Zásady bezpečného používání Internetového bankovnictví

1) Chraňte si své přihlašovací údaje pro přístup do internetového bankovnictví
a) Heslo - nikdy nesdělujte svoje bezpečnostní údaje dalším osobám (ani rodinným příslušníkům) a nevkládejte je do aplikací, pokud nemáte jistotu, že pracujete na stránkách www.anosd.cz. Nastavte si silné heslo (mělo by obsahovat velká i malá písmena, číslice i speciální znaky) a pravidelně ho měňte. Heslo do Internetového bankovnictví by mělo být odlišné od hesel do jiných aplikací. V Internetovém prohlížeči nikdy nepovolujte zapamatování hesla.
b) Autorizační SMS – každá autorizační SMS zpráva obsahuje nejen unikátní kód, jehož zadáním potvrdíte prováděnou transakci, ale také detailní informace k dané transakci. Před zadáním kódu proto dbejte na důslednou kontrolu uvedených údajů a potvrďte si tak, že se jedná o Vámi zadanou transakci.

2) 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 či v jiných veřejných místech).
Sledujte a instalujte včas opravy a aktualizace aplikací vydávané výrobci. U operačního systému MS Windows ponechte povolené automatické aktualizace.
Ověřte si, že se přihlašujete ke stránkám banky. Po otevření přihlašovací stránky zkontrolujte, že se vám v adresním řádku v horní části internetového prohlížeče zobrazuje adresa https://ib.anosd.cz/eib/. Zkontrolujte si v adresním řádku po kliknutí na zámeček v zeleně podbarvené části řádku, že se zobrazí informace o certifikovaném zabezpečení dané služby.

3) Chraňte svůj počítač a mobilní telefon
Používejte antivirové a antispyware programy. Pravidelně je aktualizujte, aby jejich účinnost byla co nejvyšší.
Připojujte se k internetu přes firewall (program nebo technické zařízení), který minimalizuje rizika neoprávněného přístupu k vašemu počítači z internetu. Ponechte aktivován osobní firewall, který je standardní součástí operačního systému Windows.
Instalujte si aplikace výhradně z oficiálních obchodů - Nikdy neinstalujte do svých počítačů programy ze zdrojů, které nemáte prověřeny. Při instalaci aplikací do svých mobilních telefonů, stahujte aplikace pouze z oficiálních obchodů (App Store, Google Play a Windows Phone Store).

4) Nereagujte na podvodné e-maily
Nereagujte na e-mailové zprávy, které jste obdrželi od neznámých adresátů, nebo zprávy s podezřelým názvem či obsahem. Soustřeďte se také na správnou gramatiku e-mailových zpráv, podvodné e-maily většinou obsahují gramatické chyby.

a) Pokud takový podvodný e-mail obdržíte, neodpovídejte na něj, neklikejte na vložené odkazy, neotevírejte přílohy. ANO spořitelní družstvo nikdy neoslovuje klienty v otázkách bezpečnosti e-mailem, proto nikdy nesdělujte své osobní ani bezpečnostní údaje v rámci reakce na obdržený e-mail.
b) Neklikejte na odkazy v e-mailech od neznámých či podezřelých odesílatelů a nezadávejte svoje citlivé údaje. ANO spořitelní družstvo to NIKDY nepožaduje.

5) Neotevírejte neznámé odkazy na cizí servery
a) Při práci na internetu neotevírejte odkazy na neznámé servery (např. s erotickým obsahem) a ty, se kterými se setkáte v nevyžádaných e-mailech.
b) Využívejte ochranu proti spamu
Používejte ke své e-mailové schránce ochranu proti spamu. Dále doporučujeme použít ještě další ochranné nástroje – označované jako antispyware, antiadware apod.

6) Pravidelně sledujte informace o bezpečnosti
ANO spořitelní družstvo zveřejňuje informace k bezpečnostní situaci na svých Internetových stránkách www.anosd.cz a také přímo v internetovém bankovnictví.

7) Mějte správně nastavený váš „chytrý“ mobilní telefon
„Chytrý“ telefon obsahuje operační systém a je tedy nutné u těchto moderních typů telefonu brát větší obezřetnost i na bezpečnost. Nepoužívejte programové úpravy svého chytrého mobilního telefonu, které umožňují plný administrátorský přístup (jedná se o úpravy typu: jailbreak (pro iOS), root (pro Android). U telefonů se systémem Android doporučujeme zakázat „instalaci z neznámých zdrojů“. Touto úpravou si zajistíte, že si stahujete a instalujete aplikace pouze z oficiálního úložiště.