenim stranicama banke ili pružatelja usluge plaćanja 08:36
Neophodno za koga? :) 08:37
Gdje si nestao? :) 08:38
Napišite poruku

Hvala na pažnji

Daniel Bara, Ph.D. | LinkedIn