Kyberpodvodníci agresívne zneužívajú aj vojnu na Ukrajine - kradnú osobné údaje aj heslá k bankovým účtom

Strach a neistotu ľudí spôsobenú pandémiou a aktuálne aj vojnovým konfliktom na Ukrajine naplno zneužívajú podvodníci na internete. Pred nárastom kybernetických útokov v tomto čase už varovalo Národné centrum kybernetickej bezpečnosti Slovenska. Škody spôsobené podvodníkmi eviduje v tomto čase aj UNIQA. Hlásenia sa týkajú najmä falošných zbierok a phishing mailov a podvodných sms správ, cez ktoré sa podvodníci dostali k osobným údajom a heslám k bankovým účtom.

Zvýšenú aktivitu ľudí na internete počas pandémie a vojnového konfliktu zneužívajú podvodníci. Neváhajú zneužiť ani vlnu solidarity, ktorú Slováci prejavujú finančnými darmi pre Ukrajinu. Softvérové spoločnosti už varovali pred falošnými humanitárnymi zbierkami, ktoré vznikli krátko po začiatku konfliktu na Ukrajine a hoci sa zatiaľ objavili v zahraničí, predpokladá sa, že čoskoro dorazia aj k nám. Bankové účty, na ktoré majú peniaze smerovať, sa preukázateľne nedajú spojiť s legitímnym subjektom a šíria sa najmä na sociálnych sieťach či prostredníctvom e-mailov.

„Ak chcete našim ukrajinským susedom finančne pomôcť, odporúčame urobiť tak len cez overené organizácie, ktoré majú v tejto oblasti dlhoročné skúsenosti“ radí Zdeněk Hruška, manažér poistenia majetku UNIQA. Zoznam overených organizácií nájdete aj tu: UNIQA reaguje na eskaláciu situácie na Ukrajine plánom pomoci | UNIQA

Veľkým problémom sú aktuálne aj škodlivé emailové a sms správy, ktoré sa snažia vylákať od ľudí peniaze alebo sa **pokúšajú infikovať ich zariadenia**. Pred podvodnými emailmi už varovali zákazníkov banky ale aj Slovenská pošta. Odosielateľ falošných mailov používal zdeformované logo Slovenskej pošty a od adresátov pýtal poplatok za doručenie zásielky. Pošta následne ľudí upozornila, že za doručenie tovaru nikdy nepožaduje peniaze mailom. Za zásielku zaplatí klient buď pri objednávaní tovaru priamo eshopu, alebo na dobierku hotovosťou alebo kartou.

Podvodnou smskou obrali klienta o 2000 EUR

Napriek tomu sa stal obeťou podobných podvodníkov aj náš klient, ktorému prišla sms, nápadne pripomínajúca správy Slovenskej pošty o oznámení doručovania balíka. Tentoraz však s upozornením o zaplatení 2 EUR poplatku za doručenie prostredníctvom platobnej karty. Keďže klient skutočne čakal doručenie balíka, cez priložený link zadal údaje svojej platobnej karty. Rodina ho následne upozornila, že môže ísť o podvod, keďže pošta nikdy platbu vopred nežiada. Kontaktoval teda svoju banku a požiadal o zablokovanie karty. Napriek tomu mu cez viaceré výbery následne z karty odišlo 2000 EUR. Banka mu peniaze odmietla vrátiť s tým, že ona nepochybila.

„ Klient následne kontaktoval asistenčnú službu ku kyberpoisteniu, ktorá prípad prevzala. Po dôkladnej analýze sme prípad uzavreli s tým, že išlo o zneužitie platobnej karty a klientovi sme zaplatili škodu, ktorá mu vznikla,“ popisuje udalosť Z.Hruška z UNIQA.

Podvodníci však stále na kyberútoky zneužívajú aj pandémiu. Naša klientka sa nevedomky stala súčasťou falošnej zbierky, keď dostala mail s linkom na stránku o Covid-19, ktorá prevádzkovala e-shop so zdravotnými pomôckami.

„Zaregistrovaním sa na stránke a objednaním tovaru poskytla prevádzkovateľovi osobné údaje. Po krátkom čase ju známi upozornili na množstvo negatívnych správ na jej osobu, v ktorých jej ľudia vyčítali podvodnú organizáciu finančnej zbierky vedenú pod jej menom,“ popisuje jeden z prípadov Zdeněk Hruška z UNIQA. Pani následne kontaktovala asistenčnú službu poisťovne.

„Tím kyber risk špecialistov začal odsúvať klamlivé správy z predných miest vyhľadávača, čím sa prístup k negatívnym správam postupne znemožnil. Medzitým poisťovňa našla osobu, ktorá správy písala a vyzvala ju, aby ich okamžite vymazala. Na šíriteľa podvodných správ bolo podané trestné oznámenie a musel uhradiť všetky náklady na vzniknuté škody,“ hovorí Z.Hruška.

Odborníci varujú, že základom podvodných mailov je vždy obsah, ktorý má v tomto čase vyvolať silnú emóciu, kvôli ktorej je obeť náchylnejšia kliknúť na nebezpečný link alebo stiahnuť si do svojho zariadenia škodlivú prílohu.

Obrana je jednoduchá: nikdy neklikajte na prílohy v podozrivých e-mailoch. Nikdy neposielajte svoje platobné údaje, a to ani vtedy, keď vám niekto zavolá. Neoznamujte bankové autorizačné SMS kódy ani iným spôsobom neautorizujte platbu cudzej osobe. Kontrolujte e-mailové adresy, odkiaľ Vám správa prišla: spravidla sa ukáže, že nejde o oficiálny kontakt odosielajúcej inštitúcie. Napovedať môže niekedy aj nedokonalá slovenčina. Kontrolujte správnosť webových adries. Dajte si pozor na nezvyčajné výzvy ohľadom využitia aktivačného kľúča vášho internetového bankovníctva alebo na podozrivé e-maily informujúce o zablokovaní vášho účtu.

Ak sa stanete obeťou útoku, okamžite kontaktujte asistenčnú službu

V prípade, že ste už podvodníkom naleteli a tí dostali k údajom o Vašej platobnej karte a zmiznú Vám z účtu peniaze, radíme nečakať. Ak máte k poisteniu domácnosti pripoistené aj kybernetické riziká alebo poistenie Kyberbalík, okamžite kontaktujte asistenčnú službu poisťovne. V prípade, že sa stanete obeťou útoku, máte nárok na kompletnú asistenciu pre nápravu a právne služby – poisťovňa zabezpečí všetky právne úkony a právne kroky tak voči subjektu, ktorý útok spáchal ako aj voči banke, od ktorej si nárokujete vrátenie peňazí. Dokonca môžete splnomocniť poisťovňu a tá prevezme komunikáciu v mene klienta s bankou.

„Ak sa potvrdí, že zo strany klienta nedošlo k pochybeniu a naozaj prišlo k zneužitiu údajov cez podvodný e-shop alebo škodlivý email, poisťovňa uhradí poškodenému náklady na právne zastupovanie a do limitu plnenia aj vzniknutú škodu," hovorí manažér poistenia majetku UNIQA Zdeněk Hruška.

Kyberpoistenie chráni pred útokmi všetkých členov domácnosti

Kyberpoistenie poskytuje ochranu pred nástrahami internetu a zároveň chráni pred finančnými následkami škody, ktorú spôsobí člen domácnosti iným osobám. Poistnú ochranu získajú všetci členovia domácnosti v týchto prípadoch:

- **útoky v rámci elektronických platieb**: ak sa stanete obeťou podvodníkov na internete a z účtu Vám napr. zmiznú peniaze, poisťovňa zabezpečí kompletnú asistenciu pre nápravu, uhradí škody klienta v súvislosti s podvodnou transakciou do limitu plnenia, uhradí náklady na súdne konanie a zabezpečí právne zastúpenie
- **ohrozenie virtuálnej identity:** v prípade zneužitia osobných údajov na podvodné získanie pôžičky či hotovosti máte nárok na právne zastúpenie, úhradu nákladov na súdne konanie, úhradu vzniknutých nákladov na vydanie nových dokladov. Ochrana sa v tomto prípade týka mena a priezviska, adresy, dokladu totožnosti, vodičského preukazu, telefónneho čísla, emailu, IP adresy, hesla a IBAN
- **poškodenie dobrého mena:** ak sa stanete obeťou kyberšikany alebo ohovárania , poisťovňa zabezpečí tzv. „Cleaning" - odstránenie nepravdivých a poškodzujúcich informácií na internete alebo tzv. „Flooding" - vytlačenie takýchto informácií z predných miest vyhľadávačov. Máte tiež nárok na právne zastupovanie a úhradu súvisiacich nákladov
- **riziko nákupu cez internet:** v prípade sporu s e-shopom vyplatíme náhradu za nedoručený, poškodený alebo nekompletný tovar, úhradu priamo vzniknutých škôd do limitu plnenia a máte nárok aj na právne zastupovanie. Poistné plnenie sa týka aj zahraničných e-shopov, pokiaľ bol tovar zaslaný z európskeho územia členského štátu EÚ, Švajčiarska a Nórska.
- ako bonus má poistený občan k dispozícii právne poradenstvo vo forme linky právnych informácií a aktívnu pomoc špecialistov pre danú oblasť na riešenie konkrétnych prípadov