# Finanční služby na Internetu

Vyplnit složenku (dvakrát, protože napoprvé jste se přepsali), dojít na poštu, vystát frontu, přežít srážku s poštovní úřednicí, předat hotovost, vzít si ústřižek jako jediný doklad o zaplacení (a stresovat se, abyste ho neztratili), odejít… To není popis nějaké bizarní formy sebetrýzně, ale vzpomínka na běžné vyřízení bankovního převodu z doby ještě před nějakými 15 lety. Ještě že už dnes máme ten Internet.

## Osobní finance online

Internet totiž oblast správy osobních financí značně zjednodušil, především v podobě nástroje označovaného jako online bankovnictví. V České republice jej poprvé nabídla v roce 1998 česká Expandia Banka. Vzhledem k tehdejším technickým možnostem služba ovšem nabízela jen základní funkce (převody, historie apod.) a nabídka platila pouze pro ty, kdo byli ochotni si zřídit elektronický podpis.

V průběhu let se začaly přidávat další banky včetně tzv. kamenných či tradičních (lídři bankovního trhu jako Česká spořitelna, ČSOB či Komerční banka) a dnes patří internetové bankovnictví do povinné výbavy každého bankovního domu a představuje nejrozšířenější typ tzv. přímého bankovnictví. Klienti si oblíbili nepřetržitou dostupnost, rychlost a jednoduchost bankovních operací, banky zase úspory provozních nákladů.

Jaké jsou nejčastěji používané funkce? Kromě zmíněných jednorázových platebních transakcí je to také zadávání trvalých příkazů, nebo možnost zdarma generovat vlastní výpisy účtu (za určité období, podle konkrétního účtu, který byl předmětem transakce, podle výše částky apod.). V závislosti na typu účtu pak online bankovnictví nabízí i pokročilejší funkce jako zahraniční platební styk, správu vydaných platebních karet (např. změna PIN, limitu výběru či platby na Internetu), správu více účtů, žádost o úvěr a jiné služby atd.

## Bezpečnost na prvním místě

Přes své nesporné výhody si ale internetové bankovnictví hledalo cestu k běžným uživatelům docela dlouho. Osobní finance jsou citlivá věc a lidé zprvu neměli k novince důvěru - spravování financí přes Internet pro ně představovalo nepřijatelné riziko. A bezpečnostní řešení, která dokázala tyto obavy rozptýlit, byla pro běžného uživatele příliš složitá (zmíněný elektronický podpis, speciální terminál, který bylo třeba vždy připojit k počítači atd.).

Postupně ale Internet a celkový rozvoj v oblasti komunikačních technologií nabídl taková opatření a nástroje, která přinesla přijatelnou úroveň zabezpečení a zároveň uživateli nekladla zbytečné překážky v jejich používání. Jednalo se zejména o oblast zabezpečení spojení mezi počítačem uživatele a serverem, na němž běží služba, a oblast přihlašování.

## Jistotu dá certifikát

Pro ověření zabezpečení spojení se serverem se dnes používají zejména tzv. certifikáty. Ty potvrzují identitu serveru a také obsahují informace o úrovni šifrování komunikace a dalších bezpečnostních

prvcích, které by měly chránit uživatele před „odposloucháváním".

U certifikátů rozlišujeme dvě úrovně. První, základní, garantuje uživateli ověření domény a šifrované spojení, ale neříká nic o pravém vlastníkovi domény. S takovým certifikátem se setkáte třeba na stránkách Facebook.com. Druhá, pokročilá úroveň, potvrzuje, že vlastník domény prošel přesnějším ověřovacím procesem. Díky tomu certifikát obsahuje jednoznačné identifikační informace o vlastníkovi. Takovým certifikátem jsou opatřeny například právě stránky pro přihlášení do internetového bankovnictví.

Většina internetových prohlížečů dnes obsahuje funkci, která uživateli v adresním řádku graficky znázorní jednotlivé úrovně zabezpečení spojení se serverem. Podrobnosti o tom, jak přesně, bývají uvedeny v nápovědě prohlížečů.

## Pozor na phishing

Díky této funkci lze odhalit i pokus o tzv. phishing. Jde o typ útoku, který se snaží uživatele vylákat na podvržené stránky, na nichž útočníci sbírají citlivé informace. Typický scénář je následující: uživateli přijde e-mail, který nese znaky oficiální komunikace banky, u níž má účet. E-mail upozorňuje na smyšlený problém, který lze vyřešit pouze přihlášením do internetového bankovnictví, na něž je v e-mailu uveden odkaz. Přes něj se uživatel dostane na stránky, které jakoby z oka vypadly těm, které provozuje banka. Uživatel vyplní své přihlašovací údaje a odešle je rovnou útočníkům.

Stránky jsou sice identické, že je ale něco v nepořádku by měla signalizovat právě varovná ikona v adresním řádku (ani samotná adresa neodpovídá oficiální doméně bankovní služby). Za normálních okolností by totiž měla indikovat šifrované a ověřené spojení se serverem.

Kromě toho také platí, že banky zásadně e-mailem (ani telefonicky) nevyzývají své klienty k přihlášení do online bankovnictví a rozhodně po nich tímto způsobem nevyžadují přihlašovací údaje.

## Nová transakce, nové heslo

Pokud jde o samotné přihlašování a autentifikaci uživatele v internetovém bankovnictví, zde se nejširšího uplatnění dočkala metoda OTP (one-time password). Jde vlastně o speciální typ jednorázového hesla, které je platné pouze pro jediné spojení mezi počítačem a serverem, případně pro jedinou konkrétní transakci.

V praxi to vypadá tak, že uživatel se k internetovému bankovnictví přihlásí pomocí standardních přihlašovacích údajů, ale provedení jednotlivých transakcí (platební příkaz, změny ve správě účtu, zadání nového trvalého příkazu atd.) musí potvrdit ještě speciálním jednorázovým heslem, které mu provozovatel služby poskytne například formou SMS.