Ako byť Smart

a nesadnúť na lep PODVODNÍKOM

MôjAndroid

SmartBanka

Bankové podvody

Najväčšie bankové podvody a ako sa im brániť

Vydavateľstvo:
Virtual studio spol. s r.o.
Pod kanálom 38, Lipovec
03861 Vrútky
IČO: 46943994
IČ DPH: SK2023664621
DIČ: 2023664621
Spoločnosť zapísaná v Obchodnom registri Okresného súdu Žilina, vložka číslo: 58075/L.

Autori:
Miroslav Mudroň
Miroslav Schwamberg
Filip Spevár
Michal Chabada

Marketing:
Miloš Debnár

Grafická úprava:
Michal Lauko

Kontakt:
redakcia@mojelektromobil.sk

OBSAH

Najväčšie bankové podvody a ako sa im brániť

Tento e-book má slúžiť pre všetkých jeho čitateľov ako pomôcka slúžiaca na prevenciu pred podvodníkmi. Obeťou takýchto podvodníkov môže byť naozaj každý, kto používa nejaké zo zariadení na komunikáciu s ostatnými.

V e-booku si prejdeme 10 najväčších a najčastejších podvodov spojených s bankami, ktorým boli bežní ľudia vystavený počas roka 2022. Niektoré z týchto podvodov sú nové, no niektoré fungujú už dlhé roky. Najlepším riešením je hlásenie každého náznaku polícii. Niekedy je však bohužiaľ aj polícia na takéto podvody krátka. Preto cítime našu povinnosť včasne varovať a upozorniť aj našich čitateľov o možných hrozbách.

Aj preto sme sa rozhodli v redakcii vytvoriť takýto e-book, v ktorom si popíšeme akým štýlom podvodníci operujú. Tí sa zameriavajú vo väčšine prípadov na tie najzraniteľnejšie skupiny občanov. Najčastejšie sú to dôchodcovia ale neobchádzajú ani mladšie ročníky. Preto budeme veľmi radi, ak tento e-book ukážete aj svojim rodičom/starým rodičom, a pomôžete im ochrániť sa pred prípadnými pokusmi podvodníkov.

Na záver sme ešte vybrali ďalšie 4 typy podvodov, ktoré sa šírili medzi slovenskou spoločnosťou, no tie už nesúvisia s bankami. Veríme, že sa vám bude manuál páčiť a využijete ho vo svojom bežnom živote.

Úvodník

Svet kybernetických zločincov sa točí v drvivej väčšine prípadov okolo peňazí. Niet preto divu, že práve služby bankovníctva sú v masívnych rozmeroch cieľom podvodov a útokov najrôznejšieho typu. Často ide o ľahko zarobené peniaze, ku ktorým sa zločinci nemusia dopracovať zložitými útokmi. Obete zväčša doplatia na psychologickú manipuláciu alebo jednoducho naletia podvodu.

Platí pritom, že útočníci nemusia vymýšľať koleso, keďže staré praktiky aj naďalej fungujú. Medzi osvedčené nástroje patrí phishing, pri ktorom sa útočníci vydávajú za banku, buď prostredníctvom mailu, SMS správy (smishing) alebo telefonátu (vishing). Obeť väčšinou dostanú pod časový tlak a donútia k unáhlenému konaniu, v rámci ktorého odovzdá útočníkovi citlivé informácie.

Phishingové hrozby dokážu odchytávať a úspešne blokovať aj ESET produkty. Z našich detekčných systémov vyplýva, že za posledný rok tvorili stránky s tematikou financií až 23 % zo všetkých zaznamenaných phishingových webov na Slovensku. Najčastejšie sa útočníci vydávali za ČSOB (20 % prípadov) a Tatra banku (18 % prípadov).

S nástupom nástrojov umelej inteligencie ako ChatGPT sa tiež musíme pripraviť na to, že phishingové podvody budú v blízkej budúcnosti pribúdať a budú kvalitnejšie. Koniec koncov, prípúšťa to aj samotné ChatGPT. Na otázku, či prispeje rozmach umelej inteligencie k nárastu phishingových podvodov, chatbot odpovedá:

„Phishingové podvody často zahŕňajú využitie sociálneho inžinierstva a manipuláciu s dôverou ľudí, aby získali prístup k citlivým informáciám, ako sú heslá, čísla kreditných kariet a iné osobné údaje. Umelá inteligencia môže pomôcť útočníkom zvýšiť účinnosť týchto útokov tým, že im poskytne nástroje na generovanie presvedčivejších a sofistikovanejších phishingových e-mailov, ktoré by mohli byť ťažšie odhaliteľné.“

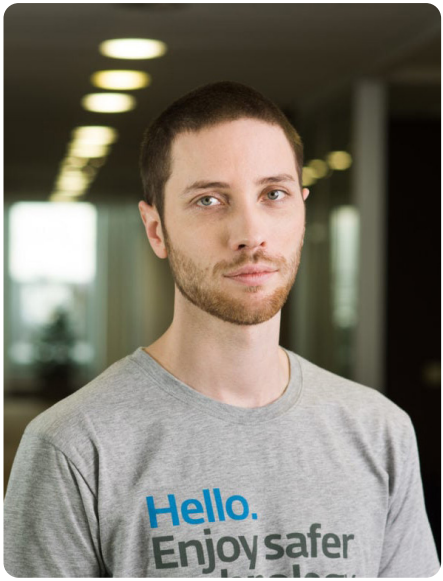
Okrem bežných podvodov striehnu na používateľov aj rôzne bankové malvéry. Ide o škodlivé softvéry, ktoré útočia na bankové aplikácie a snažia sa získať citlivé informácie, ako sú heslá, PIN kódy či údaje z kreditných kariet. Útočníci sa pritom aktuálne zameriavajú čoraz častejšie na mobilné zariadenia a svoj arzenál rozšírili aj o útoky na kryptopeňaženky. Okrem obídenia hesiel sa navyše v nemálo prípadoch snažia získať aj dvojfaktorovú autentifikáciu.

Najbežnejším spôsobom, akým si Android používatelia môžu infikovať svoje zariadenie, je stiahnutie škodlivej aplikácie z neoficiálneho obchodu. Do zariadenia sa môže ale dostať aj zo škodlivých stránok, reklám, podvodných e-mailov či cez zraniteľnosti. Takýto malvér dokáže vytvoriť transparentnú vrstvu nad otvorenou bankovou aplikáciou či kryptopeňaženkou. Keď obeť v dobrej viere zadá prihlasovacie údaje do svojej bankovej aplikácie, v skutočnosti ich píše do neviditeľného formulára, ktorý získané informácie odošle priamo útočníkom.

Bankové hrozby však stále vo významnej miere zachytávame aj na desktopoch. Najčastejšou detekciou na Slovensku je malvérová rodina takzvaných skimmerov známych aj ako Magecart. Ide o škodlivý javascript kód, ktorým útočníci infikujú cieľovú a častokrát aj legitímnu stránku, ktorá následne zbiera údaje o kreditných kartách používateľov. Tento druh útoku tvorí na Slovensku až 70 % odhalených bankových hrozieb pre PC.

Prepadnúť pocitu bezpečia by nemali ani skúsení používatelia. Na ochranu pred bankovými hrozbami odporúčam dodržiavať viaceré opatrenia, ktoré spolu minimalizujú pravdepodobnosť úspešného útoku:

- Sťahovať aplikácie iba z Google Play alebo z oficiálnych kanálov finančných inštitúcií.
- Vždy aktualizovať operačný systém aj všetky aplikácie.
- Používať spoľahlivé viacvrstvové bezpečnostné riešenie, ako na PC, tak aj na mobilných zariadeniach s funkciou anti-phishing. Produkt ESET Mobile Security najnovšie odchytáva aj škodlivé SMS správy.
- Používať unikátne a silné heslá pre každé konto.
- Používať dvojfaktorovú autentifikáciu všade, kde to je možné a ideálne sa vyhnúť jej SMS forme.
- Pri bankových službách používať autorizované aplikácie priamo od vašej banky.



Ondrej Kubovič, špecialista na digitálnu bezpečnosť spoločnosti ESET

Prostredníctvom SMS správ sa šíri nebezpečný podvod, ktorý vás chce obrať o peniaze

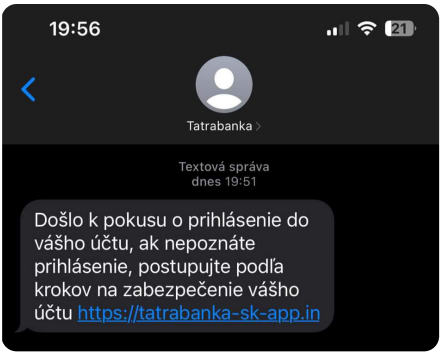
Podvodná správa informuje klienta banky o tom, že bol jeho účet zablokovaný a pre odblokovanie je nutné vykonať niekoľko úkonov. V prvom rade kliknúť na priložený link, ktorý obeť presmeruje na falošnú stránku.

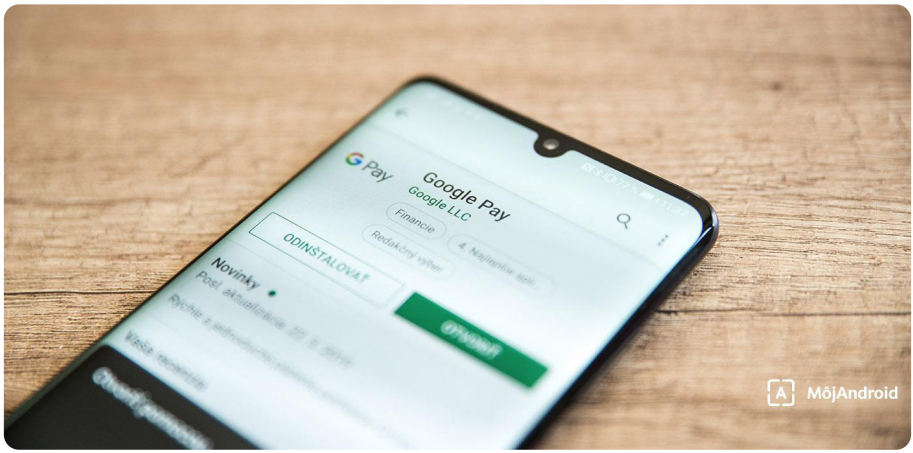
Nie je to internet banking, aj keď sa naň podobá

Tá sa samozrejme snaží tváriť ako internet banking banky. Spočiatku môže pôsobiť dôveryhodne, no väčšinou sa tu objavujú gramatické chyby a url adresa nesedí s url banky. Na tejto stránke je obeť vyzvaná, aby zadala buď prihlasovacie údaje, prípadne údaje o svojej karte.

Podvodníci sa vďaka tomu môžu dostať k prístupovým či súkromným údajom bez toho, aby o tom poškodený vedel. Následne ich môžu využiť na to, aby ho obrali o peniaze. Preto si na takéto SMS správy dávajte pozor. Žiadna banka vás nebude pomocou SMS žiadať o to, aby ste niekam zadávali svoje prihlasovacie údaje.

Tieto SMS správy chodia náhodne. Viacerým sa stalo, že dostali napríklad SMS od Tatra banky, v ktorej nemajú a ani nikdy nemali zriadený účet či inú službu. Keďže sa útočníci neustále snažia, vyzerá to tak, že im to funguje a niektorí Slováci už prišli o svoje peniaze.





Pozor na falošné telefonáty z bánk

Podvodov rôzneho typu v súvislosti s online prostredím, SMS či telefonátmi tu máme naozaj veľa. Slovenskom sa šíril aj podvod, ktorý je pomerne sofistikovaný a odhaliť ho nemusí byť najjednoduchšie. Klienti slovenských bánk sa ocitajú pod paľbou telefonických podvodníkov.

Podvodné telefonáty nie sú novinkou a postupne sa vyvíjajú. Medzi prvými na Slovensku sa objavili také, kde sa osoba na druhej strane sa predstavovala ako podpora Microsoftu a obeť sa snažila presvedčiť o tom, že v rámci ochrany potrebuje získať vzdialený prístup k počítaču. Cieľom už vtedy však bolo získanie finančných prostriedkov vo forme poplatku za údajný servisný zásah, prípadne zisk citlivých osobných údajov. Neskôr podvodníci od Microsoftu prešli priamo na bankový sektor.

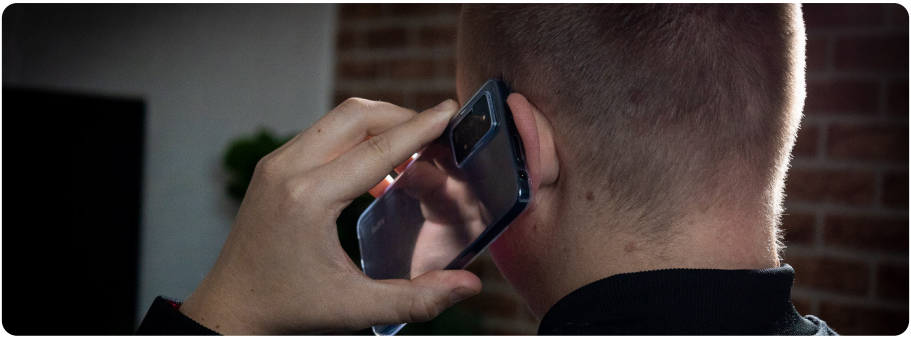
Falošné hovory nie sú nič nezvyčajné, môžu byť v češtine

Tento nový podvod je podobného typu, avšak je náročnejšie ho odhaliť. Podvodníci totiž prepli z anglického jazyka do češtiny. Taktiež telefónne číslo, z ktorého volajú, je zamaskované tak, aby sa javilo, ako reálne číslo banky.

Osoba na druhej strane sa vám predstaví ako zamestnanec banky, v niektorých prípadoch dokonca použije aj meno reálneho pracovníka banky. Obeť informuje o tom, že v jej mene niekto požiadal o úver a má sa obrátiť na pobočku banky, aby túto žiadosť zrušil.

Ešte predtým, ako to obeť urobí, mu zavolá falošný policajt a informuje ho o tom, že bol spáchaný trestný čin v súvislosti s úverovým podvodom. Polícia si s obeťou dokonca pre zvýšenie dôveryhodnosti dohodne aj osobné stretnutie.
Nasledujú ďalšie telefonáty, ktoré majú obeť ešte viac zneistiť. Falošný zamestnanec banky jej ponúkne zaujímavé riešenie tejto situácie. Má si v banke zobrať maximálny možný úver, čím vyčerpá úverový limit a tým podvodníka "predbehne." Ak si klient úver naozaj zoberie, peniaze má previesť na bežný účet dovtedy, kým sa situácia vyrieši.

„V nám známych scenároch nasmerujú klienta do pobočky banky s tým, aby si vybral celú hotovosť z poskytnutého úveru, napríklad pod zámienkou kúpy auta. Poskytnú mu QR kódy s logom banky a navigujú ho do kryptomatov na nákup bitcoinov," upozorňuje Ján Adamovský, šéf bezpečnosti SLSP.



Banky upozorňujú na smishingove SMS správy. Nereagujte na ne

Tatra banka zaznamenala podvod v podobe smishingových SMS správ. Ide o spôsob získavania vašich bankových informácií cez odkaz v SMS správe. Očividne tak ide o podvod veľmi veľkých rozmerov, ktorý vás dokáže pripraviť o vaše úspory. Ďalšie informácie poskytla samotná Tatra banka na svojej oficiálnej stránke.

Banka od vás nikdy nebude žiadať citlivé osobné údaje

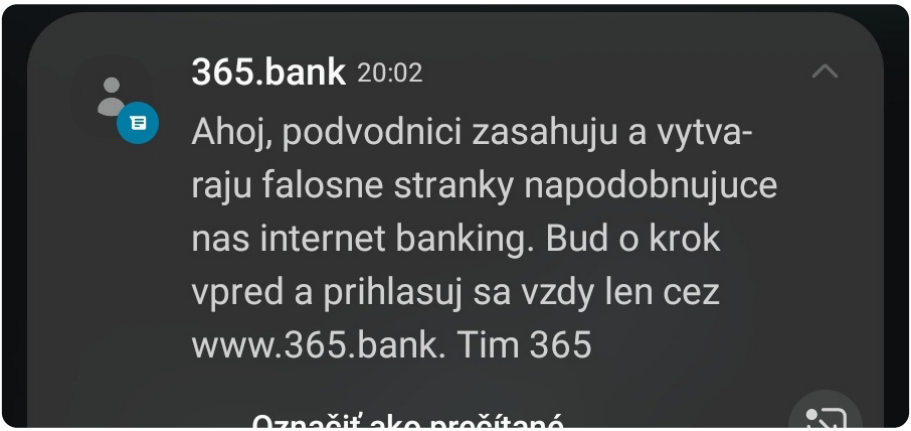
Odosielateľ správy sa vám zobrazí ako Tatra banka, no ide o podvodníka. Cieľom takzvaného "smishingu" je vytvoriť u vás pocit dôvery, na čo sa využíva technické riešenie, ktorému je pre menej skúsených pomerne jednoduché uveriť. Preto by ste na správy tohto typu nemali reagovať, pretože existuje obrovské riziko, že prídete o svoje úspory.

Pokiaľ to je možné, informujte o tom aj vašich blízkych, najmä technicky menej skúsených či starších, ktorí sú často obeťami takýchto nepríjemností. Banka totiž nikdy nežiada citlivé osobné údaje a bankové informácie cez SMS správu či priložený odkaz na nejakú webovú lokalitu.

Tieto údaje sú určené iba pre vás a nikdy ich neprezrádzate ani samotnej banke. Ak ich od vás bude niekto žiadať z nejakého podozrivého dôvodu napríklad mimo oficiálnej bankovej aplikácie, stopercentne ide o podvod.

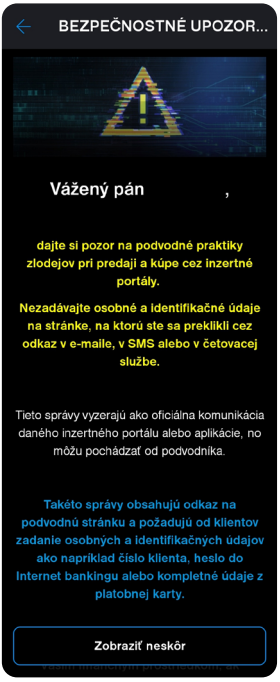
Tieto citlivé údaje nikdy nezdieľajte s treťou stranou, aj keby sa javila ako banka:

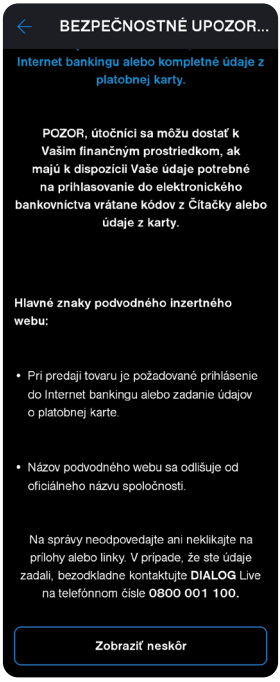
- Číslo platobnej karty, CVV kód a platnosť platobnej karty,
- PID klienta spolu s heslom do Internet bankingu,
- Pri niektorých bankách aj kódy z Karty a čítačky pre riešenie rôznych neštandardných situácií.

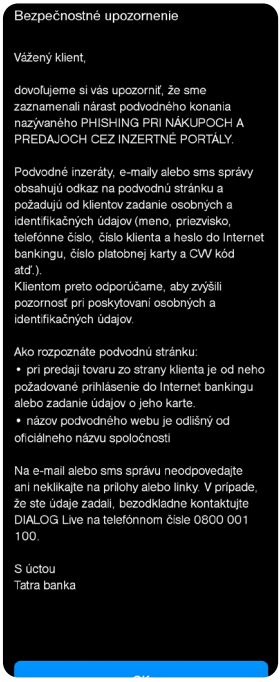


Banky varujú svojich klientov pred podvodnými telefonátmi

Banka mBank uviedla na svojich sociálnych sieťach informáciu o tom, ako sa volajúci vydáva za zamestnanca banky alebo zamestnanca firmy, ktorý zabezpečuje technickú podporu. Snaží sa tak vylákať od nič netušiacich klientov banky citlivé informácie. Ako banka ďalej upozorňuje, pokiaľ vás kontaktujú zamestnanci banky, na overenie totožnosti volaného požadujú vždy len **meno, priezvisko a dátum narodenia**.







Podvodné telefonáty – vishing

Podvodné telefonáty sú označované ako **vishing**. V skratke ide o telefonický rozhovor, ktorým sa podvodník snaží od klienta banky získať citlivé údaje. Ide o osobné údaje, prístupové heslá do internet bankingu alebo mobilnej aplikácie či čísla platobných kariet. Podvodník napríklad pošle klientovi vopred SMS so stručnou informáciou o podozrivej transakcii. Súčasťou SMS správy je aj telefónne číslo, z ktorého sa s ním podvodník následne skontaktuje. Podvodník môže tiež zavolať priamo, bez predošlej SMS správy. Tvrdí, že je napríklad ohrozený počítač alebo smart-

fón, ktorý zákazník banky používa pre správu bankového účtu. Takýto druh podvodu je veľmi dobre premyslený. Veľakrát sa preto klient banky zo strachu o svoje financie ani nezamyslí, že môže ísť o podvod.

Ako sa chrániť pred podobnými telefonátmi?

Informácie ako sú prihlasovacie heslá, údaje z platobnej karty alebo autorizačné SMS kódy za žiadnych okolností **nezdieľajte s treťou osobou**. Telefónne čísla, ktoré využívajú banky sú vždy uvedené na ich stránkach a viete si ich jednoducho overiť. Podvodné telefonáty z iných čísel, by ste mali preto ignorovať, prípadne ich nahlásiť banke.

Ak ste sa predsa len stali obeťou podobného podvodu, je potrebné aby ste si čo najskôr **zmenili všetky prihlasovacie údaje** do internet bankingu prípadne mobilnej aplikácie. Následne je potrebné kontaktovať zákaznícku linku banky.

Populárne finančné a bankové aplikácie sú tiež terčom hackerských útokov

Veľa moderných štúdií preukázalo, že aj nenápadné a na prvý pohľad neškodné aplikácie dokážu ohrozovať vaše zariadenia. V poslednej dobe sú to najmä hry, ktoré postupne napadajú systém v smartfónoch a získavajú citlivé informácie o používateľovi.

Ktoré aplikácie sú terčom útokov najčastejšie?

Vo viacerých populárnych aplikáciách odborníci našli zašifrované súbory s trójskymi koňmi. Tie podľa všetkého napádajú skutočné bankové aplikácie pomocou automatického presmerovania používateľov na falošné stránky.

Na týchto hackermi vytvorených stránkach sa po prihlásení uložia vaše údaje do útočníckej databázy. Po získaní týchto údajov následne útočníci nemajú problém s kradnutím peňazí z vášho účtu.

Top 10 najrozšírenejších vírusov len v marci 2022 napadlo vyše 639 bankových a finančných aplikácií. Až v 121 amerických aplikáciách boli nájdené trójske kone. Aplikácia, ktorá čelila útokom

Dajte si pozor na aktuálne podvody!

1) Pozor na **podvodné SMS a emaily v mene VÚB, ktoré informujú o zablokovaní účtu,** potrebe aktualizácie KYC dotazníka alebo aktivácie platobnej karty. Ak ste takúto správu obdržali, nereagujte na ňu a vymažte ju.

2) Nedajte sa nalákať na **podozrivo výhodné ponuky s investovaním do kryptomien**. Nikdy neposkytujte svoje citlivé údaje tretím osobám, ani vzdialený prístup do svojho zariadenia.

Viac informácií o podvodoch na internete nájdete na: **www.vub.sk**

Ak máte podozrenie, že ste sa stali obeťou podvodu, bezodkladne kontaktujte službu Kontakt 0850 123 000 (+421 2 4855 59 70 zo zahr.) alebo navštívte našu pobočku.

najčastejšie, bola PhonePe. Tá je známa hlavne v Indii a má vyše 100 miliónov stiahnutí. Hackeri veľmi často útočili aj na aplikáciu Binance, ktorá je taktiež v obchode Google Play veľmi obľúbenou. Veľká časť aplikácií bola napadnutá trójskym koňom s názvom Teabot. Ten bol zaznamenaný v 410 prípadoch. Druhým najrozšírenejším je Exbot. Tento druh vírusu napadol približne 324 aplikácií.

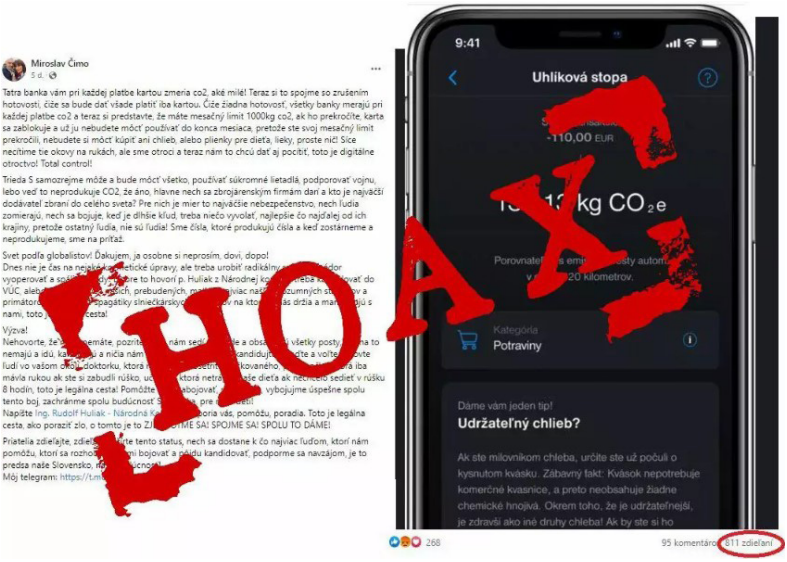
Ďalšími zaznamenanými trójskymi koňmi sú:

- BianLian – Binance, BBVA, Turecké aplikácie
- Cabassous – Barclays, CommBank, Lloys, Santander, Halifax
- Coper – BBVA, Caixa Bank, CommBank, Santander
- EventBot – Barclays, Intensa, BancoPosta, Talianske aplikácie
- FluBot – BBVA, Caixa, Santander a ďalšie Španielske aplikácie
- Medusa – BBVA, CaixaBank, Ziraat
- Sharkbot – Binance, BBVA, Coinbase
- Xenomorph – BBVA, Európske aplikácie

Každý zo spomenutých vírusov sa sústredí na konkrétne typy aplikácií a súborov. Dokým sa Googlu nepodarí vymazať všetky tieto nebezpečné vírusy z Obchodu Play, určite odporúčame dávať veľký pozor pri prihlasovaní a pri zadávaní osobných údajov.

Hoaxy od konšpirátorov neobchádzajú ani banky

Sociálna sieť Facebook sa aj na Slovensku stála útočiskom rôznych podvodníkov a konšpirátorov. Polícia SR teraz na svojom facebookovom profile upozorňuje na nový hoax o funkcii mobilnej aplikácie Tatra Banky.



Hoax šíri dobré známy konšpiračný účet

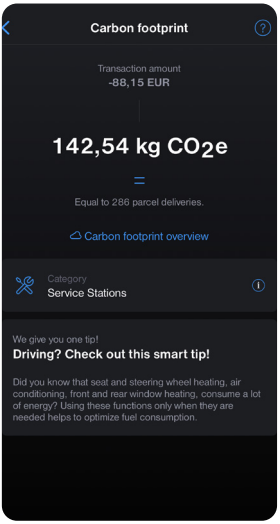
Hoax o aplikácii Tatra Banky zverejnil na svojom facebookovom profile známy konšpirátor s menom „Miroslav Čimo“. Finančná inštitúcia pred istým časom spustila vo svojej aplikácii novú funkciu, ktorá Vám po každej platbe oznámi objem vyprodukovanej uhlíkovej stopy. Banka chce poukazovať na dopady klimatickej krízy a funkcia má pre nakupujúcich predstavovať akýsi výkričník.

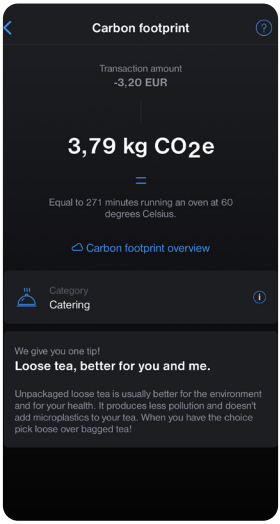
Konšpirátor sa však snaží presvedčiť o tom, že Tatra banka bude využívať dáta o objeme spotrebovaného oxidu uhličitého na našu kontrolu. Tvrdí, že finančná inštitúcia si po čase zmyslí, koľko CO2 vám denne dovolí spotrebovať. Počká si na moment, keď to prepálite a následne z vás spraví otrokov. Táto jeho konšpirácia však absolútne nedáva logiku a to z viacerých dôvodov.

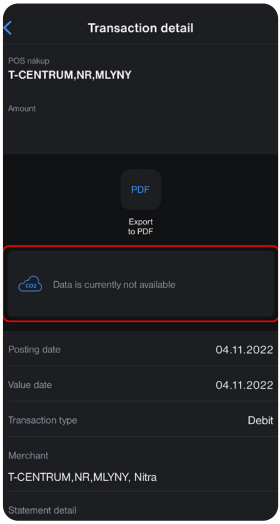
Funkcia aplikácie môže mať len edukatívny charakter

Hovorkyňa Tatra banky Simona Miklošovičová potvrdila, že meranie uhlíkovej stopy má výhradne edukatívny charakter. Funkcionalita nie je a ani logicky nemôže byť nástrojom na kontrolu klientov cez ich účty alebo prostriedkom na blokovanie platieb. Banka nemôže klientom spotrebu CO2 zakázať, ale len na ňu upozorňovať.

A určite kvôli tomu nebude obmedzovať alebo dokonca zakazovať ich platby, pretože by tým išla proti sebe a svojím príjmom. Navyše sa dá táto funkcionalita v aplikácii aj zakázať, ak človek považuje evidentné globálne otepľovanie za hoax. Cieľom konšpirátora je tak len získať vyšší počet sledovateľov. Často tiež konšpirátori pracujú na politickú objednávku s cieľom všetko spochybňovať a zasievať neistotu do systému.







Aj tieto aplikácie dokážu ukradnúť vaše bankové údaje

Stále sa objavuje čoraz viac aplikácií so škodlivým malvérom, ktorého záujmom je ukradnúť vaše bankové údaje. Ide o prihlasovacie informácie k vášmu bankovému účtu, PIN kódy, heslá a ďalšie dáta, ku ktorým by ste mali mať prístup len a len vy. Pokiaľ máte nainštalovanú čo i len jednu z nasledujúcich aplikácií, ihneď ju odinštalujte.

Pozor na nasledujúce aplikácie, ktoré sú schopné narobiť poriadnu neplechu

Malvér je okrem iných nekalých činností schopný i čítať vaše prijaté textové správy, čo je dosť zlým znamením. Horšia je však určite krádež bankových informácií. Existujú aplikácie, ktoré pomáhajú k prenášaniu malvéru cez ochranný systém Obchodu Play.

Títo zlomyseľní aktéri zároveň pomáhajú ďalším vývojárom aplikácií s obsahom škodlivých kódov dostať sa do Obchodu Play a ukradnúť bankové údaje ich používateľom. Toto sú aplikácie, ktoré sa vyznačujú týmto malvérom a v prípade, že sa nachádzajú aj na vašom mobilnom zariadení, mali by ste ich okamžite odinštalovať:

Zoznam aplikácií s malvérom na kradnutie bankových informácií v Obchode Google Play:

Aj keby ich Google zo svojho Obchodu Play vymazal, jednotlivé aplikácie sa stále môžu nachádzať nainštalované na vašom smartfóne. Skvelou správou je, že Google robil minulý rok výraznejšie zmeny v politike Obchodu Play. Zakázané bude/bolo jednotlivým aplikáciám zobrazovanie reklám na celú obrazovku, ktoré nie je možné preskočiť do 15 sekúnd.

Výnimkou však budú prípady, kedy táto forma reklám bude schopná hráčom mobilných hier odomknúť nejaké výhody, za ktoré by inak bolo

potrebné platiť skutočnými peniazmi. Ďalej platí, že aplikácie, ktoré kopírujú logá, vzhľad či názvy iných aplikácií, boli počiatkom 30. augusta vymazávané. Od tohto dátumu americký gigant robí poriadok aj s VPN aplikáciami, ktoré majú zbierať dáta používateľa a zarábať na ňom prostredníctvom kliknutí na zobrazované reklamy.

Podvodníci napádajú bankové aplikácie novými spôsobmi

Aplikácie, ktoré poskytujú bankové služby, sú v dnešnej dobe veľmi populárne. Problémom však je, že sa na tieto aplikácie radi zameriavajú aj podvodníci. Ich útoky na aplikácie, aj s následným využívaním falošných bankových prevodov, vzrástli od roku 2015 až o 600 %.

Aké nové hrozby môžeme očakávať od podvodníkov?

Výskumníci v oblasti internetovej bezpečnosti zistili, že aplikácie s mobilným bankovníctvom sú jednými z najviac atakovaných. Podvodníci totiž prišli na spôsob, ktorým dokážu obísť antivírusy a obmedzenia Obchodu Play.

Pomocou nimi vytvorených aplikácií pomaly prenášajú vírus do zariadení. Kvôli pomalému aktualizovaniu a prenášaniu nebezpečných kódov do zariadenia, ani antivírus nedokáže zachytiť takúto hrozbu. Akonáhle podvodníci dokončia prenos malvéru do zariadenia, okamžite začnú sťahovať nebezpečné aplikácie s trojskými koňmi pre bankové aplikácie bez vášho povolenia.

Aj napriek tomu, že Google neustále vydáva bezpečnostné aktualizácie bezpečnostných podmienok pre aplikácie v Obchode Play, si dokážu podvodníci nájsť nový spôsob, akým tento systém obísť.

Všetky mobilné aplikácie obsahujú tisíce riadkov kódu, ktorý Google Play každodenne kontroluje. Aplikácie podvodníkov však dokážu prejsť týmito kontrolami pretože vyzerajú ako hry, či kvízy, ktoré len zakrývajú nekalé plány hackerov. Častokrát si preto mnoho používateľov za účelom spríjemnenia voľných chvíľ nainštaluje na oko bezpečnú hru, ktorá ale skrýva nebezpečný kód, ktorý len tak neodhalíme. Po nainštalovaní kódu si už podvodníci môžu robiť s vaším smartfónom, čo sa im zachce a to všetko aj bez vášho vedomia.

Ako by sa dalo predísť napadnutiu bankovej aplikácie?

Niektoré z nebezpečných malvérov umožňujú útočníkom kradnúť vaše používateľské mená a heslá. Aj keď neexistuje spôsob na zastavenie týchto hrozieb, určite im môžete predísť pomocou antivírusov, lepšou autentifikáciou medzi klientom a serverom alebo dôkladnejšou ochranou aplikácií.

Všetky obchody s aplikáciami neustále pracujú na nových bezpečnostných aktualizáciách.

Veľké technologické spoločnosti sa každodenne stretávajú s novými aplikáciami. Preto je takmer nemožné vytriediť tie, ktoré sú tvorené podvodníkmi. Pred niekoľkými rokmi sa banky snažili upozorňovať na hackerov a podvodníkov aj pomocou emailov alebo SMS správ.

Aj napriek všetkým upozorneniam sa určite nájde niekto, kto sa nechá nachytať. Preto banky varujú pred neznámymi emailami a hlavne pred nebezpečnými aplikáciami, a to hlavne kvôli neustálemu vývoju podvodníckych stratégií.

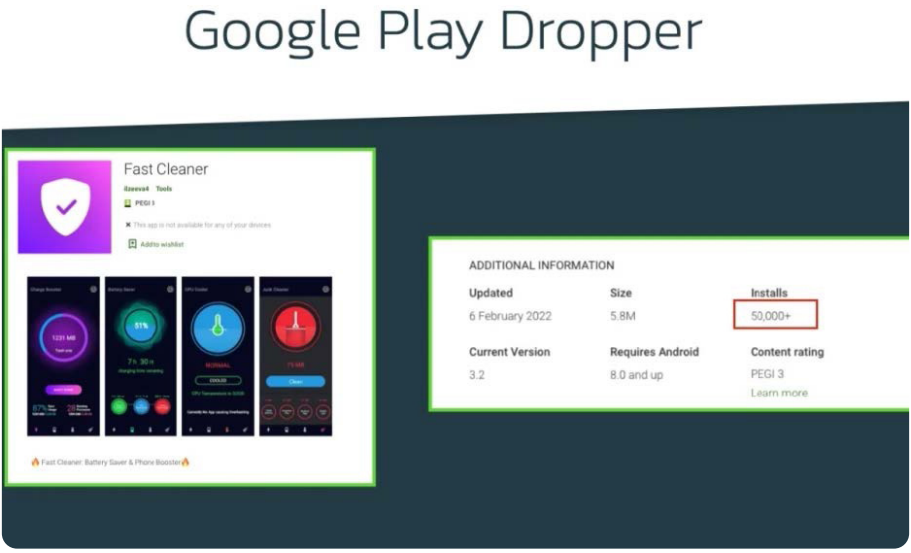
Banky a poskytovatelia služieb v bankovníctve nemajú žiadny vplyv na to, čo robíte na svojom smartfóne mimo ich aplikácie. Aj keď si zákazníci myslia, že sa banka nonstop stará o ich peniaze, tak zodpovednosť nesie hlavne majiteľ smartfónu. Na zredukovanie týchto prípadných útokov by mali bankové aplikácie sprísniť svoj bezpečnostný systém. Minimálne tak, aby dokázal odhaliť všetky nebezpečné neautorizované zásahy do aplikácie.

Zatiaľ čo odborníci pracujú na vyriešení aktuálneho spôsobu týchto útokov si podvodníci určite vylepšujú svoje technológie a aplikácie. V priebehu aktuálneho ale aj budúceho roka budú výskumníci pokračovať v dokumentovaní a zabraňovaní pred útokmi.

Aplikácie často kradnú používateľom údaje od internetbankingu

V Obchode Play sa už veľakrát našla aplikácia, ktorá priniesla používateľom viac škody ako úžitku. Jednu z nich bolo možné nájsť pod názvom Fast Cleaner a pred odstránením stihla nazbierať 50 tisíc inštalácií. Najpopulárnejšia bola v Portugalsku a Španielsku, pričom prvýkrát sa v Obchode Play objavila koncom januára 2022. Aplikácia sa tvárila ako užitočný čistič smartfónu, ktorý vám mal pomôcť zlepšiť výkon zariadenia a predĺžiť výdrž batérie.

V skutočnosti však zariadenia infikovala novým malvérom s označením Xenomorph. Napadnutým používateľom našťastie netrvalo dlho odhaliť sku-



točný zámer aplikácie a na prítomnosť malvéru a podozrivého správania upozornili v recenziách.

Dobrou správou taktiež je, že malvér bol odhalený v rannom štádiu svojho vývoja, čo znamená, že niektoré z jeho škodlivých schopností neboli zatiaľ funkčné. Hrozí však, že jeho vyvinutejšia verzia v budúcnosti infikuje ďalšie smartfóny prostredníctvom iných napadnutých aplikácií. Vtedy môže dôjsť ku krádeži prihlasovacích údajov do internet bankingu používateľov, rovnako ako v prípade podobného malvéru Alien.

Ak ste si aplikáciu do svojho zariadenia nainštalovali, okamžite ju vymažte. Následne skontrolujte stav svojho bankového účtu, či nedošlo k neoprávneným platbám. Taktiež sa odporúča zmeniť heslo aj PIN na prihlásenie do internet bankingu.

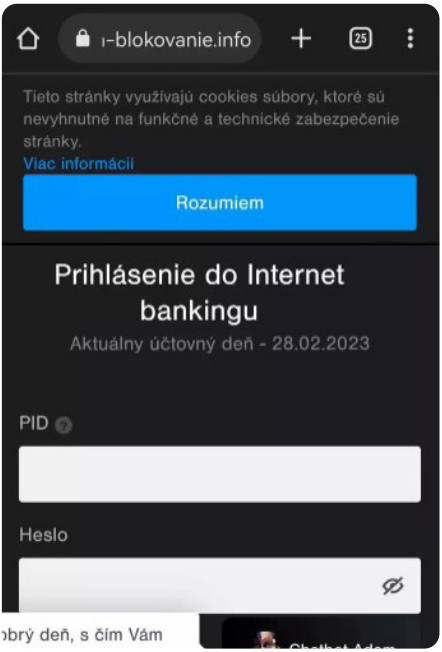
V mene banky sa šírili podvodné e-maily

Ide o starý známy podvod, ktorým sa útočníci snažia od klientov banky získať údaje platobnej karty alebo prihlasovacie údaje do internet bankingu. Používateľ dostane e-mail, ktorý sa snaží tváriť ako oficiálna správa od banky, no veľmi sa mu to nedarí.

Jeho grafické spracovanie pôsobí neprofesionálne a už hneď pri pohľade na adresu odosielateľa vieme, že správa nebola odoslaná bankou. Falošný e-mail by sa nezaobišiel bez odkazu na inú stránku. V tomto prípade s presmerovaním na web imitujúci skutočný internet banking.

Odhaliť falošné e-maily a SMS správy nemusí byť zložité

Rozposielať falošné e-maily a SMS správy je v súčasnosti trendom medzi podvodníkmi. Okrem dobrého mena rôznych bánk zneužívajú aj Slovenskú poštu a kuriérske spoločnosti. No aj napriek rozmanitosti falošných správ je útočníkov možné jednoducho odhaliť. V prípade e-mailov je ako prvé potrebné skontrolovať adresu odosielateľa. Pokiaľ obsahuje cudzojazyčné slová a koncovky, prípadne náhodné písmená a čísla, vymažte ho a neklikajte na priložené odkazy.



Pravosť správy nám pomôže určiť aj tvar priloženého odkazu. Opäť platí, že spoločnosti len zriedkavo odkazujú svojich klientov na stránky, ktoré majú na začiatku URL adresy množstvo náhodne generovaných písmen a čísel, cudzojazyčné slová alebo koncovku inú ako ".sk".

Ak si nie ste istí, či sú e-mail alebo SMS správa falošné, overte si to priamo na pobočke banky alebo prostredníctvom jej oficiálnej webovej stránky.

Kaufland rozdáva darčeky. Alebo nie? Slovenskom sa šíril ďalší podvod

V dnešnej dobe sa rôzni podvodníci nezameriavajú len na banky a finančné inštitúcie. Čoraz častejšie sa môžeme aj na sociálnych sieťach stretnúť s tým, že sa takýto ľudia vydávajú za iné inštitúcie, ako napríklad obchodné reťazce.

Tentokrát vytvorili na sociálnej sieti stránku s oficiálnym názvom a logom vo fotografii, čo sa tvári ako originálna fanúšikovská stránka **Kauflandu**.

V príspevku sú uvedené mesiace od januára až po december. Podľa "usporiadateľov" súťaže si stačí vybrať váš mesiac narodenia, napísať ho do správy a výhra je vaša. Veľmi jednoduchý spôsob ako nalákať ľudí, ktorí sa do súťaže zapoja, aj keď je vopred jasné, že výhra nebude žiadna. A zdá sa, že to funguje, lebo na súťaž reagovalo viac ako 500 ľudí, aj to len v komentároch.

Podvod a jeho typické znaky

Pozornému oku je už na prvý pohľad jasné, že ide o podvodnú stránku. Samozrejme aj všetky súťaže, ktoré sú na nej organizované, nebudú založené na reálnej výhre. Profil na Facebooku existoval len pár dní. Na spoločnosť Kaufland, ktorá pôsobí na slovenskom trhu už niekoľko rokov, je to prinajmenšom podozrivé.

Na stránke sa väčšinou nachádzajú iba súťaže. Obchodný reťazec by za bežných okolností neponúkal svojim zákazníkom iba atraktívne súťaže. Jeho hlavnou úlohou je predsa predávať. Okrem toho na podvodnej stránke nie sú žiadni sledovatelia, žiadne recenzie, žiadne ďalšie kontaktné informácie o samotnej spoločnosti. Tu by sa už mal zamyslieť každý, kto je ochotný riskovať posielanie svojich citlivých informácií podvodníkom cez aplikáciu Messenger.

Neznalosť jazyka a gramatické chyby

Krásne hostesky na úvodnej fotografii, originálny záber z predajne Kauflandu a k tomu balóny ako efektná dekorácia na umocnenie pompéznosti súťaže. Stačí sa však pozrieť na reklamný pútač a každému je hneď jasné, že fotografia nie je zo Slovenska. Na prvý pohľad to vyzerá ako poľština. Pri počte predajní, ktoré má Kaufland na Slovensku, je prinajmenšom zvláštne, že by pre svoju súťaž ako hlavný pútač zvolil fotku zo zahraničia.

Mesiace, ktoré sú v príspevku, začínajú niektoré veľkými písmenami, niektoré zas naopak malými. Aj napriek tomu, že niektorí ľudia písali do komentárov nezmyselné odpovede, podvodníci reagovali, akoby samotnému textu ani nerozumeli.

Dobre premyslený podvod

Aj napriek viacerým chybám na stránke či podvodným príspevkom, podvodníci zdieľajú originálne príspevky spoločnosti Kaufland. Ak si niektorý z potenciálnych podvedených zákazníkov pozrie len pár posledných príspevkov, je veľmi pravdepodobné, že podvodnej stránke uverí. Obzvlášť ak sa jedná o aktuálne letáky, špeciálne akcie z reklám a podobne, ktoré každý pozná či už z televízie alebo z tlače.

Podvod tohto typu spočíva väčšinou v tom, že od vás podvodník so zámienkou prebratia výhry vypýta údaje vašej platobnej karty. Existuje ale ešte jedna, menej nebezpečná možnosť. Stránka si takýmito súťažami naláka sledovateľov, neskôr sa premenuje a výhodne predá.

Podvodníci sa už neskrývajú len za vojakov a banky, ale aj políciu

Rozdiel medzi pravou políciou a podvodníkmi je hlavne ten, že polícia vás neosloví prostredníctvom mobilného zariadenia. Ak by sa s vami chcela polícia skontaktovať, riešila by to oficiálnou cestou alebo priamo.

Ako rozoznať v hovore podvodníka?

Osoba na druhej strane tvrdí, že evidujú problém s vašou ID kartou alebo občianskym preukazom
Všetky zatiaľ nahlásené hovory mali rôzne verzie. Niektoré končili vydieraním, že "polícia" nespolupracujúcim môže do 45 minút zabaviť majetok. Iné sa zase líšili hneď na začiatku. Podvodníci nevinných ľudí obvinili z trestných činov, alebo že sa niekto iný dopustil trestného činu s ich občianskym preukazom, a že na volanú osobu je vydaný zatykač.

- Tel. č. sa zobrazuje ako klasické slovenské číslo v tvare +421 XXX XXX XXX *(namiesto X sú čísla)*
- Po zdvihnutí hovoru počuť monotónny hlas rozprávajúci lámanou angličtinou
- Osoba na druhej strane sa predstaví ako príslušník Slovak Police Force alebo Interpolu (Medzinárodná policajná organizácia)

Každopádne, nič z toho nie je pravda. Podvodníci sa vás len snažia vystresovať, aby ste s nimi pod tlakom ľahšie spolupracovali.

Na čo si obzvlášť dávajte pozor je, že podvodníci využívajú aj automat. Teda podvodníci môžu volať, respektíve sa skrývať za číslo niekoho, koho už máte uloženého v kontaktoch. Človek, ktorého telefónne číslo bolo takto zneužité však vôbec netuší, že niekto používa jeho meno (číslo), aby sa vám podvodník dovolal. Robí to "zaňho" spomínaný automat – robot. Tým nechceme povedať, že by ste nemali nikomu dvíhať telefón, to nie. Len, akonáhle sa vám hlas z druhej strany nepozdáva, hovor zložte.

Čo robiť, keď máte podozrenie, že vám volá podvodník?

- Zložte hovor, nekomunikujte s druhou stranou, ak máte podozrenie, že ide o podvodníkov
- Neposkytujte žiadne osobné informácie cez telefón
- Nahláste telefónne číslo, prostredníctvom ktorého sa vás snažil podvodník kontaktovať
- Kontaktujte políciu

Pozri, kto zomrel pri tragickej nehode, myslím, že ho poznáš. Messengerom sa šíri nebezpečný podvod

Ak vám od vášho priateľa na Facebooku prišla táto správa s odkazom, neklikajte na ňu. Môže to síce vyzerať tak, že vám ju poslala osoba, ktorú dobre poznáte, no ide o podvod. **"Pozri, kto zomrel pri tragickej nehode, myslím, že ho poznáš."**

Na podvod upozorňuje už aj facebookový profil Hoaxy a podvody – Polícia SR. Tieto správy boli výrazne rozšírené v novembri a je veľmi pravdepodobne, že ste ju dostali už aj vy. Správa obsahuje **link, na ktorý by ste určite nemali kliknúť**.

Ak tak urobíte, budete presmerovaní na falošnú prihlasovaciu stránku Facebooku, ktorej cieľom je odchytiť vaše prihlasovacie údaje. Ak tak urobíte, útočníkovi vlastne odovzdáte kompletnú kontrolu nad vaším účtom. **Záchranou môže byť ešte dvojfaktorová autentifikácia, ktorú určite odporúčame zriadiť**.

Ak ste na link klikli, no svoje prihlasovacie údaje ste nezadali, nemusíte sa ničoho obávať. Ak ste ich zadali, **mali by ste ich čo najrýchlejšie zmeniť**. Ešte predtým, ako sa o prihlásenie pokúsi útočník a zmení ich sám. V tom prípade sa už k svojmu Facebook účtu nikdy nedostanete.

Príklady podvodných SMS a správ zo Slovenska:

ESET INTERNET SECURITY

Pokročilá digitálna ochrana pred všetkými druhmi hrozieb

Ochrana online platieb
Zabezpečí vaše online bankovníctvo a nákupy.

Strážca siete
Skontroluje zraniteľnosti vášho Wi-Fi routera.

Rodičovská kontrola
Zabráni, aby vaše deti videli nevhodný obsah.

Progress. Protected.

www.eset.sk