Úvod

Pro zvýšení kvality poskytovaných služeb poskytuje společnost SAB Finance svým klientům následující doporučení, jak se vyhnout bezpečnostním rizikům spojených s platebními službami. Bezpečnostní rizika na síti a při používání prostředků ICT jsou stále významnějším tématem. Prostředky ICT, jako osobní počítač nebo mobilní telefon či tablet jsou používány při komunikaci s naší společností, tudíž Vám chceme představit, jak se při obchodování se SAB Finance můžete vyvarovat vzniku nepřiměřených rizik, plynoucích z kybernetické bezpečnosti.

Hlavními prostředky, které lze zneužít při komunikaci se společností SAB Finance jsou:

- e-mail,
- telefonní přístroj,
- podpisový vzor,
- bankovní účet a internetové bankovnictví.

Všechny tyto prostředky je možné vhodně zabezpečit, aby bylo jejich zneužití pro případného útočníka výrazně ztíženo nebo ještě lépe znemožněno.

Zabezpečení e-mailové schránky

Hlavním prostředkem zabezpečení e-mailové schránky je použití silného hesla. Pro názornost uvádíme, kolik kombinací je možné získat použitím různých variant hesla. Budeme-li zvažovat jako nejmenší variantu 8 znaků dlouhé heslo, dostáváme se k těmto hodnotám počtu kombinací:

Skladba znaků	Počet znaků	Délka hesla	Počet kombinací
Čísla	10	8	100 000 000
Čísla + malá písmena	36	8	2 821 109 907 456
Čísla + mála + velká písmena	64	8	281 474 976 710 656
využití všech znaků na klávesnici	82	8	2 044 140 858 654 980

Užití hesla s kombinací malých a velkých písmen, diakritiky, číslic a příp. speciálních znaků je vhodnou ochranou před tzv. brute-force útokem (automatické vkládání různých variant hesla pomocí automatu).

I když se užije kombinované heslo, tak je nutné se vyvarovat užití notoricky známých kombinací (např. uvedeny níže). Potenciální útočníci vědí, jaká hesla lidé často používají, a proto je při použití tzv. slovníkového útoku zkouší přednostně. Problematice nejexponovanějších hesel se věnuje dlouhodobě např. server SplashData, který pro rok 2017 vydal tato hesla jako nejhorší pro zabezpečení:

123456	letmein	monkey
Password	1234567	login
12345678	football	abc123
qwerty	iloveyou	starwars
12345	admin	123123
123456789	welcome	dragon
passw0rd	freedom	trustno1
maste	whatever	
hello	qazwsx	

Ze seznamu je vidět, že i prodloužení velmi nebezpečného hesla 123456 na 123456789 ho posunulo na žebříčku o něco málo níže.

Servery dnes v podstatě bez problémů umožňují i velmi dlouhá hesla, takže je možné se zamyslet i nad tím, že místo Le_1>!,@, které by se dalo považovat za velmi silné (a taky těžko zapamatovatelné), můžeme použít *„kocka leze dirou, pes oknem“*. Pro porovnání ještě jednou tabulka ze začátku článku. Síla hesla je nesrovnatelná i při použití pouze malých písmen.

Skladba znaků	Počet znaků	Délka hesla	Počet kombinací
Čísla	10	8	100 000 000
Čísla + malá písmena	36	8	2 821 109 907 456
Čísla + mála + velká písmena	64	8	281 474 976 710 656
využití všech znaků na klávesnici	82	8	2 044 140 858 654 980
kocka leze dirou pes oknem	26	26	6 156 119 580 207 160 000 000 000 000 000 000 000

Heslo musí být pravidelně měněno, doporučená doba platnosti hesla je cca 2–3 měsíce.

Autentizační kódy

Pro komunikaci nejen s naší společností jsou nutné i autentizační kódy. Jejich význam stále roste. Autentizační kód je jedinečný pro konkrétní osobu a jeho vyzrazení zásadním narušením autentizačního prvku.

Mobilní telefon

Významným bezpečnostním prvkem je i telefon. Mobilní telefon obvykle obsahuje mj. informace, o e-mailu a dalších datech, která by měla případnému útočníkovi zůstat skryta. Zabezpečení lze na dnešních telefonech realizovat např. heslem, otiskem prstu nebo skenem obličeje. Všechny zabezpečovací prvky ztěžují případné zneužití telefonu nebo alespoň zdrží útočníka do té doby, než ztrátu telefonu zjistíme a zablokujeme přístupy, které by bylo možné přes telefonu zneužít.

Pro bezpečné používání telefonu je také nutné instalovat a používat jen takové aplikace, které jsou prověřené, a není v nich kód, který by zjišťoval data a posílal je tvůrci aplikace. Doporučuje se instalovat aplikace jen z prověřených obchodů.

Podpis

Podpisový vzor je na první pohled velmi těžko zneužitelnou záležitostí. Ovšem jen do okamžiku, kdy přijdete o peněženku nebo jiné zavazadlo, které bude obsahovat Váš občanský průkaz, řidičský průkaz nebo jiný doklad, na němž je Váš podpis.

Jako podpisový vzor proto můžete použít i jiný podpis, než jaký běžně používáte nebo je možné na občanský průkaz a další doklady použít takový podpis, který v soukromém životě nepoužíváte. Podpisové vzory lze, samozřejmě, i průběžně měnit jako hesla a tím zamezit jeho zneužití.

Bankovní účet

Všechny výše vyjmenované postupy lze použít i pro ochranu bankovního účtu. Pokud to Vaše banka umožňuje, je vhodné použít jedinečné přihlašovací jméno. Zároveň je vhodné použít silné heslo, při jeho sestavování je možné vycházet z postupu uvedeného výše.

Obecná doporučení pro používání PC

Hlavními zásadami pro udržení bezpečného počítače je pravidelně aktualizovaný antivirový program a operační systém, instalace jen takových aplikací, které jsou od prověřeného vydavatele a navštěvování bezpečných webových stránek.

Zabezpečené stránky

Bezpečnou stránku lze rozeznat pomocí přítomnosti ikonky zámku v adresním řádku. Na našich stránkách vypadá takto:

Dalším vodítkem je i adresa, začínající *https://*, některé prohlížeče celou adresu nezobrazují a zobrazují místo ní právě zelenou ikonku zámku.

Podvržení e-mailu

Aktuálním trendem je používání podvržených mailů, pro uskutečnění podvodné platby. Scénář je obvykle následující: Osobě, která je oprávněna k obsluze bankovního účtu, je poslán e-mail, který se tváří jako odeslaný vedoucím nebo ředitelem firmy. Ten žádá, aby osoba poslala prostředky z jisté faktury jinam, než je obvyklé (např. kvůli auditu nebo problémům s bankovním spojením). Adresát mailu, pokud neověří, že takový mail opravdu poslala jeho protistrana, odesílá peníze, na základě podvržené faktury jinam, a podvodníci se velmi snadno dostanou k penězům, které neprodleně vybírají z účtu nebo dále převádějí pro znemožnění jejich vystopování a vrácení platby.

V případě, že máte pochyby o tom, zda je požadavek Vaší protistrany oprávněný, doporučuje se důsledná verifikace platebních údajů.

Pokud již byly prostředky odeslány, je nutné co nejrychleji kontaktovat naše pracovníky.

SAB Finance a.s.
Senovážné nám. 1375/19, 110 00 Praha 1
Provozovna: Kvítková 4352, 760 01 Zlín