Kako se zaštititi od phishing prijevara?

Pretpostavljam da ste u posljednje vrijeme i vi osjetili porast pokušaja prijevara, bilo telefonskim pozivima koji dolaze s brojeva diljem Europe i svijeta, a prodaju dionice, kriptovalute ili vam žele popraviti internetske usluge koje ni ne koristite, ili elektroničkom poštom, od tradicionalnih masovno poslanih poruka "nigerijskih prinčeva", do pažljivo isplaniranih *man-in-the-middle* napada na vašu tvrtku ili organizaciju….

Domagoj Marić, Megatrend Poslovna Rješenja

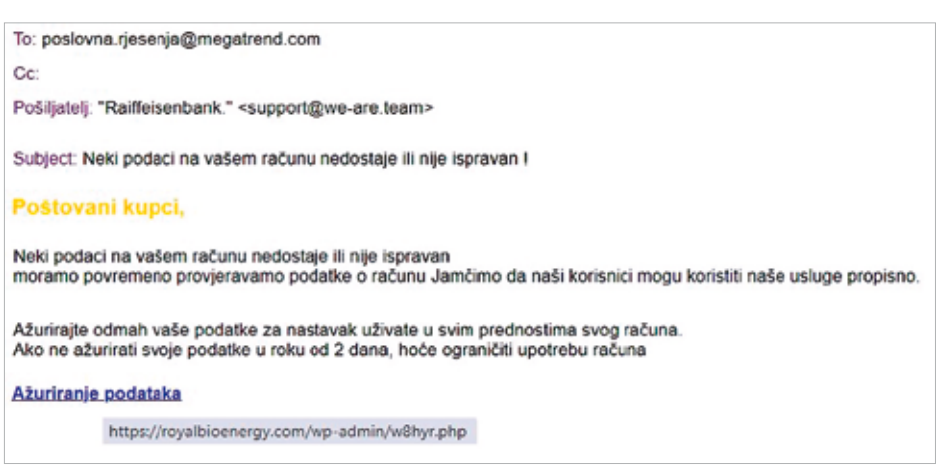
Phishing je jedna vrsta takvih internetskih prijevara, gdje je na kraju cilj napadača izvući nezakonitu financijsku dobit – u prijevodu ukrasti novac, ili podatke, što opet na kraju rezultira gubitkom novca žrtve. Takve prijevare vjerojatno su stare koliko i Internet, no napadači su tijekom godina postali vrlo sofisticirani u svojim metodama.

Cijela situacija dodatno se pogoršala posljednjih nekoliko godina, dolaskom nekoliko razdoblja *lockdowna*, gdje su ljudi bili primorani ostajati u svojim domovima te su nerijetko provodili više vremena na računalima. Stoga su se oni, koji nisu naviknuti koristiti često računala, morali prilagoditi na više digitalizacije, a s povećanom digitalizacijom dolazi i veća izloženost prevarantskim porukama elektroničke pošte.

PROJEKT PHISHRBAN

Stoga je tvrtka Megatrend poslovna rješenja ugovorila dodjelu bespovratnih sredstava iz natječaja "Povećanje razvoja novih proizvoda i usluga koji proizlaze iz aktivnosti istraživanja i razvoja – faza II", koji se financira iz Europskog fonda za regionalni razvoj (EFRD), za projekt pod nazivom "Istraživanje obrade prirodnog jezika (za hrvatski jezik) i razvoj proizvoda PhisHRban za povećanje kibernetičke sigurnosti".

Projekt provode Megatrend poslovna rješenja d.o.o., kao korisnik projekta, zajedno s partnerima – Filozofski fakultet i Ekonomski fakultet Sveučilišta u Zagrebu, a cilj projekta je razviti novi, inovativni proizvod PhisHRban, koji će omogućiti prepoznavanje *phishing* poruka na hrvatskom jeziku, s ciljem povećanja kibernetičke sigurnosti, koristeći se metodama obrade prirodnog jezika.


To: poslovna.rjesenja@megatrend.com

Cc:

Pošiljatelj: "Raiffeisenbank." <support@we-are.team>

Subject: Neki podaci na vašem računu nedostaje ili nije ispravan !

Poštovani kupci,

Neki podaci na vašem računu nedostaje ili nije ispravan
moramo povremeno provjeravamo podatke o računu Jamčimo da naši korisnici mogu koristiti naše usluge propisno.

Ažurirajte odmah vaše podatke za nastavak uživate u svim prednostima svog računa.
Ako ne ažurirati svoje podatke u roku od 2 dana, hoće ograničiti upotrebu računa

Ažuriranje podataka

https://royalbioenergy.com/wp-admin/w8hyr.php

Ogledni primjer *phishing* poruke

Unutar tog projekta postoje dvije osnovne komponente (problema, izazova) koje moramo riješiti, kako bismo postigli taj cilj – prvi je detekcija *phishing* poruka elektroničke pošte, dok je drugi detekcija zlonamjernih *phishing* URL adresa, koje najčešće vode na lažne i zlonamjerne stranice, kojima je isto tako cilj prevariti žrtvu krađom novca ili osjetljivih podataka.

KAKO NAPADAČI DOĐU DO VAŠE EMAIL ADRESE?

Postoje četiri osnovna načina kako napadači dođu do vaše *email* adrese, koja je najčešće samo jedna od stotina, tisuća, ili čak milijuna *email* adresa:

Kupovanje listi e-mail adresa (engl. paste ili **dump**) – često skup od nekoliko milijuna adresa, pa napadači šalju jednu poruku pošalju na sve

Prikupljanje *email* adresa pretraživanjem web-prostora (engl. **email harvesting**) – prikupljanje adresa pomoću procesa *web-crawlinga* i osnovnih regularnih izraza za *mail* adrese

Lažne web-stranice, koje napadači postavljaju kako bi prikupili osjetljive podatke žrtve (lakša inačica *phishinga,* koja omogućuje druge phishing prijevare)

Sigurnosni propusti povezani s povredom osobnih podataka (engl. **data breach**) – Facebook, Yahoo, Dropbox, LinkedIn, MySpace, Adobe i Snapchat – samo su neke od žrtava *data breacheva*, dakle trebamo paziti što i gdje ostavljamo od svojih osobnih podataka.

KOJE SU NAJČEŠĆE VRSTE PHISHING PORUKA?

Prvi, a ujedno i najprimitivniji tip *phishing* poruka su lažne, odnosno nepostojeće nagradne igre. Uz obavijest o tome da ste dobitnik nagradne igre, najčešće dobivate uputu za klik na sumnjivu URL adresu ili preuzimanje priloga. Naravno, tu je generalno pravilo da ako se niste prijavili na nagradnu igru, ništa nećete ni osvojiti, a čak i ako ste se prijavili, dvaput provjerite obavijest koju ste dobili. Varijacija na takvu poruku je i danas vrlo popularna prijevara nepostojeće narudžbe, gdje primatelj dobiva na prvi pogled legitimnu obavijest o izvođenju narudžbe koju nije napravio, ali se ipak radi o zlonamjernim poveznicama ili prilozima.

Jedan korak iznad u spektru primitivnosti

phishing prijevara su tradicionalne poruke "nigerijskih prinčeva", gdje pošiljatelj tvrdi da dolazi iz neke države trećeg svijeta te treba baš vašu pomoć prilikom transakcije svog bogatstva. Najčešće u tom slučaju slijedi uputa za uplatu određene "početne" svote, nakon čijeg izvršenja žrtva više ne čuje ništa od napadača. S obzirom na to da je taj tip prijevare star gotovo kao i elektronička pošta, postoji mnogo varijacija na temu s istim ciljem.

Prosječni korisnik Interneta danas koristi velik broj različitih *online* usluga, bili to multimedijski servisi za *streaming* glazbe i filmova, servisi za elektroničku poštu, fizičku poštu ili platforme za *online* kupnju, zbog čega je očigledno da postoji i velik broj prijevara povezanih s korisničkim računima takvih servisa. U takvim zlonamjernim porukama predmet je najčešće suptilno upozorenje korisniku da mora izvršiti neku uplatu kako bi mogao nastaviti koristiti uslugu (a često i direktna prijetnja gašenja, s dodatnom dozom urgentnosti). Takve poruke imaju jednak cilj i metodu kao i prošle navedene vrste, pa svakako treba pomno provjeriti gramatiku i pravopis, kao i URL adrese poveznica, kako ne biste završili na lažnim stranicama.

Posljednji, a ujedno i najgori tip *phishing* prijevara je tzv. *spear phishing*, koji je danas najveći problem. U takvoj prijevari napadač dobro poznaje prirodu komunikacije između dvije osobe (tko su te osobe, kakav je njihov odnos, kakva je njihova uloga u nekoj organizaciji i sl.), pa se ubacuje u komunikaciju koristeći lažnu, ali prividno legitimnu *mail* adresu. To je najsofisticiranija metoda napada, a najčešće se ciljaju tvrtke i organizacije. Traži se neka brza uplata, pristup nekom sustavu ili osjetljive informacije. S obzirom na to je ta vrsta *phishing* poruka vrlo raznolika i ovisi o tome tko su žrtve i što napadač točno želi postići, nema univerzalnog savjeta, osim onog da uvijek budete skeptični i svaku sumnjivu stavku poruke dvostruko provjeravate.

KAKO PREPOZNATI ZLONAMJERNU URL ADRESU?

Na kraju, očigledno je pitanje kako znati kada treba zastati prije klika na poveznicu. Ono što uvijek treba imati na umu je koncept semantičkog weba – URL adrese web mjesta trebaju biti semantičke, nositi neko značenje i biti čitljive. Primjerice, logično je da je URL adresa bloga na stranicama Megatrend megatrend.com/blog, pošto ona sadrži baš one informacije koje treba sadržavati. Zlonamjerne URL adrese najčešće su dijametralna suprotnost tom konceptu.

Ako želite saznati više o primjeni umjetne inteligencije u području informacijske sigurnosti i konkretno u rješavanju problema detekcije zlonamjernih poruka na Internetu, obratite se stručnjacima tvrtke Megatrend poslovna rješenja na poslovna.rjesenja@megatrend.com.

OSNOVNE KARAKTERISTIKE *PHISHING* PORUKA

- **spominjanje** novca i/ili kripto(valuta), primjerice eura, bitcoina...
- **generični** (neusmjereni) pozdravi
- **velika količina** nabacane informatičke ili pravne terminologije, bez previše smisla
- **urgentnost**, upozorenja i prijetnje gašenjem, kratki rokovi za reakciju
- **loša gramatika** i pravopis (najčešće loš automatizirani prijevod)
- ***mail* adresa** koja nije legitimna i tzv. doppelgänger domene, primjerice, domagoj-megatrend@prevarant.com umjesto domagoj.maric@megatrend.com
- **sumnjive URL adrese**, sumnjivi i neočekivani prilozi (najčešće zip arhive koje mogu sadržavati i *malware*)
- **spominjanje imenovanih** entiteta, poput nekih poznatih tvrtki i servisa (UPS, PayPal, Hrvatska pošta, Facebook, Netflix...)

http://megatrend.com-useridweb12347861257.prevarant-domena.com/app/76322

protokol	http://
domena	prevarant-domena.com
putanja	/app/76322
poddomena 1	com-useridweb12347861257
poddomena 2	megatrend

Prikaz strukture URL adrese na primjeru phishing adrese

OSNOVNE KARAKTERISTIKE PHISHING URL ADRESA

- **nepotrebno dugačke**, velik broj znamenki
- **vidljive ekstenzije** i portovi
- **pojava ključnih riječi** (pay, shop, secure, login, verification...)
- **ime prividno slično** nekoj popularnoj stranici (PAYPAI, Faceb00k, rnicrosoft...)
- **supstitucije znakova ->** napad homografima
- **velika količina** poddomena
- **velika količina** dodatnih parametara poslije putanje
- **dugački nizovi** alfanumeričkih znakova bez leksičkog smisla ili hex znakovi
- **prefiks za www domenu** (npr. "www702.paypal.ca")