CYBER PRIJEVARE I KAKO SE ZAŠTITITI

Hrvati masovno nasjedaju na internetske prijevare

Kibernetički kriminal se može smatrati lakšim za izvedbu od onog uobičajenog kriminala. Jedan od razloga je anonimnost koju pruža internet. Prevaranti mogu ostati neotkriveni i djelovati iz bilo koje lokacije u svijetu, što im omogućuje da izbjegnu kazneno gonjenje. Nažalost, problem je u tome što ljudi povjeruju u ono što vide na internetu i na koncu nasjednu na priču, obećanje, uputu, link ili nešto drugo

Donata Strbat

U DANAŠNJE vrijeme sve je više online prijevara u Hrvatskoj. Gotovo da ne prođe niti dan a da policija ne šalje priopćenja o svim ljudima koji su prevareni.

Svakodnevno smo svjedoci online naslova poput "Amerikanka mu obećala udaju pa ga opljačkala"; "Htjela trgovati dionicama nafte pa ostala bez pola milijuna kuna"; "U 13 navrata uplatila ukupno 17 tisuća eura"; "Zbog 'nove verzije mobilnog bankarstva' tvrtka ostala bez više tisuća eura", itd. Po svemu sudeći hrvatski narod masovno nasjeda na internetske prijevare. Tekst u nastavku trebao bi nam dati odgovor što činiti, kome se obratiti i prijaviti slučaj prijevare te kako preventivno djelovati da ne postanemo dio neumoljive statistike. Nažalost, najveći problem je u tome što ljudi povjeruju u ono što vide na internetu i na koncu nasjednu na priču, obećanje, uputu, link ili pak na nešto drugo.

Što nam je činiti?

Najučinkovitija obrana od ove vrste prijevara je obrazovanje potencijalnih žrtava a to može biti svatko od nas na internetu. Podizanje svijesti u društvu kako identificirati takve prijevarne tehnike učinit će korisnike i njihove financije sigurnijima. Nažalost, internet u današnje vrijeme je postao vrlo privlačan za kibernetičke kriminalce. Napadači se koriste vrlo profinjenim trikovima i obećanjima kako bi od vas izvukli novac ili vrijedne financijske informacije. Prijevare u kojima glavnu

ulogu igraju davno preminuli rođak ili princ nisu više jedini trikovi zanata. Taktike koje koriste kibernetički kriminalci postaju sve inovativnije i teže ih je za otkriti. Od pretvaranja da su voditelji vaše organizacije do toga da su zainteresirani za romantičnu vezu, online prevaranti današnjice učinit će sve što je potrebno da dobiju ono što žele odnosno vaš novac ili bankovne podatke.

Sedam najčešće korištenih online prijevara i kako ih izbjeći

1. CEO prijevara ili direktorska prijevara - varalice se pretvaraju da su vaši šefovi ili nadređeni u organizaciji i prijevarom vas navode da uplatite novčani iznos na lažni račun ili da neovlašteno doznačite novce s poslovnog računa.
2. Prijevara s računima - varalice se pretvaraju da su vaši klijenti ili dobavljači i navode vas da platite buduće račune na drugi bankovni račun.
3. Krađe identiteta:
   a) Vishing - Krađa identiteta pozivom - Telefonska prijevara u kojoj vas prevaranti zovu i pokušavaju navesti da otkrijete svoje osobne, financijske ili sigurnosne podatke ili da im uplatite novčana sredstva.
   b) Phishing - Mrežna krađa identiteta lažnim porukama e-pošte - Prevaranti vam šalju lažne poruke e-pošte kojima vas pokušavaju navesti na dijeljenje osobnih, financijskih ili sigurnosnih podataka.
   c) Smishing - Krađa identiteta SMS-om- Pokušaj prevaranata da dođu do osobnih, financijskih ili sigurnosnih podataka putem tekstualne poruke.
4. Krivotvorene mrežne stranice banaka - koristi se lažna e-pošta banke s poveznicom na krivotvorenu mrežnu stranicu. Jednom kada kliknete na poveznicu, koriste se razne metode prikupljanja vaših financijskih i osobnih informacija. Stranica izgleda kao i prava mrežna stranica uz nekoliko malih razlika.
5. Romantične prijevare - varalice se pretvaraju da su zainteresirane za romantičnu vezu. One se obično događaju na mrežnim stranicama za upoznavanje, a varalice često koriste društvene medije ili e-poštu za uspostavljanje kontakta.
6. Krađa osobnih podataka - vaše osobne informacije prikupljaju se kroz kanale društvenih medija.
7. Investicijske prijevare i prijevare u online kupovini - navede vas da mislite da ste na tragu pametnog ulaganja ili vam daju izvrsnu lažnu online ponudu.

Kriminalci koriste društveni inženjering kako bi postigli cijeli niz ciljeva poput dobivanja vaših osobnih podataka, otimanja vaših računa, krađe vašeg identiteta, pokretanje nezakonitih plaćanja ili pak vas uvjeriti da nastavite bilo koju aktivnost protiv svog interesa, kao primjerice doznačiti novac ili dijeliti osobne podatke. Jedan jedini klik može biti dovoljan kako bi ugrozio vašu cijelu organizaciju.

Prijevara i direktive EU

Europolov Europski centar za kibernetički kriminal (E3), Europska bankarska federacija i njihovi partneri javnog i privatnog sektora u listopadu 2018. godine proveli su kampanju osvješćivanja #CyberScams kao dio programa Europskog mjeseca kibernetičke sigurnosti (ECMS - European Cyber Security Month).

Prema podacima MUP-a vidljivo je kako je šteta od kibernetičkih napada porasla na više od 9,7 milijuna eura

Radi se o EU kampanji o podizanju svijesti koja potiče kibernetičku sigurnost među građanima i organizacijama, ističući jednostavne korake koji se mogu poduzeti radi zaštite vlastitih osobnih, financijskih i poslovnih podataka.

Prijevara je namjeran čin obmane radi osobne koristi ili nanošenja štete drugome. (Više u članku 3. stavku 2. Direktive EU 2017/1371). Nepravilnost je čin koji nije u skladu s pravilima EU-a te može negativno utjecati na njegove financijske interese, ali je posljedica nenamjernih pogrešaka korisnika sredstava ili tijela nadležnih za isplatu sredstava. Ako je nepravilnost počinjena namjerno, smatra se prijevarom. (Više u članku 1. Uredbe Vijeća 2988/95).

Kako prijaviti prijevaru OLAF-u

OLAF-u se možete obratiti anonimno. Nema nikakvih formalnosti, dovoljno je dati što točnije i podrobnije informacije te priložiti dokumentaciju ako je dostupna. S OLAF-om možete komunicirati na bilo kojem od 24 službena jezika EU-a. Prijavu možete podnijeti na sljedeće načine: internetom, putem sustava za obavješćivanje o prijevarama (anonimno, uz siguran prijenos dokumenata).

Na stranicama OLAF-a i Europskog ureda za borbu protiv prijevara /antifraud.ec.europa.eu/, možete prijaviti prijevaru i ujedno vidjeti kako se zaštititi u cyber okruženju. OLAF postupa s osobnim podacima u skladu s Uredbom EU 2018/1725. Potrebne informacije o zaštiti podataka dostavit će vam se kad ispunite obrazac na internetu. Opće informacije o zaštiti podataka u OLAF-u dostupne su u odjeljku zaštita podataka.

Hrvatska policija i suzbijanje kibernetičkog kriminaliteta

internetska stranica web heroj - ulovimo lika s weba koje tvoje €ure vreba je projekt MUP-a RH koji se nalazi na stranicama Ministarstva unutarnjih poslova (webheroj.hr) i pokrenut je u prosincu 2022. godine u svrhu jačanja kapaciteta policije u suzbijanju kibernetičkog kriminaliteta.

Preventivna kampanja naziva "Web heroj", pod sloganom "Ulovimo lika s weba koji tvoje eure vreba", provodi se kako bi se što većem broju građana približila važnost znanja o pojavnim oblicima kibernetičkog kriminala, opasnostima te mjerama prevencije i zaštite.

Nažalost, statistika je neumoljiva. Prema podacima MUP-a vidljivo je kako je šteta od kibernetičkih napada porasla na više od 9,7 milijuna eura. Naime, u 2022. godini, od različitih oblika kibernetičkih napada, najčešće internetskih prijevara, šteta je iznosila šest milijuna eura, dok u isto vrijeme 2023. godine iznosi više od 9,7 milijuna eura. Time je vidljiv porast od gotovo 50 posto, što ukazuje kako je kampanja koju provodi MUP RH uistinu potrebna. Prethodne 2023. godine zabilježen je 1781 kibernetički napad, od kojih 90 posto čine različiti oblici računalnih prijevara i to je porast od 11,5 posto u odnosu na 2022. godinu. Zaključno, kriminal raste za 11 posto, dok materijalna šteta raste za 50 posto a kako to navode iz Službe kibernetičke sigurnosti Ministarstva unutarnjih poslova. Ministarstvo unutarnjih poslova tijekom 2023. godine zaprimilo je 40-ak kaznenih prijava na štetu građana i trgovačkih društava

kojima počinitelji šalju lažne, tzv. "phishing" poruke, najčešće putem elektroničke pošte ili SMS-a u ime hrvatskih poslovnih banaka, u kojima traže da se ažurira aplikacija za internet bankarstvo, no ta poveznica vodi na lažne stranice banaka na kojima građani unose svoje osobne podatke i budu materijalno oštećeni. Materijalna šteta od samo tih 40-ak kaznenih prijava iznosi dva milijuna eura.

Što ako smo prevareni, kome se obratiti?

Iz dosadašnjeg iskustva može se vidjeti da građani ne znaju ili nemaju konkretan odgovor na pitanje kome bi se obratili za slučaj prijevare. Neki govore da bi se prvo obratili osobi od koje su kupili predmet, službi za korisnike ili prodajnom posredniku. Neki misle da se treba obratiti banci kako bi provjerili jesu li im podaci zaštićeni, dok drugima ne pada uopće na pamet što bi trebalo napraviti u toj situaciji.

Stoga je važno znati da se u slučaju internetske prijevare građanin treba obratiti policiji ili tržišnoj inspekciji Ministarstva gospodarstva, a ako je riječ o e-dućanu izvan Hrvatske treba se obratiti Europskom potrošačkom centru u Hrvatskoj.

Brojke internetskih prijevara neprestano rastu, a CERT /www.cert.hr/, svake godine dostavlja izvješće o kibernetičkoj sigurnosti. Naime, 2022. godine se uočilo povećanje broja korisničkih prijava računalno sigurnosnih incidenata za ukupno sedam posto u usporedbi s 2021. godinom. Pretpostavka je da je do povećanja došlo uslijed rezultata kampanji, edukacija i ostalih aktivnosti podizanja svijesti građana, veće medijske i javne zauzetosti za teme iz područja kibernetičke sigurnosti i posebno sigurnosti i zaštite krajnjih korisnika.

Jedan od glavnih razloga zašto ljudi ustvari olako padaju na prijevare je prvenstveno želja za lakom zaradom. Lako se mogu prevariti kad im se ponudi prilika za brzu i laku zaradu. Na to jednako tako utječe i nepažnja ili neznanje. Ljudi često ne obraćaju pažnju na detalje ili ne razumiju kako internetska prijevara funkcionira, što ih čini podložnijima prijevari.

Napadači pokušavaju iskoristiti ranjivost ljudi jer većina ljudi ima poteškoće u racionalnom odgovoru na različite emocije kroz strah, krivnju, empatiju te donose odluke bez razmišljanja. Uz to imamo i problem što ljudi vjeruju u ono što vide na internetu i ne provjeravaju informacije prije nego što ih koriste u donošenju odluka.

Teško je precizno odrediti omjer prijevara koje se tiču financijske koristi i onih koje se tiču uništavanja računalnih sustava, jer se različite vrste prijevara međusobno prepliću i mogu imati višestruke ciljeve.

Naime, u zadnjih desetak godina, iza većina napada je neki oblik financijske koristi. Prevaranti koriste kombinaciju različitih metoda kako bi dobili što više koristi od svake prijevare. Primjerice, prevaranti koji koriste malware (prvenstveno služe za napade na računalne sustave) često koriste podatke koje skupe na računalu i za financijske prijevare. Isto tako kibernetički kriminal se može smatrati lakšim za izvedbu od onog uobičajenog kriminala. Jedan od razloga je anonimnost koju pruža internet. Prevaranti mogu ostati neotkriveni i djelovati iz bilo koje lokacije u svijetu, što im omogućuje da izbjegnu kazneno gonjenje. Nažalost, problem je u tome što ljudi povjeruju u ono što vide na internetu i na koncu nasjednu na priču, obećanje, uputu, link ili nešto drugo.

Stoga, ne vjerujte svemu što vidite na internetu, provjeravajte informacije, radite na prevenciji, budite informirani na vrijeme odnosno budite dio pozitivne statistike i potražite informacije na stranicama Ministarstva unutarnjih poslova Republike Hrvatske /www.policija.gov.hr i webheroj.hr/ ili na stranicama OLAF-a i Europskog ureda za borbu protiv prijevara /anti-fraud.ec.europa.eu/, o tome kako se zaštititi u cyber okruženju. ■

Savjeti građanima

- dobro pazite na osobne podatke,
- dobro razmislite kakve podatke dijelite putem društvenih mreža,
- on-line plaćanja radite samo preko sigurnih internet stranica (https: protokol) i koristeći sigurne načine povezivanja na Internet (javne wifi mreže mogu biti rizične),
- svaku sumnju u vezi vašeg on-line računa odmah prijavite banci,
- pokušaj prijevare prijavite policiji čak i ako niste postali žrtva.