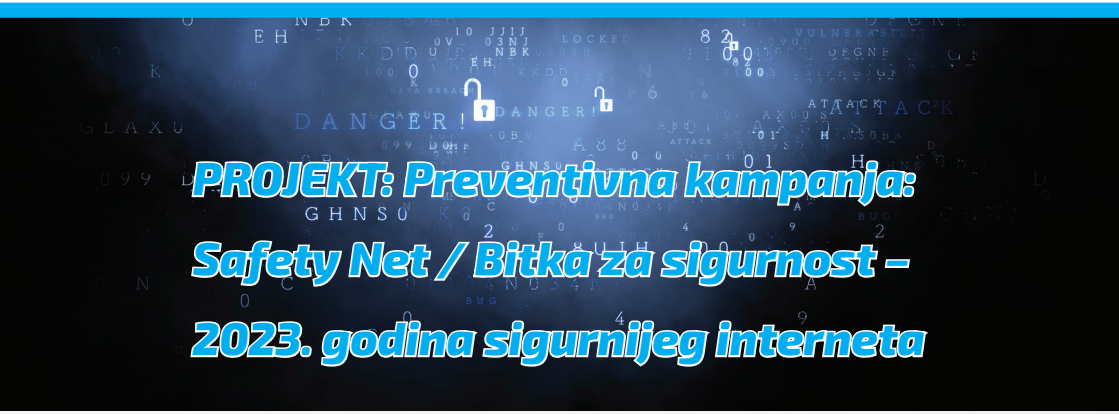
SafetyNet
BITKA ZA SIGURNOST



PARTNERI

Policijska uprava splitsko dalmatinska, Splitsko dalmatinska županija – Odbor za sigurnost, udruga djelatnika MUP-a IPA SD, udruga programera DUMP Split, Fakultet elektrotehnike, strojarstva i brodogradnje Split, IT tvrtka SPAN d.d., gradovi i općine SDŽ kroz Vijeća za prevenciju kriminaliteta.

CILJ

Kratkoročni ciljevi

- Osvijestiti građane o realnoj opasnosti od izloženosti kaznenim djelima iz domene računalnog kriminaliteta, najčešće su to prevare putem Interneta i društvenih mreža.
- Usporiti negativan trend porasta broja KD iz domene računalnog kriminaliteta.

Dugoročni ciljevi

- Razvijena svijest o potrebi preventivnog i samo zaštitnog ponašanja na mreži.
- Uspostaviti trend smanjenje broja KD iz domene računalnog kriminaliteta.

ANALIZA

Analizom statističkih pokazatelja PU SD za prethodnu 2022. godinu i kroz usporedbu sa ranijim godinama, prepoznaju se trendovi kriminaliteta koji utječu na odabir prioriteta i usmjeravanje resursa PU splitsko dalmatinske u 2023. godini.

Računalni kriminalitet, posebice u segmentu računalne prijevare statistički je u porastu, a kao posebnost izdvaja se relativno **jednostavan način počinjenja baziran na naivnosti i ponekad lakomislenosti žrtve.**

Naime, u pravilu se ne radi o složenim informatičkim operacijama, a najčešći oblik prevare je upornost počinitelja da kroz razgovor ili elektroničku korespondenciju, lažući o svom statusu, privilegijama koje će osigurati žrtvi ili joj olakšati npr. prodaju oglašenih stvari, dolazi do osobnih podataka koje nikada i nikome ne biste trebali davati.

VRIJEME PROVEDBE

2023. god.

AKTIVNOSTI

- aktivnost u okviru dosadašnje verzije kampanje Safety Net – kviz znanja dostupan na webu, nagrada najboljim poznavateljima Interneta povodom dana sigurnog interneta 7. veljače, https://safetynet-kviz.skole.hr/izbornik
- edukacija za djelatnike PU SD u suradnji sa RK IPA SD i ODO Split, 2.2.2023.
- materijali za medije dostupni na web stranici PU SD
- savjeti i primjeri na posebnoj poveznici PU SD i stranicama gradova i općina (QR kod ispod)
- materijali za građanstvo koji se izrađuju u koordinaciji sa Mrežom Vijeća za prevenciju kriminaliteta gradova i općina SDŽ
- stručni skupovi i tribine u koordinaciji sa Mrežom Vijeća za prevenciju kriminaliteta gradova i općina SDŽ do prosinca 2023.
- tematski istupi stručnjaka iz PU SD i partnera (mediji kao partner i potpora)
- inicijative Vijeća za prevenciju kriminaliteta gradova i općina SDŽ.

Ovo je jedan mali dio negativnih iskustava građana koji su nam se obratili za pomoć:

*GRAĐANIN: „U subotu tokom popodnevna mi se dogodio nesretan slučaj sa mojim bankovnim računom. Naime preko internet stranice sam prodala torbu. Cura mi se javila i poslala mi je link ***, međutim taj link je bio prevara. Kada sam upisala IBAN sa kartice, povukao mi je broj kartice i CVV... s računa mi je skinuto 250 eura....“*

POLICIJA: Nažalost, moram Vam kazati kako je ovaj događaj koji ste opisali prijevara.

Prilikom navodnog “primanja” uplate od prevaranta ste unijeli sve podatke koji štite Vaš kartični promet. Iako je na lažnoj stranici dostavne službe pisalo “primitak” u pozadini stranice je pokrenut postupak naplate s računa. Radi toga je banka u pravu kad Vam je odbila uvažiti reklamaciju jer ste vi koristeći zaštićene podatke autorizirali transakciju.

GRAĐANIN: „Ne znam da li sam se obratila na pravu adresu. Primila sam ovu poruku od nepoznatog pošiljatelja. Poruka je besmislena, ali bi je možda bilo dobro provjeriti jer je očita prijevara. Ja nisam odgovorila na poruku, ali je sigurno poslana na više adresa i netko bi mogao i nasjesti:

„Pozdrav, ja sam Cooper Samuel, privatni odvjetnik pokojnog Alexander Zvonko, državljanin vaše zemlje, bivši izvršni direktor naftne i naftne industrije sa sjedištem u Sjedinjenim Američkim Državama. Dana 3. veljače 2017. moj klijent i njegova obitelj sudjelovali su u prometnoj nesreći na državnoj autocesti Northbound i izgubili živote. Moj klijent je imao račun u iznosu od približno 18.699.800 milijuna dolara kod BB&T banke ovdje u Sjedinjenim Državama. Banka mi je dala ultimatum da odredim korisnika ili rođaka koji će koristiti novac kako bi izbjegao zapljenu fonda. Želio bih da vi budete korisnik.

Bit će poduzeti svi pravni koraci i vaša će primanja biti isplaćena 50% meni i 50% vama. Dat ću vam više pojedinosti kada izravno odgovorite na moju e-poštu.“

POLICIJA: Dobro ste primijetili da se u ovom slučaju radi o pokušaj prijevare, tzv. “fishing” e-mail.

Odgovorom na poruku ne bi nastupila nikakva šteta za Vas, no prevaranti očekuju naivne “nasljednike” ogromnih novčanih sredstava koji će mu unaprijed uplatiti troškove, poreze, naknade i slično kako bi im sredstva stigla na račun. Zanemarite ovu poruku.

GRAĐANIN: „Dobio sam ovu poruku. Nemam račun u toj banci. Znači prevara.: Tijekom vaše posljednje kupnje primijetili smo neobičnu aktivnost na vašoj kreditnoj kartici. Kao sigurnosnu mjeru, privremeno smo suspendirali Vašu bankovnu karticu.

Pozivamo vas da provjerite svoj račun kako biste ga ponovno aktivirali kako ne biste riskirali blokiranje budućih kupnji karticom. Slijedite poveznicu u nastavku kako biste dovršili postupak i prilagodili status svoje kreditne kartice:

Zahvaljujemo na ukazanom povjerenju.

Srdačno

POLICIJA: U ovom slučaju se radi o poznatom vidu prijevare gdje se "obavještava" korisnik o spriječenom napadu na njegovu imovinu, a na priloženom linku se od njega traži da stornira "blokiranu" karticu na način da upiše identifikacijske podatke o računu i kartici.

Naravno, sve to kako bi prevaranti došli do stvarnih autorizacijskih podataka koje bi brzo iskoristili za preuzimanje sredstava sa računa.

U Vašem slučaju bilo je očito da se radi o prijevari jer nemate račun u toj banci, no i drugi pokazatelji ukazuju da se radi o pokušaju prijevare. Osnovno je da se e-mail adresa jedne banke, kao ni bilo koje druge institucije, ne nalazi na domeni ".com".

OSNOVNI POJMOVI I NAJČEŠĆI NAČINI NA KOJI POČINITELJI NAPADAJU

S obzirom na način izvršenja, najčešće se pojavljuju sljedeće vrste prijevara na internetu i putem interneta:

1. **Krađe identiteta** (samostalno kazneno djelo ili pripremna radnja):

   Vishing - Krađa identiteta pozivom: Telefonska prijevara u kojoj počinitelji zovu i pokušavaju navesti sugovornika da otkrije svoje osobne, financijske ili sigurnosne podatke ili da im uplate novčana sredstva.

   Phishing - Mrežna krađa identiteta lažnim porukama e-pošte: Počinitelji šalju lažne poruke e-pošte kojima pokušavaju navesti primatelja na dijeljenje osobnih, financijskih ili sigurnosnih podataka.

   Smishing - Krađa identiteta SMS-om: Pokušaj je počinitelja da dođu do osobnih, financijskih ili sigurnosnih podataka putem tekstualne poruke.

   Krađa osobnih podataka kroz kanale društvenih mreža, poput Facebooka i sl.

2. **CEO prijevara / direktorska prijevara:** počinitelji se predstavljaju da su rukovoditelji ili nadređeni u organizaciji i prijevarom navode djelatnike da uplate novčani iznos na njihov račun ili da neovlašteno doznače novac s poslovnog računa.

3. **BEC (Business Email Compromise) prijevara ili Prijevara s računima**: počinitelji se predstavljaju da su klijenti/dobavljači i navode djelatnike trgovačkog društva da plate buduće račune na drugi bankovni račun.

4. **Krivotvorene internetske stranice banaka:** koristi se lažna e-pošta banke (ili tvrtki za dostavu) s poveznicom na krivotvorenu mrežnu stranicu. Jednom kada neka osoba klikne na poveznicu, koriste se razne metode prikupljanja financijskih i osobnih informacija. Stranica izgleda kao i prava mrežna stranica uz nekoliko sitnih razlika.
   Aktualni oblik ovih prijevara je kada oglašavate prodaju putem oglasnika, počinitelji traže od Vas informacije o računu, kreditnoj kartici, kako bi "uplatili" traženi iznos za vaš oglašeni predmet.
   Primjer: Na internetu oglasniku, na oglas o prodaji artikla se javio potencijalni kupac, kojom prilikom je oštećenom poslao link za upis podataka o bankovnoj kartici, u svrhu "izvršenja uplate". No umjesto uplate za kupnju

artikla, oštećenom je korištenjem podataka njegove bankovne kartice, počinitelj s bankovnog računa izvršio dvije transakcije prema platformi za trgovinu kripto valutama.

5. **Romantične prijevare:** počinitelji 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. **Investicijske prijevare i prijevare u online kupovini:** počinitelji navode osobe da misle da su na tragu pametnog ulaganja, poput ulaganja u virtualne valute ili im daju „izvrsnu" lažnu online ponudu za kupovinu nekog proizvoda.
7. **Ransomware računalni programi - napadi na računala i podatke:** Kada su Vaši podaci na računalima kriptirani, te im više niste u mogućnosti pristupiti, a na Vašu adrese elektroničke pošte dostavljena je ucjenjivačka poruka kojom nepoznate osobe traže uplatu iznosa u virtualnim valutama u zamjenu za pomoć u otključavanju podataka, radi se o tzv. ransomware računalnim programima. To su zlonamjerni programi, koji se distribuiraju od strane nepoznatih osoba, a usmjereni su na građane, različita trgovačka društva, tijela državne vlasti i pravne osobe s javnim ovlastima, s ciljem pribavljanja protupravne financijske koristi.

Kako ne bi sami postali žrtve kaznenog djela:

- pročitajte obavijesti i savjete pružatelja usluge kupnje / prodaje, za sigurnu kupnju putem njihove stranice,
- ako nešto prodajete, za uplatu na vaš račun kupcu je dovoljno poslati samo IBAN broj i vaše ime i prezime a nikako CVC/CVV kod(kod za verifikaciju koji se nalazi na poleđini kartice, a koji se koristi kod internetskih plaćanja),
- nemojte dijeliti kartični pin ili lozinku za online bankarstvo. Ne šaljite novac na neki nepoznat račun bez prethodne provjere, a ako mislite da se radi o lažnom pozivu za uplatu prijavite svojoj banci,
- budite sumnjičavi prema ponudama za unosne investicijske mogućnosti kao što su dionice, obveznice, kripto valute, plemeniti metali i uvijek tražite nepristrani financijski savjet prije nego što date novac ili uložite sredstva nepoznatoj osobi.

POLICIJSKA UPRAVA
SPLITSKO-DALMATINSKA

ŽUPANIJA SPLITSKO-DALMATINSKA
ODBOR ZA SIGURNOST

Budite sumnjičavi i obavite detaljne provjere ukoliko sumnjate na prevaru!

Na CERT-ovim internetskim stranicama www.cert.hr i društvenim mrežama svakodnevno se objavljuju materijali edukativnog sadržaja, objavljuju slike, info grafike i video materijali s popratnim tekstom kao savjeti za zaštitu od napada i prijevara.

Informacije o različitim oblicima internetskih prijevara te savjete kako se zaštiti, možete pronaći na internetskim stranicama Ravnateljstva policije https://policija.gov.hr i na YouTube kanalu MUP-a.

Jedan od najtežih oblika kibernetičkih napada su napadi zlonamjernim ucjenjivačkim softverima koji onemogućuju korisnicima pristup njihovom informacijskom sustavu ili uređaju. Pomoć možete potražiti na internetskoj poveznici dostupnoj na hrvatskom jeziku https://www.nomoreransom.org/cro/index.html na kojoj se nalazi alat pod nazivom KRIPTO ŠERIF.

Igraj. Uči. Pobjedi. Pokaži svoje znanje i zavladaj SefetyNet kvizom o sigurnosti na internetu https://safetynet-kviz.skole.hr