Desatero bezpečnosti

Modrá pyramida stavební spořitelna, a. s.,
sídlo: Bělehradská 128, č. p. 222, 120 21 Praha 2,
IČO: 60192852 – zapsaná v obchodním rejstříku vedeném
u Městského soudu v Praze v oddílu B, ve vložce 2281
(dále jen „MP“, „Modrá pyramida“ nebo „my“)

Modrá pyramida

Člen skupiny KB

Desatero bezpečnosti je jednoduchý přehled opatření a zásad, které vám pomůžou být na internetu dostatečně chráněni. Přijměte je prosím za své, mějte je vždy před očima a řiďte se jimi za každé situace.

Deset bezpečnostních přikázání:

1. Navštěvujte jen známé webové stránky a stahujte prověřené aplikace.

TIP

U každé navštívené webové stránky si zkontrolujte, jestli její internetová adresa sedí k zobrazenému obsahu. Nestahujte a nespouštějte soubory s neznámým obsahem. Do chytrého telefonu stahujte pouze aplikace z oficiálních obchodů Google Play a App Store.

2. Zvolte si bezpečný PIN

TIP

Jako PIN si nastavte 4 číslice. Vyberte takové, které nejde jednoduše uhádnout. PIN nikomu neprozrazujte, nepište si ho na papírky nebo do mobilu a pravidelně PIN měňte. Pokud váš telefon neumožňuje přihlašování otiskem prstu, nastavte si pro odemčení telefonu jiný PIN, než je PIN pro vstup do aplikace. Nezapomínejte, že zodpovědnost za ochranu vašeho účtu je jen na vás.

3. Pokud máte chytrý telefon, můžete povolit ověření otiskem prstu nebo snímáním obličeje.

TIP

Pokud váš telefon odemknutí otiskem prstu nebo snímáním obličejem umožňuje, můžete tuto možnost pro zabezpečení aplikace využít. Odemykání telefonu tímto způsobem nepovolujte žádné další osobě. Pokud máte dvojče nebo sourozence, který je vám velmi podobný, doporučujeme přihlašování snímáním obličeje nepoužívat.

4. Své citlivé údaje nikdy nikomu neprozrazujte ani nepředávejte přes e-mail. Neklikejte na odkazy v podezřelých e-mailech.

TIP

U e-mailů od nás si vždy zkontrolujte, jestli přišly z e-mailové adresy končící @mpss.cz nebo @kbinfo.cz. Nedůvěryhodné e-maily ze své poštovní schránky vymažte. Banka, policie ani nejbližší členové rodiny nemají právo požadovat vaše přihlašovací údaje apod. V žádném případě nereagujte na výzvy k zadání/ověření přihlašovacích údajů. Své uživatelské jméno a PIN k aplikaci MP Home chraňte a nikomu je neprozrazujte. Pokud se setkáte s podezřelým jednáním, hned se nám ozvěte na čísle +420 210 220 230.

5. Aplikaci MP Home používejte pouze na svém mobilu. Ten vždy chraňte před zneužitím.

Pokud se o zařízení dělíte s jinými členy domácnosti nebo s přáteli, dáváte jim současně přístup i k vašim aplikacím, včetně aplikace MP Home. Nainstalujte si proto aplikaci do zařízení, která používáte jenom vy.

6. Používejte programy pro ochranu svého mobilu. Jde hlavně o antivirový program.

TIP

I když placené antiviry nabízí mnohem lepší ochranu, dají se najít i kvalitní bezplatné programy. Při jejich výběru se řiďte hodnocením a recenzemi uživatelů, kteří už program používají. Svůj antivirový program pravidelně aktualizujte.

7. Pravidelně aktualizujte operační systém a veškeré programy. Používejte jen legálně pořízené programy a systémy.

Používejte jen originální operační systém a neprovádějte v něm úpravy, které umožní plný administrátorský přístup typu root nebo jailbreak. Takto upravená zařízení nekupujte a nepoužívejte.

8. Používejte jen důvěryhodné Wi-Fi sítě

Pokud pracujete s aplikací MP Home, nepoužívejte nedůvěryhodné Wi-Fi sítě (např. bezplatné a otevřené Wi-Fi sítě v obchodních centrech, kavárnách apod.). Hrozí totiž, že by někdo cizí mohl „odposlechnout“ vaše citlivá data (např. přihlašovací údaje) a zneužít je.

9. Nastavte si možnost najít a smazat zařízení

Nastavte si ve svém zařízení možnost vyhledání zařízení. Pokud svůj telefon ztratíte nebo budete mít obavy, že se dostal do nepovolaných rukou, můžete ho najít a případně z něj i vzdáleně vymazat data. U Androidu tuto funkci nastavíte v sekci Najdi moje zařízení, u iOS zařízení ji najdete v sekci Nastavení pod položkou Najít iPhone.

10. V případě dotazů ke smlouvě se ozvěte svému poradci. Pokud objevíte problém s aplikací, hned volejte infolinku +420 210 220 230.