CERT.hr

#SurfajSigurnije

Radionica za podizanje svijesti o kibernetičkoj sigurnosti

Autor: CERT.hr

Sadržaj

- Prijetnje kibernetičkoj sigurnosti
  - Akteri u kibernetičkoj sigurnosti
    - Hakeri i haktivizam
    - Hakerske skupine
    - Državno potpomognuti napadi
    - Zlonamjerni sadržaj
  - Zlonamjerni sadržaj
  - Socijalni inženjering
  - Zaštita

Prijetnje kibernetičkoj sigurnosti

- Prijetnje kibernetičkoj sigurnosti danas predstavljaju prijetnje svim oblicima sigurnosti
  - Vojna
  - Politička
  - Ekonomska
  - Društvena
  - Ekološka
- Svaki od navedenih sektora može biti pogođen kibernetičkim napadom
- Kibernetička sigurnost je temelj sigurnosti digitalnog društva

Akteri u kibernetičkoj sigurnosti

- Razlikujemo tri razine aktera u kibernetičkoj sigurnosti
  - Hakeri
  - Hakerske skupine
  - Državno potpomognute skupine
- Prikupljanje informacija o akterima
  - Strateško – usmjereno na informacije o namjerama, motivacijama, sposobnostima i planovima zlonamjernih aktera
  - Taktičko – usmjereno na razumijevanje taktika, tehnika i procedura kojima se zlonamjerni akteri služe
  - Operacijsko – usmjereno na usporedbu podataka u svrhu otkrivanja je li do napada već došlo ili bi do njega moglo doći

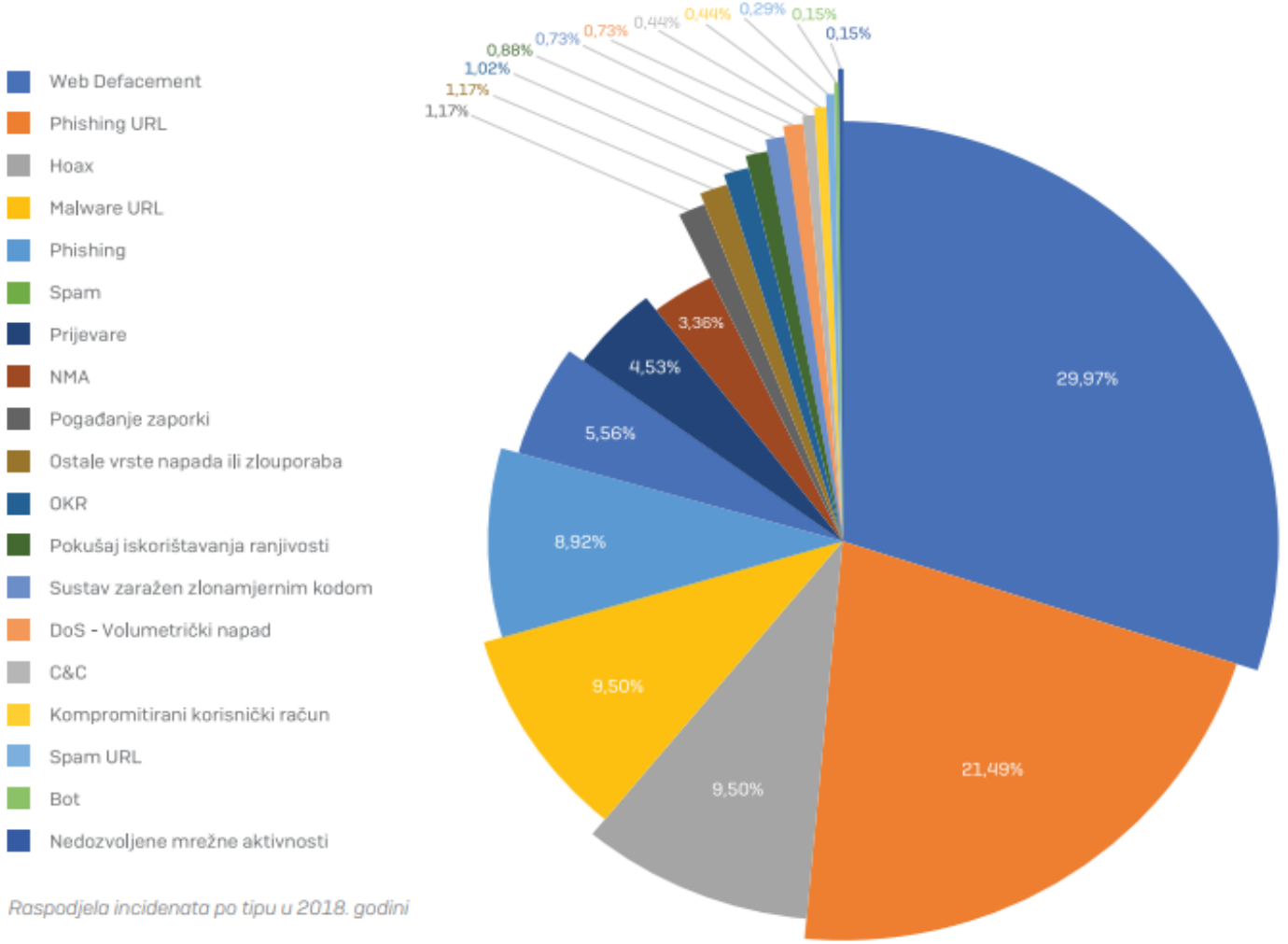
Akteri u kibernetičkoj sigurnosti

- Haker je bilo koja osoba s visokom razinom znanja o računalnim sustavima koja to znanje koristi kako bi riješila problem
  - Black hat – pojedinci koji svoje znanje o informacijskokomunikacijskim sustavima koriste na zlonamjeran način. Često su tvorci zlonamjernih sadržaja kojima žele ukrasti neke podatke ili ih izmijeniti, a mnogi od njih rade isključivo zbog novčane dobiti
  - White hat – etički hakeri koji svoje znanje koriste kako bi povećali razinu sigurnosti nekog sustava. Iz nesebičnih i dobronamjernih razloga pronalaze sigurnosne propuste te ih prijavljuju. Svojim radom brinu o sigurnosti mnogih sustava te razvijaju inovativna sigurnosna rješenja
  - Grey hat – pojedinci s velikim znanjem o načinu rada informacijsko-komunikacijskih sustava koji su kombinacija black i white hat-a. Iako vlastite vještine i znanja često ne koriste za osobni dobitak, mogu imati dobre i loše namjere
- Hakerske skupine
  - Organizirani kriminal
  - Najčešće motivirani novčanom dobiti
- Državno potpomognute skupine
  - Dobro financirane skupine koje izvode složene i precizne napade
  - Najčešće motivirani političkim, ekonomskim, tehnološkim i vojnim ciljevima

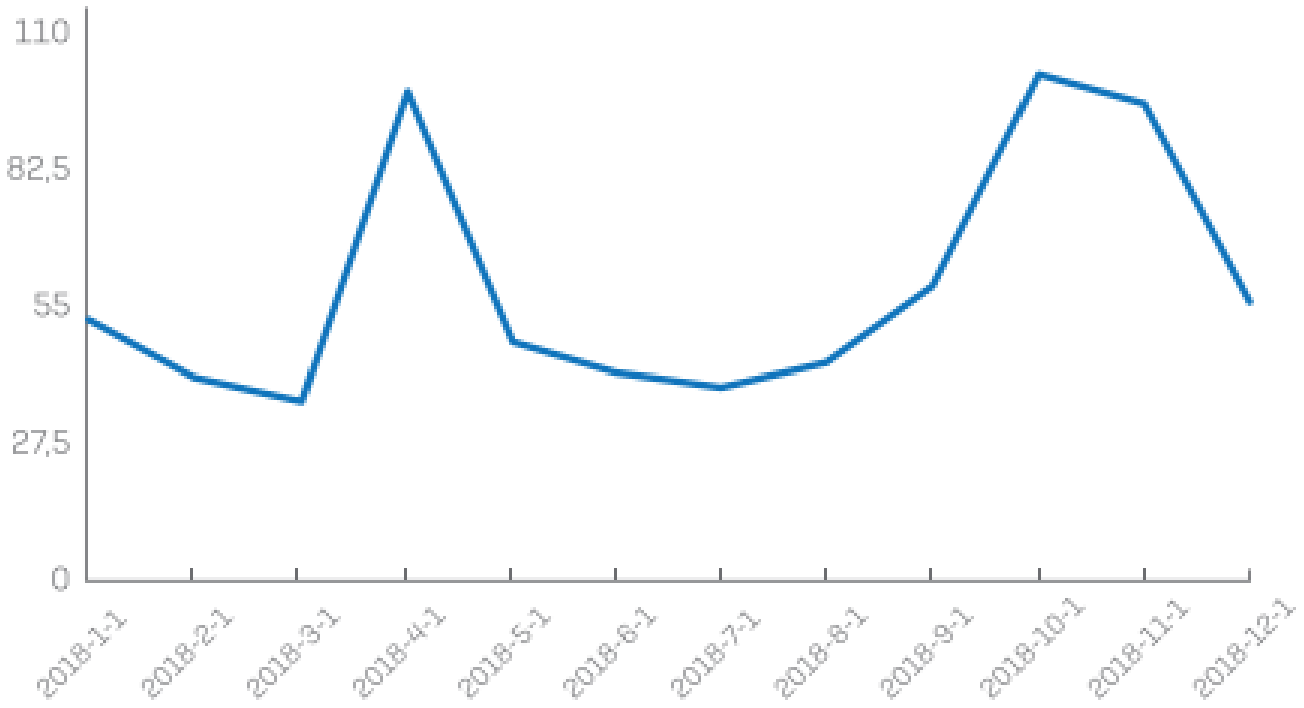
grow-cert

CERT.hr

Zlonamjerni sadržaj



Raspodjela incidenata po tipu u 2018. godini



Broj incidenata koje je 2018. godine obradio Nacionalni CERT s prikazom po mjesecima

TIP INCIDENTA	BROJ	TREND
Web defacement	205	▼
Phishing URL	147	▲
Hoax	65	–
Malware URL	65	▲
Phishing	61	▲
Spam	38	▲
Prijevare	31	–
NMA	23	▼
Pogađanje zaporki	8	–
Ostale vrste napada ili zlouporaba	8	▼
OKR	7	▲
Pokušaj iskorištavanja ranjivosti	6	–
Sustav zaražen zlonamjernim kodom	5	–
DoS - Volumetrički napad	5	▼
C&C	3	▲
Kompromitirani korisnički račun	3	–
Spam URL	2	▼
Bot	1	▼
Nedozvoljene mrežne aktivnosti	1	▼
UKUPNO	684	▼

Prikaz incidenata po tipu u 2018. godini

Prikaz popularnih vrsta zlonamjernih sadržaja

- Zlonamjerni ransomware sadržaj
  - Naziv za skup zlonamjernih programa koji korisniku onemogućuju korištenje računala
  - Nakon zaraze zlonamjerni ransomware sadržaj može šifrirati datoteke ili onemogućiti njihovo korištenje tako da se pojavi početni ekran s određenom porukom koju nije moguće maknuti
  - Od korisnika čije je računalo zaraženo 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.

- 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.

- 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 ili 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 ili "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 (ili 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.

- APT (eng. Advanced persistent threat) Malware
  - Advanced persistent threat (APT) je ciljani kibernetički napad kod kojeg zlonamjerna skupina ili osoba stekne neovlašteni pristup mreži i ostaje nezapažena dulje vrijeme
  - Namjera APT napada uglavnom je praćenje aktivnosti na mreži i krađa informacija, a ne prouzrokovanje štete na mreži ili u organizaciji
  - Meta ovih napada su organizacije iz sektora nacionalne obrane, proizvodnje ili financijskog sektora koje obrađuju vrijedne podatke, npr. intelektualno vlasništvo, vojne planove i druge podatke vrijedne za državu ili veliku organizaciju
  - Ovakve vrste napada velikih su razmjera, s naprednim tehnikama i točno određenim ciljem, a motivi za izvođenje ovakvih napada uglavnom su poslovni ili politički
  - Kako bi "upali" u mrežu, napadači se koriste naprednim metodama napada, iskorištavaju "zero-day" ranjivosti, koriste se socijalnim inženjeringom, npr. vrlo dobro pripremljenim ciljanim (spear phishing) napadom itd.
  - Kako bi što dulje nezapaženo ostali u mreži napadači koriste napredne metode poput mijenjanja zlonamjernog koda, neprestanog nadziranja i izvlačenja informacija iz mreže korištenjem naredbenog i kontrolnog sustava i sl.

- Stegware
  - Zlonamjerni program koji se sakrije u sliku, dokument ili čak piksel korištenjem steganografije
  - Steganografija je znanstvena disciplina koja proučava metode skrivanja informacija u naizgled bezazlene objekte
  - Iako se donedavno koristila uglavnom u vojne svrhe kako bi se osigurala tajnost podataka jer osoba kojoj podaci nisu namijenjeni nije svjesna postojanja istih, napadači su steganografiju prepoznali kao odličnu priliku za sakrivanje zlonamjernog sadržaja
  - Velika je prednost za napadače što tradicionalna antivirusna zaštita neće prepoznati zlonamjerni sadržaj
- Zlonamjerno oglašavanje
  - (eng. Malvertising – Malicious advertising)
  - Zlonamjerno oglašavanje je korištenje internetskog oglašavanja u svrhu širenja zlonamjernog sadržaja
  - Najčešće se zasniva na ubacivanju zlonamjernog koda u reklame koje se potom šire putem legitimnih oglašivačkih servisa i internetskih stranica
  - Oglašivački servisi i reklame pružaju dobar temelj za širenje zlonamjernih sadržaja jer su prilagođene korisnicima i pokušavaju ih privući.

- 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 pošte
    - Osim u slučaju e-pošte, 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 pošte 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 te narušavanje njihovog ugleda, kao i ugleda određenih organizacija, tvrtki i poznatih osoba.

Socijalni inženjering

- Kako se socijalni inženjering razvijao kroz povijest?

Socijalni inženjering

- Kako se socijalni inženjering razvijao kroz povijest?

Pozdrav!

Zanimaju Vas novim trendovi u nastavi? Željeli biste svoje ideje podijeliti s kolegama?

Prijavite se putem poveznice!

Otvorite sebi mogućnosti izravne komunikacije s ostalim sudionicima, organizatorima i predavačima na konferenciji Suvremene tehnologije u obrazovanju – STO.

Potražite dodatne materijale, nenajavljena predavanja te okrugle stolove na kojima ćete moći postavljati pitanja poznatim stručnjacima te uz njihovu pomoć razviti svoje ideje te povećati vašu kompetenciju za rad u školama budućnosti.

Tajni kod za prijavu na nasoj stranici glasi: ZnanjeJeUvijekUModi".

Za sva pitanja i dodatne informacije stojimo na raspolaganju.

Vaš STO team!

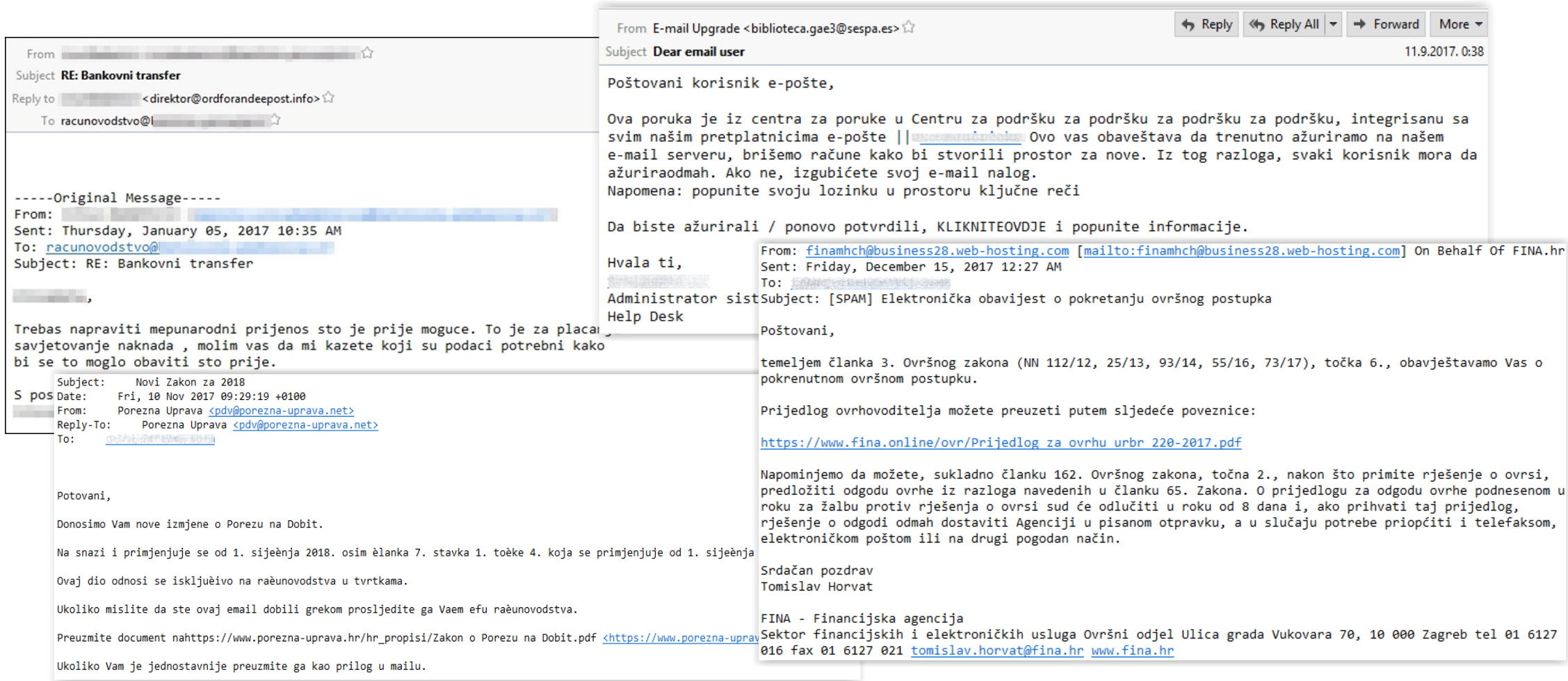
https://goo.gl/qqVwAT

[redacted]

O događanju – CARNet – Suvremene tehnologije u obrazovanju 2017

Krajem mjeseca travnja, točnije 27. i 28. travnja u organizaciji CARNeta, Prirodoslovno-matematičko...

sto.carnet.hr



From [redacted]
Subject **RE: Bankovni transfer**
Reply to [redacted] <direktor@ordforandeepost.info>
To racunovodstvo@[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 05, 2017 10:35 AM
To: racunovodstvo@[redacted]
Subject: RE: Bankovni transfer

[redacted],

Trebas napraviti mepunarodni prijenos sto je prije moguce. To je za placa
savjetovanje naknada , molim vas da mi kazete koji su podaci potrebni kako
bi se to moglo obaviti sto prije.

S pos

From E-mail Upgrade <biblioteca.gae3@sespa.es>
Subject **Dear email user**

Reply | Reply All | Forward | More

11.9.2017. 0:38

Poštovani korisnik e-pošte,

Ova poruka je iz centra za poruke u Centru za podršku za podršku za podršku za podršku, integrisanu sa svim našim pretplatnicima e-pošte || [redacted] Ovo vas obaveštava da trenutno ažuriramo na našem e-mail serveru, brišemo račune kako bi stvorili prostor za nove. Iz tog razloga, svaki korisnik mora da ažuriraodmah. Ako ne, izgubićete svoj e-mail nalog.
Napomena: popunite svoju lozinku u prostoru ključne reči

Da biste ažurirali / ponovo potvrdili, KLIKNITEOVDJE i popunite informacije.

Hvala ti,
[redacted]
Administrator sist
Help Desk

Subject: Novi Zakon za 2018
Date: Fri, 10 Nov 2017 09:29:19 +0100
From: Porezna Uprava <pdv@porezna-uprava.net>
Reply-To: Porezna Uprava <pdv@porezna-uprava.net>
To: [redacted]

Potovani,

Donosimo Vam nove izmjene o Porezu na Dobit.

Na snazi i primjenjuje se od 1. sijeènja 2018. osim èlanka 7. stavka 1. toèke 4. koja se primjenjuje od 1. sijeènja

Ovaj dio odnosi se iskljuèivo na raèunovodstva u tvrtkama.

Ukoliko mislite da ste ovaj email dobili grekom prosljedite ga Vaem efu raèunovodstva.

Preuzmite document nahttps://www.porezna-uprava.hr/hr_propisi/Zakon o Porezu na Dobit.pdf <https://www.porezna-uprav

Ukoliko Vam je jednostavnije preuzmite ga kao prilog u mailu.

From: finamhch@business28.web-hosting.com [mailto:finamhch@business28.web-hosting.com] On Behalf Of FINA.hr
Sent: Friday, December 15, 2017 12:27 AM
To: [redacted]
Subject: [SPAM] Elektronička obavijest o pokretanju ovršnog postupka

Poštovani,

temeljem članka 3. Ovršnog zakona (NN 112/12, 25/13, 93/14, 55/16, 73/17), točka 6., obavještavamo Vas o pokrenutnom ovršnom postupku.

Prijedlog ovrhovoditelja možete preuzeti putem sljedeće poveznice:

https://www.fina.online/ovr/Prijedlog za ovrhu urbr 220-2017.pdf

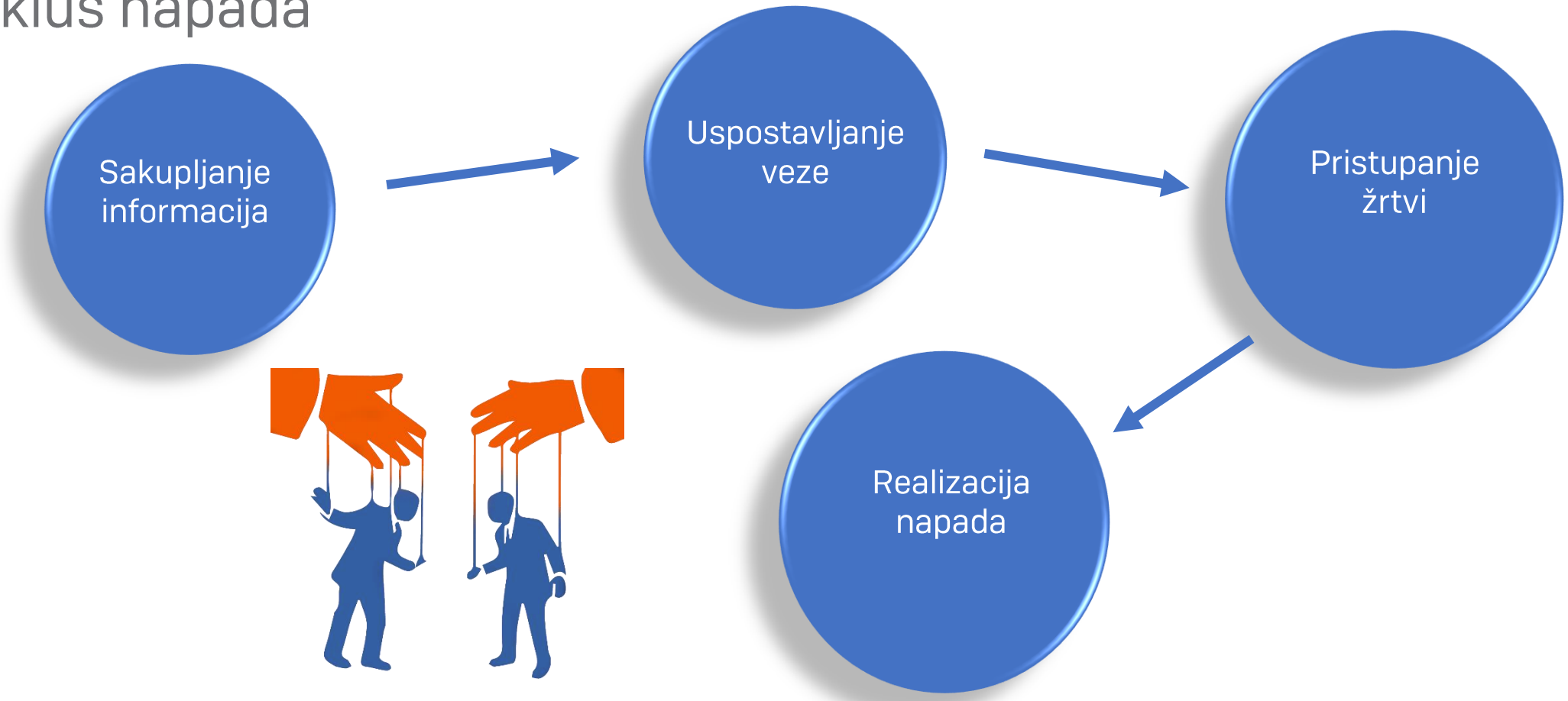
Napominjemo da možete, sukladno članku 162. Ovršnog zakona, točna 2., nakon što primite rješenje o ovrsi, predložiti odgodu ovrhe iz razloga navedenih u članku 65. Zakona. O prijedlogu za odgodu ovrhe podnesenom u roku za žalbu protiv rješenja o ovrsi sud će odlučiti u roku od 8 dana i, ako prihvati taj prijedlog, rješenje o odgodi odmah dostaviti Agenciji u pisanom otpravku, a u slučaju potrebe priopćiti i telefaksom, elektroničkom poštom ili na drugi pogodan način.

Srdačan pozdrav
Tomislav Horvat

FINA - Financijska agencija
Sektor financijskih i elektroničkih usluga Ovršni odjel Ulica grada Vukovara 70, 10 000 Zagreb tel 01 6127 016 fax 01 6127 021 tomislav.horvat@fina.hr www.fina.hr

Socijalni inženjering

Ciklus napada



Ostali oblici socijalnog inženjeringa

- Vishing
  - Vishing se odnosi na krađu identiteta putem telefonskih poziva
  - Budući da se glas koristi za ovu vrstu krađe 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 ili 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
- Spear phishing
  - Spear phishing se razlikuje od klasičnog phishinga u kojem se jedna e-poruka šalje milijunima nepoznatih korisnika, u spear phishingu napad cilja određenog korisnika uz pažljivo osmišljen tekst e-poruke
  - Ovi napadi imaju veći rizik jer napadači prvo dobro istražuju sve dostupne informacije o korisniku (putem društvenih mreža, organizacijskih podataka, web stranica)
  - Ova vrsta phishinga se najviše koristi pri napadu na korisnika pojedinca ili na organizaciju.

- Whaling
  - Whaling phishing ili tzv. kitolov se ne razlikuje mnogo od spear phishinga, no ciljana skupina je specifičnija / posebnija te ograničena za ovakav tip napada
  - Ova vrsta napada cilja na direktorske/upravljačke radne pozicije kao što su izvršni direktor, financijski direktor za koje se smatra da su veliki igrači - “kitovi” u informacijskom lancu organizacije
  - Ovom vrstom napada najviše ciljani sektori su tehnologija, bankarstvo i zdravstvo zbog dva glavna faktora: velikog broja korisnika i veće ovisnosti o podacima.

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 ili 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 mrežne komunikacije
      - Operacijski sustav Windows od inačice XP već sadrži vatrozid s odgovarajućom zaštitom.

- Opće metode zaštite
  - Automatsko ažuriranje operacijskog sustava i aplikacija
    - Sigurnosni propusti u programima stalno se otkrivaju
    - Kako bi zaštitili računalo, važno 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

- 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
      - Nacionalni CERT svakodnevno objavljuje informacije o novim trendovima u svijetu kibernetičke sigurnosti u obliku koji je prilagođen svim korisnicima bez obzira na razinu tehničkog znanja
  - 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

Zaštita

- Educirati o kibernetičkoj sigurnosti
  - Razlikovati aktivno i pasivno učenje
    - Pasivno učenje – pasivni prijenos znanja
    - Aktivno učenje – stvaranje kognitivnih struktura potrebnih za obradu novih situacija na temelju prethodno prikupljenih informacija
  - Razgovarati o kibernetičkoj sigurnosti
    - Razgovor i osvještavanje važnosti kibernetičke sigurnosti su temelj za stvaranje sustava vrijednosti koji kibernetičku sigurnost vrednuje kao temelj života u digitalnog društvu
  - Osvijestiti važnost higijene
    - Svakodnevne sigurnosne prakse koje korisnik svjesno poduzima, aktivno propitkuje i po potrebi mijenja

Najveći slučajevi curenja podataka u 2018.

- British Airways
  - 380 000
- Orbitz
  - 880 000
- SingHealth
  - 1,5 milijuna
- T-Mobile
  - 2 milijuna
- myPersonality
  - 4 milijuna
- Saks and Lord & Taylor
  - 5 milijuna
- SheIn.com
  - 6,42 milijuna
- Cathay Pacific Airways
  - 9,4 milijuna
- Careem
  - 14 milijuna
- Timehop
  - 21 milijuna
- Tickterfly
  - 27 milijuna
- Facebook
  - 29 milijuna
- Chegg
  - 40 milijuna
- GooglePlus
  - 52,5 milijuna
- Cambridge Analytica
  - 87 milijuna
- MyHeritage
  - 92 milijuna
- Quora
  - 100 milijuna
- MyFitnessPal
  - 150 milijuna

- Exactis
  - 340 milijuna
- Marriott Starwood hotels
  - 5 milijuna
- Aadhar
  - 1,1 milijardi

Postotak neželjene pošte

KASPERSKY lab

Najčešće phishing poruke

- Verifikacija računa
- Dijeljenje datoteka putem oblaka
- Dostava paketa
- Poruke Porezne uprave
- Lažni računi
- Kompromitirani računi e-pošte
- Poruke vezane uz GDPR
- Sextortion
- Kriptovalute
- Političke kampanje
- Hrana

Zaštita

- Kako educirati o sigurnosti?
  - Komunikacija putem interneta
    - Utvrđivanje pravog identiteta osobe
    - Digitalni trag
    - Povjerenje se mora steći
  - Korisnički podaci
    - Virtualni identitet
    - Objasniti zašto biramo složene lozinke
  - Povjerljivi podaci
    - Upoznavanje s vrijednostima podataka
    - Postupanje s povjerljivim podacima
    - Promišljeno djelovanje
  - Opasnosti
    - Nepromišljeno i neodgovorno ponašanje vodi u opasnost

Zaštita

- Hrabar, ali oprezan korisnik
  - Strah i panika onemogućavaju korisniku da sagleda situaciju i na pravi način reagira
  - Iako nam se čini kako je strah katkad dobar poticaj, ne smijemo izazivati strah kod korisnika
    - Pojedini korisnici mogu odlučiti ne služiti se internetom u potpunosti te jednostavno odbiti koristiti ga zbog straha od napada
    - Neki korisnici bi mogli odlučiti kako je njima teško održavati visoku razinu kibernetičke sigurnosti
- Znatiželjan, ali odgovoran korisnik
  - Internet je prozor u svijet, prečac do novog znanja i vrijedan alat
    - Korisnik ga mora moći koristiti neograničeno i slobodno
  - Ali Internet koriste i zlonamjerni korisnici
    - Korisnik mora moći prepoznati prijetnju te ju prijaviti nadležnoj službi
    - Korisnik je prva linija obrane i onaj čija pravilna reakcija uvelike podiže sigurnost mreže