REPUBLIKA HRVATSKA
Zavod za sigurnost informacijskih sustava

SIGURNOST KOMUNIKACIJE ELEKTRONIČKOM POŠTOM

EDUKATIVNI MATERIJAL O SIGURNOSTI KOMUNICIRANJA ELEKTRONIČKOM POŠTOM

www.zsis.hr

SADRŽAJ

ELEKTRONIČKA POŠTA I OPASNE PORUKE

Današnju komunikaciju, privatnu ili poslovnu, ne možemo zamisliti bez korištenja elektroničke pošte, popularno zvane *e-mail*. Elektronički uređaji, razni alati i aplikacije za razmjenu poruka elektroničke pošte su sveprisutni. S obzirom na navedeno, elektronička komunikacija postala je primarni način međusobne razmjene informacija. Koristimo ju svakodnevno u poslovne i privatne svrhe. Također, primjenom elektroničke komunikacije, u realnom vremenu možemo kontaktirati bilo koga bez obzira na lokaciju i doba dana.

U odnosu na bilo koji drugi način elektroničke komunikacije, neovisno o razvoju novih tehnologija, više od polovice korisnika i dalje daje prednost elektroničkoj pošti.

Elektronička pošta je jednostavan, brz, diskretan i vrlo dostupan način komunikacije koji je ujedno i najrasprostranjeniji. Međutim, on postaje i preferirani kanal putem kojeg pojedinci i kriminalne skupine izvršavaju kibernetičke napade na druge pojedince ili organizacije (tzv. mete).

Upitajte se sljedeće:

Kad ste posljednji put pogledali svoj telefon ili računalo?

Prema provedenim istraživanjima, prosječna osoba provjeri svoj telefon i do 150 puta dnevno. To je poznato i kriminalcima koji žele iskoristiti ranjivosti u postojećim načinima komunikacije kako bi ostvarili određenu korist.

Upotrebom elektroničke komunikacije cijeli svijet je postao igralište kriminalaca koji mogu jednostavno pristupiti svakome od nas. Svojim aktivnostima, oni mogu iskoristiti ranjivosti tehnologije kako bi se sakrili iza nepostojećeg ili ukradenog identiteta.

Upravo je ovo razlog zašto moramo biti oprezni u načinu kako koristimo tehnologiju i kome vjerujemo.

TKO NAM PRIJETI I S KOJIM CILJEM?

Ovim vam putem želimo približiti jednu od najčešćih vrsta napada putem elektroničke pošte – takozvani *phishing*. Tim se aktivnostima kriminalci koriste kako bi putem lažiranih poruka elektroničke pošte, mrežnih stranica ili glasovnih poziva napravili određenu radnju. Na primjer, naveli žrtve da preuzmu zlonamjerni kod ili otkriju povjerljive informacije.

Kako bi se razumjeli razlozi korištenja *phishinga* kao prijetnje informacijskoj sigurnosti, potrebno je biti svjestan profila potencijalnog napadača i njegovih motiva. Profili i motivi napadača su raznoliki; od igre i potrebe za dokazivanjem pojedinca preko manje ili više uspješnih pokušaja krađe i iznude od strane pojedinih kriminalaca ili organiziranih skupina pa sve do visoko sofisticiranih ciljanih *phishing* napada. Takve napade provode educirani i sposobni napadači koje često sponzoriraju pojedine države.

Primarni cilj *phishing* napada je prevariti korisnika na način da povjeruje u izvor, istinitost i opravdanost zahtjeva iskazanog putem poruka elektroničke pošte, mrežnih stranica, glasovne komunikacije ili SMS poruka. Svrha je navođenje na poduzimanje željene aktivnosti.

Aktivnosti na koje su usmjerene ovakve vrste napada, odnosno cilj napada, prvenstveno ovisi o motivu napadača. Raspon može biti od klasičnog kibernetičkog kriminala (koji uključuje krađu osobnih i financijskih podataka s ciljem stjecanja materijalne koristi) pa do preuzimanja zlonamjernog koda na vaše uređaje, prezentiranja neželjenog marketinškog materijala ili prezentiranja lažnih vijesti kojima se želi formirati određeno (javno) mišljenje.

KOGA SE NAPADA I ZAŠTO?

Ovisno o ciljevima napada, formiraju se skupine potencijalnih meta kojima će se *phishing* napadi prilagoditi kako bi izgledali što uvjerljivije i postigli maksimalni učinak. Najčešće mete napada ovise o veličini populacije, motivu i ciljevima.

Osim stjecanja financijske koristi, napadima se želi utjecati i na povjerljivost, cjelovitost i raspoloživost podataka kako bi se onemogućilo normalno funkcioniranje informacijskih sustava.

Važnost i zastupljenost elektroničke komunikacije putem elektroničke pošte ključni je razlog učestalih i raznovrsnih napada na korisnike.

Primjena različitih organizacijskih i tehničkih sigurnosnih mjera koje omogućuju zaštitu od napada često je kompleksna i financijski zahtjevna.

Velik dio tereta prepoznavanja zlonamjernih poruka pada na krajnje korisnike, pošiljatelje i/ili primatelje elektroničke pošte.

Mnoga istraživanja pokazuju da su korisnici najslabija karika sigurnosti u komunikaciji elektroničkom poštom. Upravo zato napadači koriste napade putem poruka elektroničke pošte kako bi što jednostavnije, brže i jeftinije ostvarili svoje ciljeve.

Ciljane skupine *phishing* kampanja:

Šira javnost

Putem *phishing* kampanje određene se informacije žele prezentirati što većem broju pojedinaca, odnosno korisnika elektroničke pošte.
U ovu kategoriju uključene su neželjene poruke (*spam*), zlonamjerno oglašavanje (*mal-vertising*) i poruke neistinitog sadržaja (*hoax, fake news*).

Korisnici usluga

Putem *phishing* kampanje ciljaju se skupine pojedinaca koji koriste određene usluge. Kod ovakvih napada ciljevi mogu biti krađa ili neovlaštena izmjena podataka koji se obrađuju putem usluge, ali i onemogućavanje korištenja usluga što direktno utječe na samog pružatelja usluga.

Informacijski sustavi državne uprave

Putem *phishing* kampanje ciljaju se skupine pojedinaca koji su članovi državnih tijela, tijela jedinica lokalne i područne (regionalne) samouprave kao i pravne osobe s javnim ovlastima te kada se napadom na pojedinca, zaposlenika, želi neposredno ostvariti napad na samo tijelo.

Neki od najčešćih razloga korištenja *phishing* napada su:

- Niska razina svijesti korisnika elektroničke pošte
- Sve veća javna dostupnost osobnih podataka pojedinaca
- Jednostavnost napada zbog dostupnosti alata i znanja
- Relativno niska cijena *phisihing* napada
- Oslanjanje napadača na *zakon velikih brojeva*

KOJE SU VRSTE NAPADA?

Postoji nekoliko vrsta *phishing* napada koji se razlikuju po mediju putem kojeg se vrše i po obujmu. Mediji kojima se izvode napadi najčešće su elektronička pošta, SMS ili glasovni poziv. Što se tiče obujma, postoje ciljani napadi na velike skupine, odnosno grupe korisnika i usmjereni napadi na jednu skupinu ili manju grupu korisnika. Kod široko ciljanih napada ne postoji usmjerenje na određenu skupinu i ne postoji snažna poveznica među njima, obično nisu sofisticirani i jednostavno ih je prepoznati. Usmjereni napadi su sofisticirani, puno manjeg obujma i njima prethode opsežna istraživanja mete putem otvorenih izvora podataka.

Phishing napadi mogu se podijeliti u tri kategorije:

1. *Phishing* napadi putem poruka elektroničke pošte bez napredne selekcije meta, slanjem na veliki broj adresa potencijalnih meta. Napade je obično jednostavno prepoznati i izbjeći.

2. *Spear phishing* napadi su kategorija kod kojih poruka nije usmjerena na široku grupu korisnika nego je precizno ciljana na određenog pojedinca.

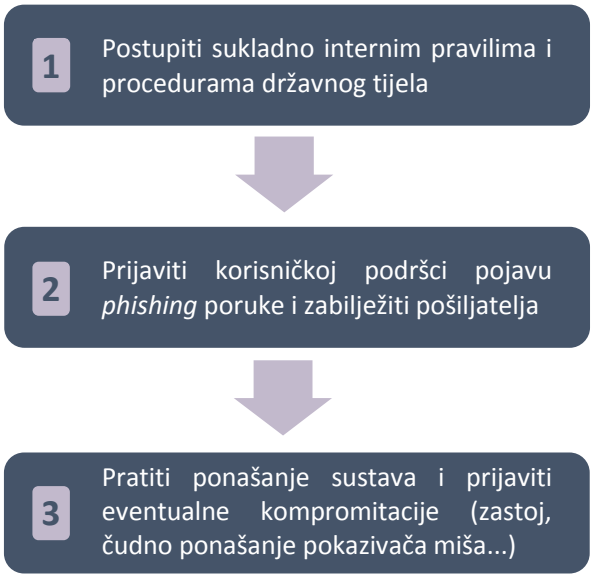
3. *Whaling* je podvarijanta *spear phishing* napada kod koje se cilja na upravljačke pozicije koje imaju pristup povjerljivim podacima organizacije. Još jedna varijanta *phishing* napada poznata kao *catphishing* je korištenje lažnog profila na društvenim mrežama. Metu se namami u neku vezu (najčešće romantičnu) koja postaje alat za ucjenjivanje i dobivanje informacija ili pristup određenim resursima.

Poruke elektroničke pošte koje su dizajnirane kao *spear phishing* i *whaling* teško je izbjeći i prepoznati ukoliko meta nema dovoljno visoku razinu svijesti o *phishing* napadima. Prilikom izvođenja *spear phishing* i *whaling* napada koriste se metode proučavanja društvenih mreža, međuodnosa mete s drugim osobama i ostale javno dostupne informacije o metama.

ŠTO UČINITI KAD UOČIMO SUMNJIVU PORUKU?

Ukoliko postoji sumnja da je pristigla *phishing* poruka, ključno je **ne slijediti poveznice u poruci i ne preuzimati sadržaje iz poruke**.

Nakon utvrđene sumnje preporučljivo je provesti aktivnosti na način kako je prikazano u nastavku:



NA ŠTO SVE TREBA OBRATITI PAŽNJU KOD PRIMITKA PORUKE ELEKTRONIČKE POŠTE?

Po primitku neočekivane poruke, potrebno joj je oprezno pristupiti kako bismo utvrdili možemo li vjerovati pošiljatelju i sadržaju. Kod ovakvih poruka pripazite na sljedeće:

- **Provjerite ime pošiljatelja i adresu s koje se poruka šalje** – pošiljatelji su često prikazani lažnim imenom. Ako se promijeni samo jedno slovo ili znak (npr. slovo O i brojka 0) korisnik vjerojatno neće primijetiti kako se radi o lažnom nazivu.

- **Poruka vam je poslana s generičke/javne domene** – elektronička pošta u državnim tijelima (kao i u svakoj drugoj organizaciji) po internim pravilima i procedurama mora biti korištena isključivo u poslovne svrhe. Primitak poruka s generičkih domena te poduzimanje akcija temeljem primljenih poruka (posjećivanje poveznica, otvaranje privitaka), kao i slanje poruka na generičke/javne domene (npr. gmail.com, hotmail.com, outlook.com) nije u skladu s internim pravilima te najvjerojatnije predstavlja povredu politike o primjerenom korištenju informacijskog sustava.

- **Elektronička pošta sadrži privitak za koji tvrdi da je potvrda ili traži dodatne informacije od vas** – ukoliko sumnjate na poruku koja vas traži otvaranje privitka, a istu poruku zajedno s privitkom niste očekivali, nemojte ga otvarati. Ovim putem dozvoljavate instalaciju zlonamjernog koda na vaš uređaj. Primitak bilo koje neočekivane poruke s privicima mora biti popraćen provjerom njezine autentičnosti alternativnim kanalima (usmenim upitom ili telefonskim pozivom prema osobi koja je zahtjev poslala).

- **Poruka sadrži poveznice** – legitimne poruke rijetko sadrže poveznice na tražene akcije. Također, one ne bi trebale biti sakrivene iza riječi nego prikazane u cijelosti. Prije samog odlaska na poveznicu prijeđite mišem preko nje i provjerite upućuje li na adresu istovjetnu uobičajenim adresama organizacije koja vam šalje poruku. Obratite pozornost na dijakritičke znakove drugih jezika koji su vrlo slični znakovima koje koristimo (npr. o, ö, ô, ó).

- **Prijete vam ili zahtijevaju hitnu akciju** – vrlo je često namjera *phishing* poruke izazvati paničnu reakciju putem prijetnje ili traženja hitne akcije. Pod utjecajem osjećaja hitnosti meta zaboravlja na znakove koje opisujemo u ovom tekstu i radi greške, na što napadači računaju.

- **Poruka koja od vas zahtijeva akciju koja nije očekivana** – čest primjer ovog tipa poruke jest *CEO fraud* (https://www.zsis.hr/default.aspx?id=404) u kojem se od zaposlenika traži provođenje neuobičajenog zahtjeva (npr. zahtjev za novčanim prijenosom kojeg je poslao izravno čelnik tijela). U slučaju primitka takve poruke, potrebno je provjeriti njezinu autentičnost alternativnim kanalom (usmenim upitom ili telefonskim pozivom prema osobi koja je zahtjev poslala).

- **Traže vas da odgovorite uz dostavu svojih privatnih podataka** – organizacije s kojima komunicirate putem poruka vas nikada ne bi smjele tražiti vaše privatne podatke poput korisničkog imena, zaporke, kontrolnog broja na kartici, statusa vašeg zdravlja, itd. Čak i da utvrdite kako je zahtjev organizacije legitiman, pokušajte ne odavati ovakve informacije putem poruka.

- **Poruka u kojoj je adresa pošiljatelja različita od naziva pošiljatelja** – zbog načina na koji popularni klijenti elektroničke pošte prikazuju zaglavlja i podatke u primljenoj poruci, kao i zbog karakteristika korištenih mehanizama komunikacije, napadači mogu vrlo jednostavno lažirati naziv pošiljatelja, bez potrebe za lažiranjem i adrese pošiljatelja. Tipičan primjer je *CEO fraud* u kojem je naziv pošiljatelja često čelnik tijela ili druga visokopozicionirana osoba, dok je adresa pošiljatelja generička i nema veze s organizacijom koja je poruku primila i iz koje poruka navodno dolazi.

- **Nudi vam se nešto jako vrijedno bez da ste isto zatražili** – vrlo često *phishing* poruke nude velike nagrade kako bi vam privukli pažnju i angažirali vas. Ako ne očekujete nagradu ili niste igrali igru, na ovakve poruke nemojte reagirati.

- **Sadržaj poruke ne odgovara adresi s koje ste primili poruku** – vrlo često adresa elektroničke pošte pošiljatelja upućuje na vrstu organizacije koja se bavi određenom djelatnošću. Ukoliko ste, na primjer, dobili poruku od autoprijevozničke tvrtke, a sadržaj poruke se odnosi na lijekove i farmacijske proizvode, moguće je da se radi o *phishing* poruci.

- **Ako ste dobili poruku od poznanika, a niste sigurni u njenu valjanost** – često zaraza zlonamjernim kodom kojim ste se vi zarazili može rezultirati slanjem iste poruke i vašim kontaktima. Takve poruke često se stilski i sadržajno razlikuju od uobičajene komunikacije s poznanikom, stoga je potrebno kritički razmišljati čak i kad je pošiljatelj vaš provjereni kontakt.

- **Obratite pažnju na pravopis** – vrlo često *phishing* poruke sadržavaju pravopisne pogreške i/ili neuobičajene izraze u znatno većoj mjeri od uobičajenih poruka. Posebno se to odnosi na generičke poruke na kojima je moguće uočiti prijevod korištenjem automatiziranih alata.

- **Provjerite potpis s kojim završava poruka** – legitimne poruke završavaju s očekivanim potpisom i detaljima uz potpis. Pripazite kad potpisa nema, a pošiljatelja ne poznajete.

- **Poruke koje korisnik šalje sam sebi** – ponekad napadači šalju lažirane poruke u kojima je pošiljatelj jednak primatelju – ovo je vrlo jednostavan indikator *phishing* poruka.

- **Poruka u kojoj je lista primatelja prazna** - napadači ponekad šalju poruke korištenjem BCC liste primatelja. Takva poruka će u klijentu elektroničke pošte biti prikazana s praznom listom primatelja. Ovo nije nužno indikator *phishing* poruka, budući da se neke distribucijske liste i reklamne kampanje znaju koristiti istim metodama, no može upućivati na zlonamjernu poruku.

- **Provjerite broj primatelja poruke elektroničke pošte** – ponekad veći broj primatelja u poljima PRIMA i KOPIJA koji nisu povezani s vama može biti pokazatelj zlonamjerne poruke.

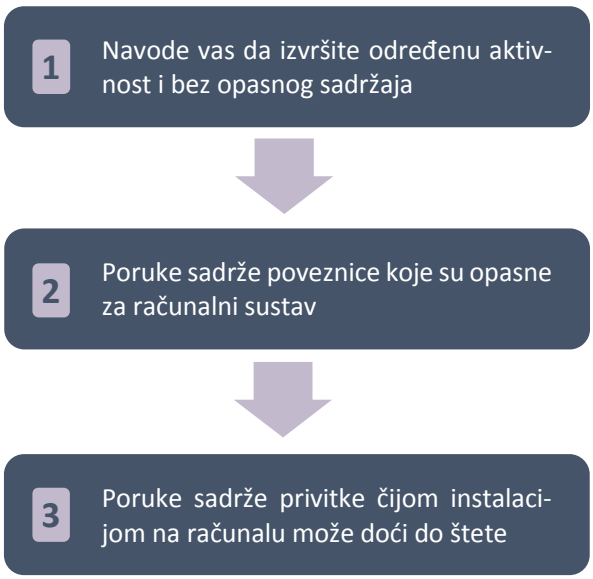
Ovisno o temama koje su od interesa za zaposlenike državnih tijela, poruke mogu biti sadržajno prilagođene. Takve prilagodbe mogu sadržavati teme koje su usko povezane s pojedinim državnim tijelom ili temama koje su vezane za određeno doba godine.

To su vrlo često:

- teme vezane uz blagdane, osobito one koje se odnose na popuste, posebne ponude u ljetnim mjesecima ili za zimovanja,

- teme koje su vijesti u medijskom prostoru, poput afera, financijskih ili statističkih podataka.

Ne zaboravite da zlonamjerne poruke elektroničke pošte mogu biti opasne iz tri razloga:



Proučite primjere u nastavku i naučite na koje još načine prepoznati problematične i potencijalno opasne poruke te što sve napadači rade kako bi napravili štetu vama ili sustavu.

PRIMJERI OPASNIH PORUKA

Poruke u nastavku su primjeri iz *phishing* prakse u Republici Hrvatskoj. Na porukama je moguće uočiti sljedeće pokazatelje lažnih i opasnih poruka:

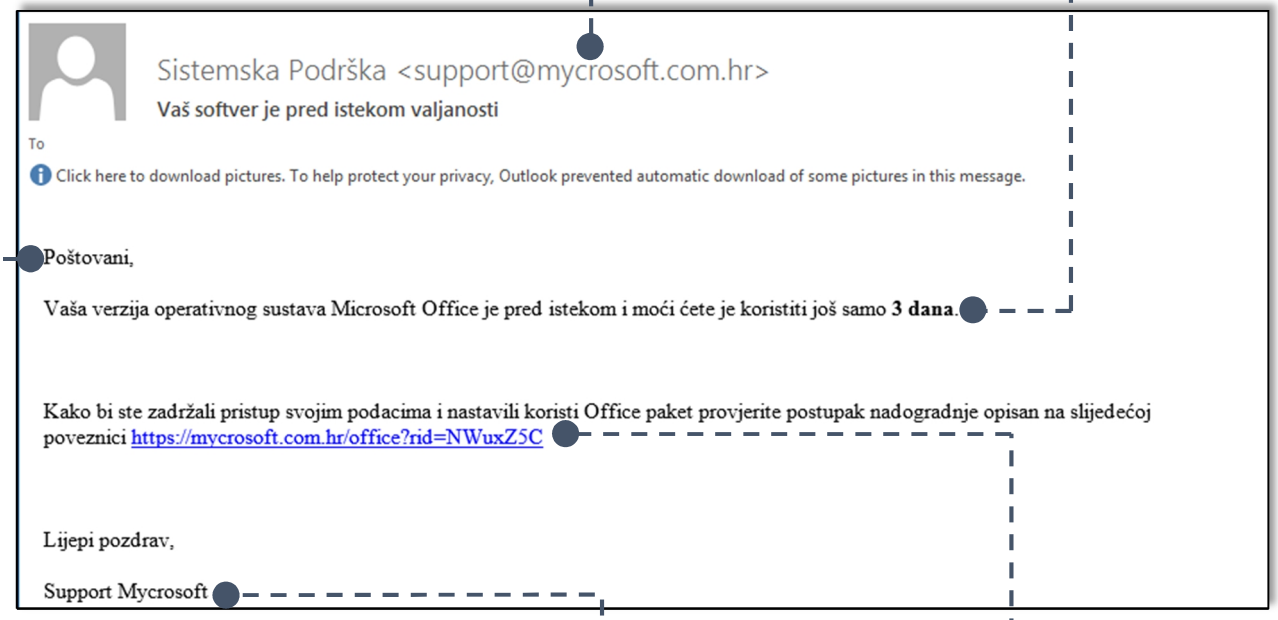
Primjer 1

POŠILJATELJI SU ČESTO PRIKAZANI LAŽNIM IMENOM KOJE JE JAKO SLIČNO STVARNOM

Ako se promijeni samo jedno slovo ili znak (npr. slovo O i brojka 0) korisnik vjerojatno neće primijetiti kako se radi o lažnom nazivu.

ZASTRAŠIVANJE ILI POZIVANJE KORISNIKA NA AKCIJU U ODREĐENOM ROKU

Ovo su taktike koje koriste napadači kako bi vas naveli na poduzimanje aktivnosti.



Sistemska Podrška <support@mycrosoft.com.hr>

Vaš softver je pred istekom valjanosti

To

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Poštovani,

Vaša verzija operativnog sustava Microsoft Office je pred istekom i moći ćete je koristiti još samo **3 dana**.

Kako bi ste zadržali pristup svojim podacima i nastavili koristi Office paket provjerite postupak nadogradnje opisan na slijedećoj poveznici https://mycrosoft.com.hr/office?rid=NWuxZ5C

Lijepi pozdrav,

Support Mycrosoft

POZDRAV S KOJIM POČINJE PORUKA JE DEPERSONALIZIRAN

Ukoliko poruka počinje s pozdravom poput "Poštovani", moguće da je poruka generička i namijenjena širem krugu meta.

POVEZNICE KOJE SE NALAZE U ELEKTRONIČKOJ POŠTI SU NAJOPASNIJI DIO ZLONAMJERNIH PORUKA

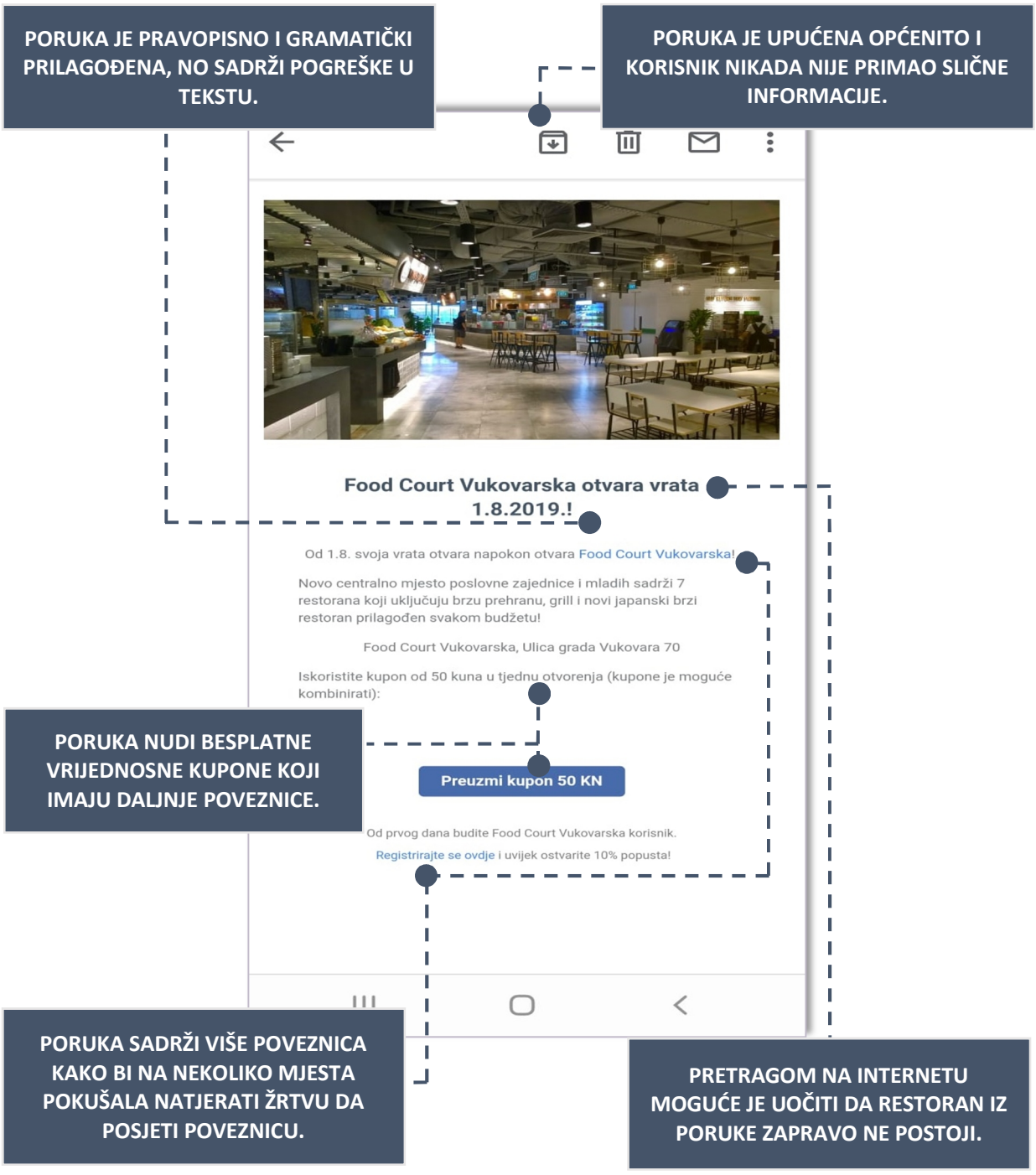
One često sadrže lažne nazive stranica slične stvarnima kao i velik broj slova i znakova.

IZOSTANAK POTPISA POŠILJATELJA ILI NEISPRAVNI PODACI U POTPISU

Legitimne poruke završavaju potpisom i detaljima uz potpis; pripazite ukoliko potpisa nema ili su znakovi izmijenjeni.

Primjer 2

Ne zaboravite, poruke su često prilagođene i mobilnim uređajima te mogu biti jednako opasne. U ovoj zlonamjernoj poruci napadači koriste nekoliko mehanizama kako bi prevarili svoje žrtve:



Primjer 3

U prikazanom primjeru ove poruke elektroničke pošte možemo uočiti:

VIJEST VEZANU ZA RAZLIČITE ANALIZE, POPUT VISOKIH IZNOSA BONUSA ILI ZARADA NA SVE POPULARNIJI „CRNI PETAK“.

PORUKA NA NEKOLIKO MJESTA SADRŽI POVEZNICE KAKO BI PUTEM VIŠE LAŽNIH TEMA NAVELA KORISNIKA NA ODLAZAK NA NEKU OD NJIH.

S OBZIROM NA TO DA KORISNIK INAČE NE PRIMA PORUKE OVAKVOG IZGLEDA, POVEZNICA NA KRAJU PORUKE LAŽNO NAVODI MOGUĆNOST ODJAVE S LISTE PRIMATELJA.

LAŽNU VIJEST VEZANU ZA HRVATSKO GOSPODARSTVO KOJA NE OTKRIVA O ČEMU SE RADI, VEĆ POZIVA ČITATELJA DA PROČITA VIŠE NA POVEZNICI.

ŠTO NAM DONOSI BUDUĆNOST?

Proučavajući podatke uzroka sigurnosnih incidenata vidljivo je kako su *phishing* poruke vrlo popularan i čest način pristupanja metama i iskorištavanju njihovih ranjivosti kao i da taj trend ne jenjava, već se povećava. Ovakve vrste napada vrlo često uspijevaju zbog niske razine osviještenosti korisnika što želimo promijeniti informacijama i uputama iz ovog dokumenta.

Svi smo mi potencijalna meta napada bez obzira na lokaciju, vrstu posla, poziciju u organizaciji, svrhu u koju koristimo tehnologiju i stoga je iznimno bitno povećati ukupnu svijest o prijetnjama kojima smo svi izloženi, a sve u svrhu kreiranja boljeg društva i uspostavljanja povjerenja u tehnologiju i prednosti koje nam ona nudi.