Obecná pravidla bezpečnosti

- ✓ Udržujte v tajnosti své heslo k bankovním aplikacím, nikam si jej nepoznamenávejte a pravidelně si jej měňte. Nepoužívejte slabá hesla, která lze snadno rozluštit a zneužít.
- ✓ Nesdělujte svá hesla nikomu, a to ani rodinným příslušníkům nebo Sparkasse. Speciálně je třeba upozornit na podvodné žádosti formou e-mailu a ve jménu bankovní instituce s žádostí o předání / zadání hesla. Tyto údaje Sparkasse nikdy od klientů nepožaduje. Emailovou formou nikdy nepožaduje také jiné údaje (osobní, k platebním kartám apod.). Zároveň Sparkasse nikdy nezasílá nevyžádané e-maily s odkazy na internetové adresy. V případě, že obdržíte nevyžádaný e-mail obsahující internetový odkaz na stránky Sparkasse, na e-mail nereagujte a na odkaz neklikejte.
- ✓ Navštěvujte na internetu pouze známé a důvěryhodné stránky.
- ✓ Nestahujte a nespouštějte soubory/aplikace s neznámým obsahem, které mohou společně se svým proklamovaným účelem vykonávat i nebezpečnou činnost (trojští koně, spyware apod.).
- ✓ Otevírejte pouze důvěryhodné e-maily od známých a očekávatelných odesílatelů. Neotvírejte neznámé nebo podezřelé přílohy (obsahující zkomolená slova, neobvyklé slovní obraty, pravopisné chyby apod.) ve Vaší emailové schránce. Na tyto zprávy nereagujte a bez otevření je smažte – může se jednat o tzv. phishing.
- ✓ Chraňte svůj počítač a mobilní zařízení, tj. používejte legální a aktualizovaný operační systém a ostatní software, aktuální antivirový program, antispyware a personální firewall.
- ✓ Neumožňujte práci s Vaším počítačem / mobilním telefonem neznámé osobě. Používejte pro práci v aplikaci internetového bankovnictví pouze svůj, popř. firemní, PC. Ideálně nepoužívejte službu na počítačích, nad kterými nemáte kontrolu (viz internetové kavárny a nebezpečí na pozadí běžících procesů a programů).
- ✓ Zabezpečte svůj počítač, pokud s ním právě nepracujete. V případě krátkodobé nepřítomnosti jej uzamkněte, v případě dlouhodobé nepřítomnosti počítač vypněte.
- ✓ S počítačem pracujte pod účtem neprivilegovaného uživatele (user). Práce s vyššími oprávněními (např. administrátor), umožňující instalaci programového vybavení, je bezpečnostním rizikem. Neprovádějte programové úpravy mobilního telefonu nebo jiného mobilního zařízení, které umožňují plný administrátorský přístup (root, jailbreak)
- ✓ Chraňte svůj mobilní telefon používaný pro přihlášení k bankovním aplikacím nebo k autorizaci pokynů z těchto aplikací. Zabezpečte svůj mobilní telefon heslem. Do mobilních telefonů instalujte pouze prověřené aplikace. Mělo by jít výhradně o oficiální aplikace pro iOS, Android a Windows Phone dostupné na oficiálních aplikačních marketech. Také mobilní telefony by měly mít nainstalovanou antivirovou ochranu, jestliže je pro daný typ zařízení k dispozici, případně možnost vymazání jeho obsahu na dálku v případě ztráty nebo krádeže
- ✓ Nepoužívejte pro přístup k internetu neověřené veřejné bezdrátové sítě, např. na letištích nebo v restauracích
- ✓ Nastavte si zasílání notifikačních zpráv, tj. SMS (zpoplatněná dle sazebníku WSPK), e-mail (bez poplatku) nebo notifikace pro Smartbanking (bez poplatku), které Vás budou informovat o veškerých platbách provedených z Vašeho účtu. Nastavení provedete snadno v internetovém bankovnictví.
- ✓ Přihlašujte se do služby „s INTERNETBANKING“ standardním způsobem, ideálně ručním zadáním adresy eb.wspk.cz přímo do adresního řádku internetového prohlížeče. Zkontrolujte si také důvěryhodnost certifikátu.

- ✓ V případě jakýchkoli pochybností nebo dotazů kontaktujte naši technickou podporu na tel. čísle +420 384 344 123 nebo emailem na adrese eb@wspk.cz.

Slovníček pojmů

Phishing
Phishing jsou podvodné e-mailové zprávy, které mají vzbudit dojem, že byly odeslány z legitimní e-mailové adresy, např. SPARKASSE. Cílem podvodného emailu může být získání klientských údajů (identifikační a autentizační údaje, bezpečnostní kódy nebo například PIN k platební kartě) a jejich následné zneužití. Phishingová zpráva může typicky vypadat jako výzva k aktualizaci bezpečnostních údajů. SPARKASSE zásadně takové zprávy nerozesílá a o bezpečnostních údajích s klientem zásadně nekomunikuje prostřednictvím e-mailu.

Spyware
Spyware je program, který využívá internetové stránky k odesílání dat z počítače či mobilního telefonu nebo jiného zařízení bez vědomí jeho uživatele. Spyware se často šíří jako součást volně šiřitelných programů, většinou bez vědomí uživatelů (ale s vědomím autorů programu)

Trojský kůň
Trojský kůň je uživateli skrytá část programu nebo aplikace s funkcí, se kterou uživatel nesouhlasí (typicky je to činnost škodlivá). Trojský kůň může být samostatný program, který se tváří užitečně – například hra, spořič obrazovky nebo nějaký jednoduchý nástroj. Někdy se trojský kůň vydává za program k odstraňování jiných programů nebo nastavení. Tato funkčnost slouží ale pouze jako maskování záškodnické činnosti, kterou v sobě trojský kůň ukrývá.

Root
Systémový uživatelský účet, který má v operačním systému nejvyšší oprávnění, které je prakticky absolutní. Za standardních okolností nelze činnost root účtu omezit, což lze považovat za vadu bezpečnostního návrhu systému, protože správce může v systému provést jakoukoliv činnost a posléze o ní zničit všechny stopy a důkazy.

Jailbreak
Jailbreak je softwarová úprava mobilního telefonu iPhone. Po Jailbreaku lze do iPhonu instalovat neoficiální aplikace (nevydávané v App Store), které mají přístup do souborového systému a mohou být škodlivé. Pomocí Jailbreak dojde i k softwarovému odemknutí zahraničního iPhone pro použití s jakýmkoliv operátorem.