Rozhovor s Romanom Fusekom: Bezpečnosť elektronického bankovníctva

1. 2. 2016; Viera Horáková; Rozhlasová stanica Regina

Viera Horáková, moderátorka:

"Elektronické platby a bezpečnosť elektronického bankovníctva, to je ďalšia téma, o ktorej sa budeme zhovárať s riaditeľom odboru ochrany finančných spotrebiteľov Národnej banky Slovenska Romanom Fusekom.

Bezpečnosť sa rovná autorizácia príkazov. Povedzme najprv, ako vnímať, čo je to vlastne tá autorizácia?"

Roman Fusek:

"Autorizácia, to je kľúčové slovo, o ktorom sa budeme teraz baviť zvyšok relácie. Ide v zásade o to, že autorizáciou banke potvrdzujete, že ten príkaz dávate vy. V prípade, ak prídete na pobočku banky, tak autorizujete svoj príkaz podpisom, ktorý porovnáva banka so vzorovým podpisom. To je taký ten najbežnejší a ľuďom v podstate veľmi blízky spôsob autorizácie. Dnes ale nie všade je možné urobiť podpis, elektronický podpis, taký ten kódový elektronický podpis, ktorý poznáme v styku so štátnymi orgánmi nefunguje ideálne v súkromnej sfére, čiže elektronický podpis sa veľmi používať nedá. preto banky majú vlastné systémy, akým spôsobom autorizujete svoje platby, pokiaľ ich robíte elektronicky. Takže autorizácia je inými slovami potvrdenie toho, že ste platbu realizovali vy."

Viera Horáková:

"Vy ste povedali, že tak, ako sa správame zodpovedne k svojim peniazom, k bankomatovej karte, k peňaženke, ktorú nenosíme v zadnom vrecku nohavíc, tak tak by sme mali zodpovedne správať, aj keď využívame tú inú formu."

Roman Fusek:

"Áno, platia úplne rovnaké pravidlá. Pre nás je úplne bežné, keď máme bankovky pri ruke, tak že si ich chránime nejakým spôsobom, každý má vlastný overený spôsob, ako sa nedať okradnúť. A rovnako by sme sa nemali nechať okradnúť ani v elektronickom bankovníctve. Tie peniaze sú úplne rovnaké, akurát nám rovnaké nepripadajú, pretože sú to len nejaké čísielka na monitore, ale majú úplne rovnakú hodnotu a preto pri nich platia tiež určité bezpečnostné zásady rovnako, ako tá peňaženka v zadnom vrecku nohavíc by nemal byť."

Viera Horáková:

"Natíska sa otázka, aké zásady?"

Roman Fusek:

"Závisí od toho, akú formu elektronického bankovníctva si rozoberieme, máme ich niekoľko takých tých bežných prípadov. To, čo vnímame pod elektronickým bankovníctvom sú jednak prístupy do internet bankingu, dnes už je možné urobiť internet banking aj prostredníctvom mobil bankingu. To je to, že pristupujete zo svojho mobilného telefónu do svojho bežného účtu, ktorý používate na platby. A potom sú to ešte elektronické prevody prostredníctvom internetových platieb. To sú platby, ktoré realizujete napríklad, ak si nakupujete niečo cez internet a urobíte rovno platbu za tovar, ktorý si nakúpite, tak to je internetová platba, ktorá tiež vyžaduje určité pravidlá pre to, aby ste mali istotu, že ju spravíte bezpečne."

Viera Horáková:

"Tak si rozmeňme na drobné, spomínali ste prístupy do internet bankingu. Na čo si dávať pozor, ako postupovať?"

Roman Fusek:

"Dôležité je, úplne taká prvotná zásada, rozmýšľať nad tým zariadením, z ktorého pristupujete do internet bankingu. To znamená, že ak pristupujete zo svojho počítača doma zo svojej internej siete, od svojho internetového providera, tak je to plus mínus ok. Dôležité je ale v tomto prípade, aby ste mali istotu, že ten počítač je zabezpečený proti vírusom, proti tzv. malvéru, čo je nejaký škodlivý obsah, ktorý vám rôzni hackeri sa snažia nahrať do počítača. Dnešná relácia bude plná cudzích slov, čiže budeme sa snažiť rozšifrovávať postupne tie slovíčka. Dôležité je, aby ste ten počítač, ktorý používate na internet, zabezpečili nejakým antivírusom a nejakou súvisiacou ochranou, ktorá súvisí s antivírusom."

Viera Horáková:

"Ako to zabezpečíme?"

Roman Fusek:

"Ak si kúpite antivírusový program, ktorý stojí dneska niekoľko desiatok eur, tak to máte určite v istote, pretože tam dochádza aj k pravidelným aktualizáciám antivírusov a tie firmy, ktoré sa tým zaoberajú vyhľadávajú práve takýto škodlivý obsah a snažia sa chrániť klientov pred ním. Antivírus sa dá získať z internetu aj zadarmo, nie je síce taký dobrý ako keď si ho kúpite, ale je dobré zainvestovať do, či už používate povedzme počítač, tablet, pristupujete cez WiFi do nejakej siete, tak určite máte na svojom počítači antivírus."

Viera Horáková:

"A odkiaľ viem, že ho mám?"

Roman Fusek:

"Zobrazuje sa vám ikonka antivírová na počítači, ten bežný používateľ počítača by mal vedieť, či antivírus má alebo nemá. Keď nemá istotu, tak sa treba obrátiť na profesionála a spýtať sa ho teda, že či v ktoromkoľvek obchode, ktorý sa zaoberá elektronikou, počítačmi, tak vám vedia odporučiť antivírusovú ochranu nejakú. Ja to zdôrazňujem práve kvôli tomu, že mnohé banky to, že pristupujete z počítača s antivírovou ochranou, do svojho internet bankingu majú vo svojich podmienkach. To znamená, že by ste mali mať počítač zabezpečený takouto antivírusovou ochranou, aby ste neporušili obchodné podmienky banky pri používaní internet bankingu."

Viera Horáková:

"Vy ste predchvíľočkou povedali, že pokiaľ používam domáci počítač, je to viac-menej plus mínus ok. To znamená, že aj tento program je to plus."

Roman Fusek:

"Áno, je to dôležité, práve preto, že hoci používate program doma, tak zvonku cez internetovú sieť sa do toho počítača môže nabúrať ktokoľvek a dneska sú tu už v podstate zločinecké skupiny, ktoré sa zaoberajú práve takýmito vecami, takýmito elektronickými útokmi na počítače bežných ľudí práve s cieľom vykradnúť účty ľudí. Dôležitá zásada v prípade, ak nepoužívate počítač doma, to znamená, že internetová kaviareň alebo ste niekde na námestí, radšej tam prevody z účtu nerobte. Cez nezabezpečenú WiFi sieť naozaj neodporúčam robiť bankové prevody."

Viera Horáková:

"A čo riaditeľ odboru ochrany finančných spotrebiteľov Národnej banky Slovenska Roman Fusek odporúča, o tom už o chvíľu.

Viera Horáková:

"Zhovárame sa s riaditeľom odboru ochrany finančných spotrebiteľov Národnej banky Slovenska Romanom Fusekom, hovoríme o bezpečnosti elektronického bankovníctva. Hovorili sme, že tak, ako sa zodpovedne správame k peniazom, k peňaženke, tak by sme zodpovedne sa mali správať aj pri používaní elektronického spôsobu vybavovania. Takže elektronické platby, o tom by sme sa mohli rozprávať teraz."

Roman Fusek:

"Čiže keď chcete elektronicky spraviť platbu v internet bankingu, ale chcete si niečo kúpiť a realizovať platbu priamo cez svoju kreditnú alebo platobnú kartu, tak je veľmi dôležité v prvom rade si overiť, či ste na tzv. zabezpečenej stránke alebo stránke zabezpečeného obchodníka..."

Viera Horáková:

"Čo to znamená?"

Roman Fusek:

"Znamená to, že sa nachádzate na internetovej stránke, ktorá začína takým zámkom tam, kde máte riadok, na ktorej stránke sa nachádzate, tak začína spravidla zámkom, ktorý máva zelenú farbu a za tým je https. To "s" je dôležité na konci, to znamená, že sa nachádzate v zabezpečenej elektronickej komunikácii a údaje, ktoré budete nahadzovať zo svojej platobnej karty do toho systému, teda bude to od vás chcieť číslo platobnej karty, bude to od vás chcieť meno, priezvisko komu bola tá karta vydaná, kedy karta exspiruje, čiže dokedy platí, a potom bezpečnostný kód z druhej strany platobnej karty, tak pokiaľ nie ste na zabezpečenej stránke, tak určite tú platbu nerealizujte. Dnes už viac-menej vo veľkej skupine takýchto internetových stránok a internetových predajov je ešte vyššia forma zabezpečenia, tzv. 3D Secure, čo je systém, kde si po realizácii platby, po zadaní týchto čísiel, keď dáte enter, tak ešte vám na váš telefón, na vaše telefónne číslo príde SMS-ka s kódom, ktorý ako overovací kód musíte ešte raz zadať do internetu. To znamená, že ešte sa overuje, či ste platbu naozaj realizovali vy, a to telefónne číslo, ktoré ste banke uviedli ako telefónne číslo, ktoré patrí majiteľovi platobnej karty."

Viera Horáková:

"Čiže akási dvojitá ochrana."

Roman Fusek:

"Presne tak. Pri tomto spôsobe zabezpečenia, ktorý je ešte aj elektronicky zabezpečený vyššou formou ako predchádzajúce, ale o tom sa veľmi baviť nemusíme, pre laikov to nie je dôležité. Dôležité je, že ak sa nachádzate na platbe cez 3D Secure, tak s najväčšou pravdepodobnosťou sa vám nestane vôbec nič a bezpečne zrealizujete svoju platbu."

Viera Horáková:

"No a keď hovoríme o tej bezpečnosti, tak sú nejaké také varovania, že nie som správne, ja neviem, nie je to po slovensky alebo nejaká diakritika."

Roman Fusek:

"Také tie základné pravidlá vo vzťahu k tomu, čo hovoríte, že sa nachádzate na internetovej stránke s čudnou diakritikou, tak s tým sa môžete stretnúť predovšetkým v prípade, ak vás niekto chce presmerovať na internetovú stránku nejakého zlodeja v prípade, ak pristupujete do internet bankingu. Čiže to nie sú ani prípady práve tohto internetového predaja, ale prístupu do internet bankingu. Zas sa dostanem k cudzím slovám, k anglickým výrazom, ktoré znamenajú rôzne formy útokov. Rozoznávame také tri pomerne populárne formy útokov pharming, vishing a phishing..."

Viera Horáková:

"Čiže vlastne prešli sme na také spôsoby elektronického napadnutia."

Roman Fusek:

"Áno. Je to vlastne to, akým spôsobom sa môžete stať obeťou nejakého útoku. Keď sa vrátim znovu k platbe cez internet banking, tak v prípade pharmingu je veľmi dôležité, takto, čo je pharming. Pharming je prípad, keď práce chcete pristúpiť na svoju internetovú stránku, cez ktorú realizujete internet banking, čiže na internetovú stránku banky, ale niekto vás automaticky bez toho, aby ste o tom vedeli, presmeruje na svoju internetovú stránku. Je to spravidla tento zlodej, ktorý vám chce ukradnúť autorizačné kódy..."

Viera Horáková:

"Ako na to prídem, že ma chce presmerovať?"

Roman Fusek:

"Na to sa prichádza pomerne ťažko, chrániť sa pred takýmto automatickým presmerovaním je možné buď takýmito tými programami, ktoré sú súčasťou antivírových balíkov, ale pre laika môže byť varovným signálom práve to, že sa na takúto webovú stránku dostane buď z mailu, ktorý mu príde, že mu príde emailová nejaká adresa, z nejakej zvláštnej emailovej adresy mu príde email a je tam informácia, že máte kliknúť na nejaký link, teda na nejakú adresu a ono vás to presmeruje na túto adresu, resp. vám to nahrá do počítača nejakého Trójskeho koňa."

Viera Horáková:

"Čiže neklikať."

Roman Fusek:

"Áno. Zo zvláštnych emailových adries neklikať, radšej vymazať takýto email. Navyše, ak ide o email, ktorý vám signalizuje, že vaša banka od vás niečo chce, je to so zvláštnu diakritikou, prišlo to zo zvláštnej adresy nie zo slovenskej emailovej adresy, prípadne z emailovej adresy, z ktorej s vami komunikuje táto vaša banka..."

Viera Horáková:

"A ešte sa chcem opýtať, môže banka odo mňa niečo chcieť, vlastne mám reagovať, aj keby to prišlo zo slovenskej adresy?"

Roman Fusek:

"Banka od vás nikdy nebude chcieť práve tie identifikačné údaje. Čiže autorizačné údaje, s ktorými sa pripájate, banka od vás nebude chcieť ani cez internet, pokiaľ vám pošle nejaké emailovú správu, nebude to chcieť ani cez telefón, čo je vishing, to znamená, že by vám niekto zavolal a pýtal si od vás číslo vašej platobnej karty alebo nejaké údaje z platobnej karty alebo vaše autorizačné údaje do internet bankingu, toto banka nikdy nespraví. A takisto banka nijakým spôsobom cez tú nezabezpečenú komunikáciu mimo svojho internet bankingu od vás nebude chcieť údaje v emailovej komunikácii. Čiže tá najjednoduchšia obrana je, ak máte niečo podozrivé, neklikať. Ak sa vám zdá, že sa nachádzate na inej webovej stránke ako na webovej stránke svojej banky, že vás to presmerovalo na niečo, na čo nie ste zvyknutí, prípadne si všímate, že nie je úplne ideálna slovenčina na tej webovej stránke, tak radšej odtiaľ zmiznúť a nezadávať tam údaje. Ale je pravda, že dnes už títo internetoví zlodeji sú veľmi prešpekulovaní a tie obrázky internet bankingu na falošných stránkach sú pomerne autentické."

Viera Horáková:

"Takže povedali ste, že relácia bude aj plná takých cudzích slov, takže sme si objasnili tie najbežnejšie spôsoby elektronického napadnutia, a to pharming, vishing a phishing."

Viera Horáková:

"Elektronické platby a bezpečnosť elektronického bankovníctva, to je téma, o ktorej sa zhovárame s riaditeľom odboru ochrany finančných spotrebiteľov Národnej banky Slovenska Romanom Fusekom, ak máte nejakú otázku horakova@rtvs.sk.

Údaje z bankomatovej karty sa dajú zneužiť pri elektronických platbách. Možno si niekto povie, akým spôsobom vlastne mi niekto tie všetky údaje môže odčítať alebo na ne prísť."

Roman Fusek:

"No môže na ne prísť tým spôsobom, že v prípade, ak platíte svojou kartou, tak by ste ju nemali dať z ruky, resp. by ste ju nemali spustiť z očí. Dnes sa tá karta a tie čísla, ktoré máte na karte a všetky údaje, ktoré sú potrebné k elektronickej platbe, nachádzajú priamo na karte a ktokoľvek si ich opíše alebo zoskenuje, tak vám ich vie vzápätí zneužiť. Preto som rozprával o 3D Secure, čo je vyššia forma zabezpečenia, a preto sa overuje potom tá platba ešte SMS-kou. Ale v prípade, ak ste napríklad na nezabezpečenej stránke tak, ako sme sa bavili o tom, že máte mať visiaci zámok a https v riadku, kde je adresa, tak v takom prípade vám dokáže nejaký hacker, teda ten, ktorý kradne údaje z internetu, tie údaje odčítať, zobrať a môže sa tváriť naďalej ako majiteľ karty. V prípade 3D Secure je malá pravdepodobnosť, že vám ten účet vybieli. Čiže je to vyššia forma zabezpečenia. To, čo je oveľa nebezpečnejšie ako ukradnutie karty, pretože tam vám môže urobiť niekoľko transakcií a spravidla to zistíte a zablokujete, oveľa nebezpečnejšie je, keď sa stanete obeťou nejakého pharmingu alebo phisingu. To znamená, že niekto sa dostane k vašim údajom priamo z internet bankingu, dokáže vám v prípade, ak sa dostane k údajom z internet bankingu prakticky jednou transakciou vybieliť celý účet."

Viera Horáková:

"Natíska sa teda otázka, ako predchádzať napadnutiu, ako sa bezpečne správať."

Roman Fusek:

"Niektoré zásady sme si už povedali priebežne, určite platí nepristupovať z nezabezpečenej WiFi siete do svojho internet bankingu, ďalej platí to, aby ste svoj počítač mali zabezpečený proti vírusom. Ďalej v prípade, ak vám zatelefonuje v úvodzovkách pracovník banky, tak žiadne údaje pracovníkovi banky zo svojej karty alebo z internet bankingu neprezrádzajte. Ak sa nachádzate na nejakej internetovej stránke, ktorá má zvláštnu diakritiku, nepokračovať ďalej, hoci sa tvári ako váš internet banking. Pokiaľ sťahujete nejaké aplikácie, dnes sú veľmi populárne mobilné aplikácie na mobilný telefón, na tablet, nesťahujte tie aplikácie z nejakých zvláštnych stránok, je lepšie použiť také tie overené Google Play alebo App Store kvôli tomu, že tam už dochádza ku kontrole toho, čo sa tam nachádza. To znamená, že tam by nemal byť nahratý žiadny Trójsky kôň, ktorý vám narobí v počítači alebo teda v telefóne šarapatu. Potom dôležité je si kontrolovať vždy pri elektronickej platbe https visiaci zámok, to sme si hovorili takisto. No a keby ste boli zbehlejší v počítačových technológiách, tak by ste si mohli skontrolovať v prípade, ak by sám to nezdalo, či sa nachádzate naozaj na webovej stránke banky cez vlastne číslo tej webovej stránky, cez ktoré sa pristupuje. Server tej banky má tzv. SSH fingerprint, to sa už pre bežnú laickú verejnosť zbytočne rozpráva."

Viera Horáková:

"Pán riaditeľ, skôr ako budeme hovoriť o tom, čo robiť v prípade, že sa staneme obeťou napadnutia, tak vyzývame poslucháčov, aby písali. Píše verný poslucháč Gejza z Dražoviec, mimochodom, veľmi rád počúva túto reláciu a ďakuje vám za prínosné informácie a píše: Počul som, že v rámci zavádzania týchto zmien by sme mali uvádzať okrem IBAN-u aj žiadosť urgentných platieb a nákladov a on sa pýta, čo znamenajú tie skratky ZUPAN a kde nájde nejaké konkrétne udanie k tomu ZUPAN-u."

Roman Fusek:

"V prípade, ak sa nachádzate v rámci SEPA, teda v systéme jednotných platieb a chcete zrealizovať platbu cez vlastne zadaním tohto IBAN-u do ktorejkoľvek banky v rámci Európskej únie, prípadne v krajinách EÚ, tak za rovnakých podmienok ako realizujete platby na Slovensku, musíte byť schopní zrealizovať aj platby do zahraničia. To znamená, že tá platba by mala zbehnúť za dva dni, bežná platba takú, akú máte na Slovensku, vám garantuje SEPA systém, že zbehne v rámci celej Európy za dva dni a za tú istú cenu. A banky majú prednastavené práve tie prípady zdieľania nákladov na tú platobnú transakciu, prednastavené spravidla tak, aby tá platobná transakcia stála rovnako, ako domáca platobná transakcia. Čiže by ste nemali platiť viac. V prípade, ak by ste chceli riešiť nejaké zrýchlené platby, tak tam je lepšie si kontaktovať banku, pretože v prípade zrýchlených platieb alebo iného rozdelenia nákladov na platby, bývajú tie platby pomerne drahé."

Viera Horáková:

"No a teraz sa vráťme k tej otázke, stala som sa obeťou napadnutia, čo mám robiť ako prvé?"

Roman Fusek:

"Ako prvé zablokovať účet. To je úplne prvá dôležitá vec. Hneď ako zistíte, že sa vám niečo podozrivé deje na účte, tak svoj účet je najlepšie okamžite zablokovať, najlepšie na klientskej telefonickej linke banky alebo na najbližšej pobočke banky, a potom riešiť následne už ďalšie prípadné škody, ktoré vám vznikli. Platí zásada, že od okamihu blokácie vášho účtu za akúkoľvek transakciu, ktorá je zrealizovaná po blokácii vášho účtu, nesie zodpovednosť banka. To znamená, že za straty, ktoré sú realizované po blokácii už nesie zodpovednosť banka. Za straty, ktoré sú pred blokáciou a neboli riadne autentifikované, teda neboli riadne autorizované vaše platby, tak tam sú pravidlá na to, kto za čo zodpovedá a v akej výške."

Viera Horáková:

"Môžem dvojakým spôsobom zistiť, že niečo sa deje, po prvé, že idem do bankomatu a vidím nejaké pohyby na účte, ale možno nikto nevyberá peniaze z bankomatu každý deň a príde na to, až keď mu príde výpis."

Roman Fusek:

"Dnes má veľa ľudí nastavenú SMS notifikáciu. Čiže keď pracujete pomerne veľa cez internet, robíte elektronických platieb viac, tak je lepšie si nastaviť SMS notifikáciu..."

Viera Horáková:

"Čiže odchádzajúce peniaze."

Roman Fusek:

"Presne tak. Banka vám bude signalizovať každé odchádzajúce peniaze, akékoľvek podozrivé transakcie tak dokážete zachytiť veľmi rýchlo. V prípade, ak ju nemáte zapnutú, tak v takom prípade naozaj sa môže stať, že v krajnej situácii sa dozviete až z výpisu z účtu, že vám nejaké transakcie odišli. No a začne banka skúmať, či tie vami namietané platby, ktoré ste nezrealizovali, boli riadne autorizované alebo nie a začnete sa teraz s bankou dohadovať o to, kto za čo zodpovedá. Či ste porušili nejaké pravidlá elektronických platieb a práce so svojou platobnou kartou alebo nie."

Viera Horáková:

"To znamená, že prvý krok je zablokovať, mimochodom, môže niekto aj vybieliť jedným šmahom ako sa hovorí, náš účet?"

Roman Fusek:

"Áno, je to teoreticky možné. Ak sa dostane k vašim všetkým údajom internetového bankovníctva a nemáte cez internet banking zabezpečené to, že máte len nejaký objem transakcií, ktoré môžete realizovať behom jedného dňa, tak naozaj je možné vybieliť aj celý účet prakticky okamžite. Existuje veľa zabezpečovacích prostriedkov, ktorými sa banky snažia práve svoj internet banking chrániť, povedzme práve tie SMS autorizácie, ktoré sa robia už aj v prípade internet bankingu, nielen v prípade elektronickej platby a podobne. Ale dnes sú hackeri veľmi šikovní a dokážu presmerovať už aj váš mobilný telefón na svoje číslo, resp. zmeniť telefónne číslo priamo v internet bankingu, na ktoré sa potom tie autorizácie posielajú a prakticky vám tak veľmi rýchlo vybieliť celý účet."

Viera Horáková:

"Ako a koľko sa na týchto stratách môžeme podieľať my?"

Roman Fusek:

"No, podľa toho, ako ste sa správali. My sme sa skoro hodinu rozprávali o tom, ako by ste sa mali bezpečne správať a aké pravidlá by ste mali dodržať. Ak ich dodržiavate alebo dodržiavate naozaj väčšinu z nich..."

Viera Horáková:

"Čo banka zistí."

Roman Fusek:

"Čo banka veľmi ľahko a rýchlo zistí práve dodatočným šetrením jednotlivých platieb, a to, kde tie údaje s najväčšou pravdepodobnosťou odišli, pretože ona dokáže došetriť spätne prakticky všetky platby a dokáže zistiť, odkiaľ vám s najväčšou pravdepodobnosťou ten hacker ukradol dáta. V prípade, ak ste teda ale dodržiavali tieto pravidlá, nie vždycky sa aj dodržiavaním týchto pravidiel dá úplne ideálne chrániť, tak v takom prípade sa podieľate na stratách na svojom účte len do výšky 100 eur. V prípade ale ak ste postupovali hrubo nedbanlivo, to znamená, že ste sa správali obzvlášť ľahkovážne alebo ľahkomyseľne vo vzťahu či už vo vzťahu k svojej platobnej karte alebo vo vzťahu k svojmu internetovému bankovníctvu, tak môže sa stať, že banka vám povie, že znášate si stratu v celej výške."

Viera Horáková:

"Ešte som sa chcela opýtať, že sú nejaké situácie, že nám banka naozaj môže zatelefonovať a niečo od nás telefonicky požadovať?"

Roman Fusek:

"Samozrejme, že áno, ale banka v takom prípade nebude od vás pýtať číslo vašej platobnej karty. Nebude od vás pýtať heslo do internet bankingu, to v žiadnom prípade od vás elektronicky pýtať nebude. Ak by od vás nejaký operátor banky, ktorý sa predstaví teda ako telefonický operátor banky niečo také pýtal, tak mu určite takéto veci neodpovedajte."

Viera Horáková:

"A v akých prípadoch odo mňa niečo môžu chcieť, len ma informujú a nič nežiadajú?"

Roman Fusek:

"Áno, buď vás informujú alebo robia nejaký prieskum, prípadne vás na niečo upozorňujú, ale nikdy si nepýtajú práve tie autorizačné údaje. Možno ešte jedna dôležitá informácia, pokiaľ chcete zistiť, aké útoky sa v tejto dobe odohrávajú a môžu sa odohrávať alebo sa odohrali v nejakom

minulom čase, tak je to dobré si kontrolovať v rámci internet bankingu aj notifikáciu alebo správy banky. Mnoho ľudí ich ignoruje, pretože sa im zdajú obťažujúce, ale banky v týchto notifikáciách informujú práve aj o takýchto útokoch a o podozrivých internetových stránkach, o podozrivých emailoch. Takéto informácie má banka zavesené aj na svoje webovej stránke, takže pokiaľ si chcete overiť, že či náhodou niečomu podozrivému nečelíte, tak si nalogovať buď svoj internet banking alebo si nalogovať webovú stránku banky a tam zistíte, že či sa aktuálne neodohrávaj nejaké útoky na klientov banky. Banka spravidla klientov upozorňuje vopred."

Viera Horáková:

"Milí poslucháči, takže v dnešnej relácii odznelo množstvo dôležitých informácií týkajúcich sa bezpečnosti elektronického bankovníctva, spolu s riaditeľom odboru ochrany finančných spotrebiteľov Národnej banky Slovenska Romanom Fusekom dúfame, že ich prijmete len ako informáciu a nikdy ich nebudete musieť využi, pretože práve vy ste sa stali obeťou napadnutia. Ďakujem pekne za návštevu."