Pravidla bezpečného používání webového platebního prostředku ZFP Payments. Doporučení pro klienty.

1. Své bezpečnostní údaje znáte jen vy a nikdo jiný

Nikdy nesdělujte nikomu dalšímu své bezpečnostní údaje do webového platebního prostředku (dále jen „*internetového bankovnictví*“), zejména uživatelské číslo, login, heslo, PIN, autorizační kód ani je neposílejte e-mailem či prostřednictvím sociálních sítí. Především při přihlašování dbejte na své soukromí a kontrolujte, že další osoby nemohou zaregistrovat vaše přihlašovací údaje. Stejně tak nenechávejte váš počítač či mobilní telefon bez dozoru, používejte zámky klávesnic a přístupové kódy k zařízení. Vyvarujte se používání produktů tzv. internetového bankovnictví na veřejnosti (například v dopravních prostředcích) nebo v monitorovaných místnostech (například v dohledu bezpečnostních kamer).

2. Hlídejte si, odkud přistupujete do internetového bankovnictví

Nepoužívejte internetové bankovnictví na počítačích, u kterých si nemůžete být jisti, zda na něm nejsou nainstalovány škodlivé programy. Rozhodně se vyvarujte jakýmkoliv veřejným počítačům v internetových kavárnách nebo na letištích a v infocentrech. Pokud to jde, používejte pro přístup do svého internetového bankovnictví jen svůj osobní počítač či telefon. Vždy si v hlavičce prohlížeče zkontrolujte, zda do internetového bankovnictví přistupujete zabezpečeným připojením. Poznáte to jednoduše, stránka začíná https:// (důležité je „**s**“ na konci), případně vás na to upozorní samotný prohlížeč zelenou barvou nebo symbolem zamčeného zámku před názvem webu.

3. Pozor na neznámé odkazy a webové stránky

Navštěvujte na internetu pouze známé a důvěryhodné stránky. Dnešní útočníci jsou vynalézaví a dokážou velmi věrně reprodukovat například přihlašovací stránku do internetového bankovnictví a chytře vás na ni navést. Proto pozor na jakékoliv neznámé odkazy na internetu a v e-mailu, které by vás dovedly na stránky připomínající přihlašovací formulář do internetového bankovnictví, e-mailu nebo například sociálních sítí. Pokud se vám jeví přihlašovací obrazovka k produktům internetového bankovnictví jakkoli podezřelá, nepřihlašujte se. Vždy si v hlavičce prohlížeče pro jistotu zkontrolujte, zda se skutečně nacházíte na dané webové stránce, a ne na té falešné.

Obzvlášť nebezpečné mohou být stránky s erotickým obsahem nebo stránky ke stahování softwaru, videí a hudby, které často obsahují množství nebezpečného softwaru a virů.

4. Podezřelý e-mail? Neotevírat a raději smazat.

Společnost vám nikdy nepošle e-maily s výzvou ke sdělení identifikačních údajů, uživatelského čísla, loginu, hesla, PIN, autorizačního kódu, údajů k platební kartě apod. Na takovéto výzvy nikdy nereagujte. Ve své emailové schránce otevírejte pouze důvěryhodné emaily od známých a očekávatelných odesílatelů. Pokud se jeví email jakkoliv podezřele, raději jej rovnou smažte. Pokud jste jej již otevřeli, určitě neotevírejte přílohy a odkazy, které obsahuje. A pokud se vám nechtěně podaří kliknout na odkaz nebo otevřít přílohu, rychle ji zavřete a nenechávejte program ani prohlížeč nic instalovat. Následně doporučuje prověřit počítač či mobilní zřízení antivirovým softwarem.

5. Chraňte se proti spamu

Nejlepším nástrojem, jak většinu nechtěné a nebezpečné pošty eliminovat, je nastavit a aktivně používat emailovou ochranu proti spamu. Většina veřejných služeb ji nabízí, stejně tak mnoho emailových klientů jako Outlook a další. Její nastavení je často intuitivní a jednoduché. Zvažte použití také dalších bezpečnostních programů jako antispyware a antiadware, které vás ochrání před nechtěnými reklamami a nebezpečnými programy.

6. Používejte a aktualizujte antivirový program i firewall jak v počítači, tak telefonu

Provádějte pravidelně kontrolu svých zařízení prostřednictvím antivirového programu. Antivirový program nikdy nevypínejte, nezapomínejte pravidelně aktualizovat (dá se nastavit automatická aktualizace prostřednictvím internetu) a používejte jeho nejnovější verzi, která má implementovanou ochranu i detektory škodlivého softwaru. Podvodníci nespí, proto čím starší antivirový program, tím méně účinný je proti novým hrozbám. Zároveň doporučujeme na počítači používat firewall. Vybavte antivirem i svůj chytrý mobilní telefon. Že telefony viry nenapadají je nebezpečný mýtus, který se vám může lehce vymstít. Pokud máte podezření, že váš počítač nebo mobilní telefon napadl virus, nepoužívejte jej pro přístup do internetového bankovnictví ani k jiným službám s vašimi osobními údaji (e-mail, sociální sítě, internetové obchody atd.) a kontaktujte IT odborníka.

7. Aktualizujte svá zařízení, počítač i mobilní telefon

Pravidelně také aktualizujte své programy i operační systém. Obzvláště důležité je aktualizovat internetový prohlížeč v počítači i telefonu a všechny jeho takzvané zásuvné moduly (například přehrávač Flash). Aktualizujte také všechny své bezpečnostní programy. Hlídejte si také vydávání oprav operačního systému a neodkládejte jejich instalaci „na příště“. Pro chytré telefony a tablety doporučujeme používat nejnovější verzi operačního systému (tzv. firmware), který výrobce pro zařízení oficiálně nabízí. Všechny staré verze vašich programů jsou potenciální hrozbou pro bezpečné surfování i pro vaše finanční prostředky. Nikdy neinstalujte do svého počítače a telefonu programy, jejichž původ neznáte. Na mobilní telefony instalujte pouze aplikace z oficiálních obchodů s aplikacemi – Google Play (Android), App Store (iOS), Windows Marketplace (Windows Phone).

8. Mějte přehled o svém zůstatku a transakcích, nesrovnalosti ihned hlaste společnosti

Vědět, kolik peněz vám zbývá na účtu a jaké transakce jste provedli, je nejlepší nástroj včasného varování, že je cokoliv v nepořádku. Pokud zaregistrujete jakoukoliv operaci, kterou jste neprovedli, či máte pochybnost o správnosti zůstatku na vašem účtu, okamžitě kontaktujte společnost telefonicky nebo e-mailem. Neodkládejte prosím nahlášení! Jen rychlou reakcí lze zabránit případným dalším škodám či nalézt rychlé řešení případné chyby.

9. Pravidelně sledujte novinky o bezpečnosti na internetu

Čím více informací máte, tím bezpečněji se dokážete na internetu chovat. Pravidelně proto sledujte nejnovější zprávy z oblasti bezpečnosti na internetu a dodržujte všechna doporučená pravidla.