

V čase koronavírusu stúpajú kybernetické útoky na domácnosti – podvodníci útočia aj cez falošné e-shopy na respirátory



Mimoriadnu situáciu vyvolanú šírením koronavírusom aktuálne zneužívajú podvodníci na internete, ktorí sa na úkor vystrašených ľudí snažia obohatiť. Falošné e-shopy s respirátormi, podozrivé súťaže na facebooku o ochranné zdravotné pomôcky ako aj podvodné emaily, ktoré pôsobia, akoby s Vami komunikovala banka, hoci v skutočnosti ide o snahu dostať sa k prístupovým heslám klientov do elektronického bankovníctva. Ponúkame niekoľko rád, ako spoznať podvodníkov a čo robiť, ak ste im už naleteli.

Nedostatok ochranných pomôcok na trhu a zatvorené obchody spôsobili, že ľudia sa snažia mnoho vecí nakúpiť online. „Aktuálne nás klienti vo zvýšenej miere kontaktujú práve kvôli problémom s dodaním online objednaného tovaru cez e-shopy, vrátane tých zo zahraničia. Nie všade ide o podvody, niekde sa dodávky oneskorili kvôli aktuálnej situácii alebo e-shop ukončil činnosť. Každý podnet od klientov však preverujeme a ak majú k domácnosti poistené kybernetické riziká, snažíme sa im pomôcť cez našich právnikov, prípadne náhradou vzniknutej škody,“ hovorí Róbert Koch z oddelenia poistenia majetku UNIQA.

Cez falošný e-shop až k peniazom na Vašom účte

Pri akomkoľvek nákupe cez internet však treba byť v tomto období opatrný, odborníci už varujú pred podvodnými webstránkami v slovenčine aj v češtine, ktoré predávajú zdravotné rúška a infra-teplomery. „Tieto weby sa snažia kradnúť osobné údaje ľudí, ktorí si chcú cez tieto stránky objednať tovar,“ vysvetľuje Ondrej Kubovič, špecialista na digitálnu bezpečnosť zo spoločnosti ESET. Podľa neho útočníci na zvýšenie svojej kredibility na stránky umiestňujú aj falošné recenzie používateľov. Celý web, vrátane objednávkového formulára pritom nie je šifrovaný a osobné údaje tak okrem podvodníkov za týmto webom môžu odchytiť aj ďalší útočníci.

Polícia už upozornila aj na fiktívnu súťaž na facebooku o respirátory. Takýmto spôsobom sa podvodníci snažia vylákať od ľudí informácie

o platobnej karte alebo ich navedú posielat' SMS správy na spolplatnené čísla.

Veľkým problémom sú aktuálne aj škodlivé emailové správy, ktoré sa snažia vylákať od ľudí peniaze alebo sa pokúšajú infikovať ich zariadenia. Základom je vždy obsah, ktorý má v čase koronavírusu vyvolať silnú emóciu, kvôli ktorej je obeť náchylnejšia kliknúť na nebezpečný link alebo stiahnuť si do svojho zariadenia škodlivú prílohu. „*Napríklad v Českej republike šírený spam s tematikou koronavírusu obsahuje škodlivý kód známy ako Fareit, ktorý z infikovaného zariadenia odchyťava heslá uložené v internetových prehliadačoch,*“ upozorňuje ESET. Spoločnosť v posledných dňoch tiež zaznamenala niekoľko e-mailových kampaní, ktoré zneužívajú toto ochorenie a varuje, že aj keď väčšina týchto správ koluje najmä v zahraničí, škodlivé e-maily sa môžu objavovať aj na Slovensku.

Na podvodné e-maily, ktorými sa podvodníci snažia získať prístupové heslá k elektronickému bankovníctvu klientov, už upozornila aj veľká slovenská banka.

Ako spoznať falošný e-shop a podvodný email a čo robiť, ak ste už naleteli

Upozorňujeme, že falošný alebo nedôveryhodný e-shop sa dá spoznať vizuálne na prvý pohľad – zlá gramatika (nepresný preklad do slovenčiny zahraničnými útočníkmi), neúplné alebo chýbajúce informácie o prevádzkovateľovi obchodu, nereálne nízke ceny a pod. „*Ďalším typickým výkričníkom býva chýbajúce šifrovanie komunikácie (httpS na začiatku www adresy), prípadne problémy s elektronickým certifikátom (na ktoré zvyčajne upozorní prehliadač). Žiadny seriózný obchod nebude od svojich zákazníkov požadovať zadanie citlivých údajov prostredníctvom nezabezpečeného kanála,*“ upozorňuje Róbert Koch z oddelenia poistenia majetku UNIQA.

Ak si v online obchode vytvárate konto, základom je kvalitné, zmysluplne dlhé a komplexné heslo, unikátne pre každú dôležitú službu. Údaje o platobnej karte neodporúčame ukladať do konta daného online obchodu.

V prípade, že ste podvodníkom naleteli a cez falošný e-shop podvodníci dostanú k údajom o Vašej platobnej karte a zmiznú Vám z účtu peniaze, radíme nečakať a okamžite kontaktovať asistenčnú službu poisťovne, ak máte k domácnosti poistené aj kybernetické riziká. To isté sa týka prípadu, ak ste nechtiac otvorili škodlivý email a po čase zaregistrujete pohyby na účte, ktoré ste nevykonali. Máte nárok na kompletnú asistenciu pre nápravu a právne služby – poisťovňa zabezpečí všetky právne úkony a právne kroky tak voči subjektu, ktorý útok spáchala ako aj voči banke, od ktorej si nárokuje vrátenie peňazí. Dokonca môžete splnomocniť poisťovňu a tá prevezme komunikáciu v mene klienta s bankou. hovorí Róbert Koch z oddelenia poistenia majetku UNIQA.

Čo robiť, ak kvôli koronavírusu tovar z online obchodu neprišiel

Na finančnú a právnu pomoc máte nárok aj v prípade, ak sa aktuálne sporíte s e-shopom pre poškodený alebo vôbec nedodaný tovar. „*Ak ste si objednali a zaplatili tovar, ktorý Vám neprišiel alebo e-shop medzičasom zanikol, poisťovňa Vám poskytne právnu pomoc a ak sa spor nepodarí vyriešiť do 3 mesiacov, poisťovňa uhradí vzniknutú škodu do limitu plnenia,*“ vysvetľuje R. Koch. Najväčším problémom pri spotrebiteľských sporoch bývajú zahraničné e-shopy, ktoré nepodliehajú kontrole Slovenskej obchodnej inšpekcie (SOI). Kontrolná činnosť SOI sa totiž týka iba podnikateľských subjektov so sídlom na území SR. Poistený klient má však nárok na pomoc aj v prípade zahraničných online obchodov: „*Poistné plnenie sa týka aj zahraničných e-shopov, pokiaľ bol tovar zaslaný z európskeho územia členského štátu EÚ, Švajčiarska a Nórska,*“ upresňuje R. Koch z UNIQA. Znamená to, že náhradu škody nedostanete za tovar objednaný z Číny alebo USA.