Dodržujte Zásady bezpečného užívání internetového bankovnictví

1. Používejte bezpečný počítač

Pro práci s internetovým bankovnictvím používejte pouze bezpečné a známé počítače doma nebo v práci, které máte plně pod kontrolou (tzn. můžete ovlivnit jejich bezpečnostní nastavení). V žádném případě nedoporučujeme používat neznámé počítače (např. v internetových kavárnách, na veřejných hotspotech apod.). Sledujte a instalujte včas opravy a aktualizace aplikací vydávané výrobci. U operačního systému MS Windows ponechte povolené automatické aktualizace.

2. Mějte svůj počítač zabezpečený

Používejte antivirové a antispyware programy. Pravidelně je aktualizujte, aby jejich účinnost byla co nejvyšší. Připojujte se k internetu přes firewall, který umožní minimalizovat rizika neoprávněného přístupu k vašemu počítači z venkovní sítě. Ponechte aktivován osobní firewall, který je standardní součástí operačního systému Windows XP SP3 a výše.

3. Chraňte přihlašovací údaje pro přístup do internetového bankovnictví

Přihlašovací údaje (jako přihlašovací jméno a heslo) si nikam nezaznamenávejte. Zcela nevhodný je zápis přihlašovacích údajů do mobilního telefonu, počítače, diáře nebo na papírky (v bezpečí rozhodně nejsou nalepené na monitoru nebo pod klávesnicí). V internetovém prohlížeči nikdy nepovolujte zapamatování hesla. A své přístupové údaje nikomu nesdělujte (ani rodinným příslušníkům) ani je prostřednictvím sociálních sítí nikomu nepředávejte.

4. Nepoužívejte jednoduchá hesla

Nepoužívejte jednoduchá a snadno odvoditelná hesla. Určitě nepoužívejte data narození, po sobě jdoucí číslice a písmena, části telefonních čísel apod. Heslo je vhodné jednou za 3 měsíce změnit.

5. Chraňte svůj mobilní telefon

Na váš mobilní telefon posíláme pro potvrzení různých operací SMS klíč. Chraňte proto svůj mobilní telefon, nenechávejte jej bez dozoru a nepůjčujte jiným osobám. Používáte-li tzv. „chytrý“ telefon (telefon s operačním systémem Android, Windows Phone, iOS apod.), neinstalujte do něj aplikace z neznámých zdrojů a pokud možno používejte antivirový program.

6. Při přihlašování na stránkách internetového bankovnictví buďte opatrní

V každé chvíli, kdy jste v internetovém bankovnictví nebo se do něj přihlašujete, musí být v adresním řádku vašeho internetového prohlížeče adresa našeho internetového bankovnictví (https://ib.artesa.cz/) a vedle ní ikona „zámku“. Po kliknutí na ni se zobrazí certifikát potvrzující platnost a ověřující identitu stránky. V moderních internetových prohlížečích se kontrola provádí automaticky (řádek s adresou stránky zezelená). Artesa pro zabezpečení těchto stránek využívá serverové certifikáty společnosti Thawte.

7. V případě problémů nebo pochybností nás kontaktujte

Máte-li kdykoliv jakékoliv pochybnosti o platnosti a pravosti certifikátu nebo stránek internetového bankovnictví, přerušte práci a kontaktujte náš Helpdesk telefonicky na čísle 800 128 836 nebo e-mailem na adrese info@artesa.cz.

8. Pozor na nedůvěryhodné e-maily

Neotvírejte e-mail od neznámého adresáta nebo s podezřelým či prázdným předmětem či obsahem. V žádném případě nespouštějte jeho přílohy a neklikejte na žádné odkazy. Takový e-mail rovnou smažte. Nikdy nereagujte na e-mail, který po vás požaduje sdělení vašich osobních údajů, hesla nebo přihlašovacího jména. Artesa od vás nikdy vaše údaje touto formou nebude požadovat.

9. Nestahujte z internetu neznámé soubory

Navštěvujte na internetu pouze známé a důvěryhodné stránky. Vyvarujte se stahování neznámých souborů z internetu (zejména s příponou EXE, BAT, COM apod.). Takové soubory mohou společně se svým původním účelem nainstalovat na váš počítač i nebezpečné programy.