

---

## Úvod

Vítejte v části internetových stránek věnované zabezpečení. Tato část Vám poskytne odpovědi na otázky, které si kladete v souvislosti s bezpečností při využívání internetového bankovníctví. Obsahuje informace o následujících oblastech:

- Nejnovější pokyny pro zabezpečení
- Ověření, zda se jedná o ING Online
- Aktualizace počítačových programů
- Antivirové programy
- Firewally
- Slovníček pojmů z oblasti počítačové bezpečnosti

Internetové bankovníctví ING Online můžete používat bez obav, protože ING Online využívá nejmodernější dostupnou šifrovací technologii. K tomu, abyste mohli této výhody využít, používejte nejnovější verzi doporučeného internetového prohlížeče. V současné době nabízí šifrovací technologii poslední verze prohlížeče Microsoft Internet Explorer.

V souladu se zásadami ochrany osobních údajů jsou veškeré údaje, jež nám svěřujete, uchovávány v nejpřísnější tajnosti. Vy jste jediná osoba, která má přístup k Vašemu účtu a která může potvrdit transakci při použití Vašeho přihlašovacího jména, jedinečného hesla a jedinečného osobního identifikačního čísla (PIN). Při zadávání transakce po internetu se všechny transakce evidují pro případ následného ověřování.

*[Oznámení v případě posílení zabezpečovacích prvků:*

*Zanedlouho budeme vylepšovat zabezpečení přihlašování k naší internetové službě. K tomuto kroku přistupujeme proto, že zabezpečení internetu pokládáme za velmi důležité. Kromě dodržení našeho jednoduchého, jasného a proveditelného slibu se totiž jedná o jednu z našich hlavních priorit.]*

---

## Nejnovější pokyny pro zabezpečení

### Osobní údaje

Vaše heslo a PIN představují klíč k Vašemu účtu. Pamatujte na to, že jste povinni své bezpečnostní údaje chránit:

- Uchovávejte svou kartu Smart Card na bezpečném místě.
- Osobní přístupové kódy si nikam nezapisujte, nesdělujte je jiným osobám a neposílejte je e-mailem.
- Při přihlašování postupujte tak, aby Vaše osobní přístupové kódy nikdo nezjistil.
- Nepoužívejte jednoduchá hesla, která lze snadno uhodnout.
- Provádějte často změnu hesla. Z hlediska zabezpečení společnost ING vyžaduje, abyste si heslo měnili alespoň jednou měsíčně.
- V případě ztráty nebo krádeže Vaší karty Smart Card neprodleně kontaktujte ING pro zablokování přístupu k ING Online.
- Při odhlašování používejte funkci „Odhlásit“.
- Dbejte zvýšené opatrnosti při používání internetového bankovníctví v internetové kavárně, protože není jasné, jaká je tam úroveň zabezpečení počítačů.

### Internetové bankovníctví ING Online

- Každá kombinace přihlašovacího jména a hesla je jedinečná. Při přihlašování se ověřuje platnost zadaných údajů. Jste-li přihlášení na stránky ING Online a po dobu 15 minut systém ING nezaznamená žádnou akci, Vaše pracovní relace bude ukončena. Pro pokračování v práci se musíte znovu přihlásit.
- Při podepisování transakce se k transakci připojí Váš elektronický podpis, který zaručí, že transakce splňuje podmínku neodvolatelnosti.

- Na stránkách ING Online jsou prováděny pravidelně nezávislé penetrační testy specializovanými externími společnostmi. Jakékoli zjištěné nedostatky v zabezpečení se ihned odstraňují.

## Komunikace pomocí e-mailu a bezpečnostní výstrahy

ING Online Vám nikdy nezašle e-maily, ve kterých by Vás žádala o Vaše důvěrné nebo osobní bezpečnostní údaje. Obdržíte-li podobnou žádost, okamžitě se prosím obraťte na Help desk elektronického bankovníctví na čísle +420 257 474 666, nebo kontaktujte mailem adresu [abuse@ing.com](mailto:abuse@ing.com).

Obdržíte-li e-mail obsahující vložený odkaz a žádost o zadání osobních údajů, považujte jej za podezřelý. Neuvádějte žádné citlivé údaje, které by mohly napomoci přístupu k Vašemu účtu, přestože se stránka jeví jako legitimní.

## Vishing

Vishing je obdobou phishingu a k útokům využívá telefon nebo VoIP (nástroje pro přenos hlasových informací pomocí sítí založených na protokolu IP). V případě takového útoku obdržíte e-mail nebo zprávu SMS s žádostí, abyste zavolali na bezplatné telefonní číslo a potvrdili své údaje, nebo obdržíte nahranou telefonickou zprávu s žádostí o zadání údajů k Vašemu účtu. Pokud tak učiníte, útočník může s Vašimi osobními údaji volně nakládat a zneužít Váš účet.

V zájmu ochrany používejte pouze zveřejněná oficiální čísla telefonního centra Vaší finanční instituce a při poskytování Vašich osobních údajů po telefonu dbejte opatrnosti. Pamatujte si, že ING Vás nikdy po telefonu o heslo žádat nebude.

## Nápodoba internetových stránek ING Online

Zabezpečení má pro ING Online zásadní význam a rádi bychom všechny naše zákazníky ujistili, že již jsou přijata rychlá a vhodná opatření pro případ, že by se někdo pokusil imitovat stránky ING Online. Podrobnější informace o dalších možných preventivních opatřeních jsou uvedeny v části „Ověření, zda se jedná o ING Online“.

Podezřelé e-maily prosím přepošlete na adresu: [abuse@ing.com](mailto:abuse@ing.com) a my záležitost podrobně prozkoumáme.

## Prozrazení úplného čísla PIN

O sdělení Vašeho čísla PIN Vás nikdy nebudeme žádat. Budete-li o to někdy požádáni, přestaňte stránku nebo službu používat a okamžitě nás kontaktujte na telefonním čísle +420 257 474 666 nebo nám zašlete e-mail na adresu [abuse@ing.com](mailto:abuse@ing.com).

## Falešné stránky a varování před phishingem

Podvodníci vytvářejí věrohodně se tvářící, ale falešné nebo klamavé internetové stránky. Jejich záměrem je nalákat zákazníky, aby zadali své osobní údaje. Tyto údaje jsou poté použity při pokusu o přístup na Váš bankovní účet. Podvodníci čím dál častěji zasílají e-maily, aby zákazníky na tyto stránky přesměrovali. Tento postup se také označuje jako „phishing“.

Podobné e-maily v nedávné době obdrželi zákazníci několika finančních institucí a tento druh činnosti se bude pravděpodobně objevovat čím dál častěji. Podvodné e-maily obvykle obsahují odkaz na falešnou internetovou stránku a snaží se majitele účtů oklamat výzvou, aby zadali své jméno a bezpečnostní údaje pod záminkou toho, že bezpečnostní údaje se mohou aktualizovat nebo měnit. Podrobnější informace naleznete v části „Ověření, zda se jedná o ING Online“.

## Krádeže osobních údajů

Zákazníci by si měli být vědomi toho, že existují zlomyslné způsoby, kterými mohou cizí osoby napadnout jejich počítač a pokusit se do něj nainstalovat falešný software, který dokáže zachytit osobní údaje a přesměrovat zákazníka na falešné internetové stránky. Společnost Microsoft se je některých problémů vědoma a nejnovější informace a rady můžete získat poklepnutím na [tento odkaz](#).

Stejně jako jindy Vám doporučujeme, abyste na svém počítači pravidelně aktualizovali antivirové programy i jiný software. Používejte aktualizované počítačové programy a dbejte na to, aby byl Váš

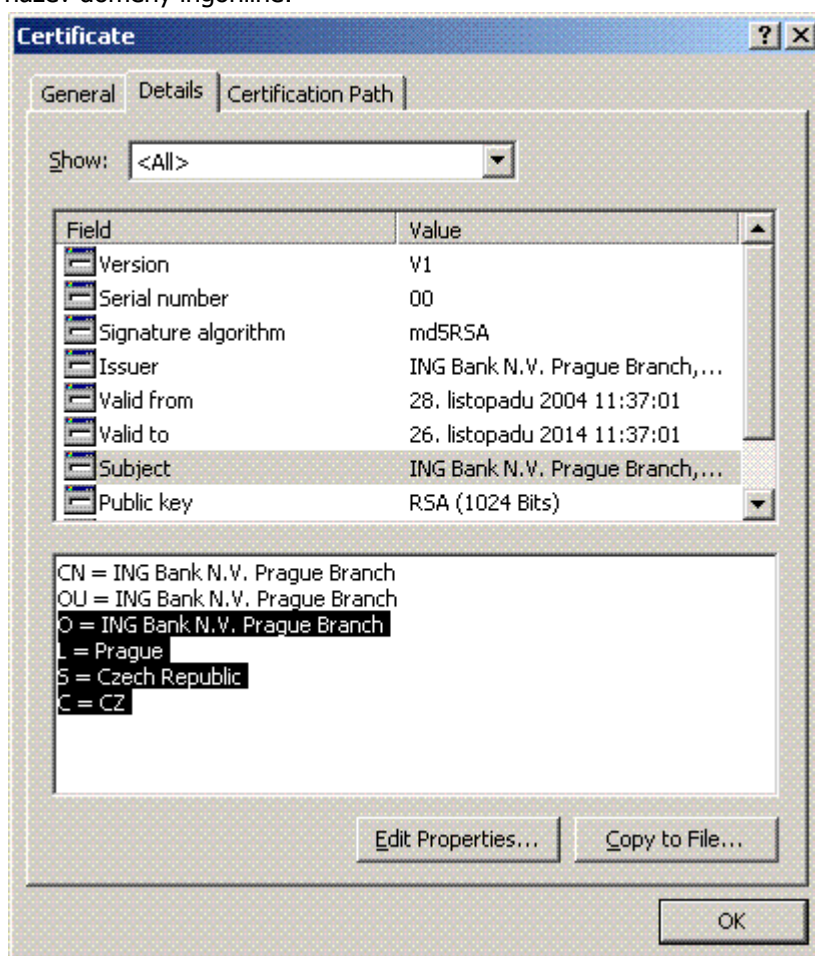
počítač vybaven nejnovějšími zabezpečovacími a antivirovými programy. Přečtěte si prosím části „Aktualizace počítačových programů“ a „Antivirové programy“.

---

## Ověření, zda se jedná o ING Online

Před poskytnutím osobních údajů si vždy ověřte následující:

- Kdykoli budete na jakékoli internetové stránce zadávat své osobní údaje, například údaje k bankovnímu účtu, ujistěte se, že stránka všechny údaje, které na ní zasíláte a které jsou Vám zasílány, šifruje. Vždy se též ujistěte, že je správně zapsán název domény.
- Ujistěte se, že pole URL začíná písmeny „https“ a ne „http“ (viz níže):
- Zkontrolujte, zda je ve spodní části prohlížeče zobrazen symbol visacího zámku (viz níže):
- Dvojitým poklepnutím na symbol zámku ve Vašem prohlížeči si ověřte, zda doménu vlastní společnost, s níž chcete komunikovat. Hledaným prvkem je to, zda se v následujícím příkladě vyskytuje název domény ingonline:



Např.: secure.ingonline.cz = (poddoména=secure).(doména=ingonline).(top-level doména=cz)

Narazíte-li na falešné stránky napodobující naše stránky, kontaktujte nás prosím na adrese [abuse@ing.com](mailto:abuse@ing.com).

---

## Aktualizace počítačových programů

Hackeri, popř. viry občas najdou slabiny v programech, které jim umožní získat nelegální přístup do Vašeho počítače. V zájmu předcházení takovým útokům a ochrany Vašeho počítače nabízejí tvůrci softwaru na svých internetových stránkách možnost bezplatného stažení aktuální verze jejich programu.

Chcete-li si ověřit, jaká existuje nejnovější verze Vašeho programu, zadejte jednoduše internetovou stránku jeho vydavatele (většinou v části Stáhnout – Download). Pokud například používáte Microsoft Windows, navštivte stránky Microsoft Windows Update.

Máte-li nainstalovány starší verze prohlížeče než je verze 6, je snadné stáhnout si jeho aktualizovanou verzi:

- pro Internet Explorer: klepněte na odkaz pro bezplatné stahování (Download) na stránce Microsoft: <http://www.microsoft.com/cze/windows/products/winfamily/ie/default.msp>

Jaké jsou nejčastější problémy spojené s používáním bezpečnostního certifikátu v prohlížeči a jak je lze odstranit? Klepněte [zde](#) (v anglickém jazyce) pro zobrazení problémů při používání prohlížeče a aplikací poskytovaných třetími stranami, které byly zaznamenány firmou VeriSign.

---

## Antivirové programy

Možná již používáte nějaký antivirový program, ale aby byl tento software účinný, musí být pravidelně aktualizován nejnovějšími soubory s definicemi virů. Pokud si nejste jisti, jak to udělat, měli byste se podívat do nápovědy programu.

Existuje mnoho účinných programů, ze kterých je možno vybírat, ale k nejběžnějším komerčním produktům patří\* (v abecedním pořadí):

- AVAST
- AVG
- Kaspersky Labs
- McAfee
- Norman
- Panda
- Sophos
- Symantec
- Trend Micro

*\*Seznam dodavatelů výrobků je uveden pouze pro informaci a neměl by se považovat za doporučení ING Online. Pokud si zákazníci nejsou jisti vhodností jednotlivých produktů, měli by požádat o odbornou radu. Další informace je možno najít hledáním výrazů 'Antivirové programy' a 'Spyware' v internetových vyhledávacích.*

## Programy na odstraňování spywaru

Možná již používáte nějaký program na odstraňování spywaru, ale aby byl tento software účinný, musí být pravidelně aktualizován. Pokud si nejste jisti, jak to udělat, měli byste se podívat do nápovědy programu.

Existuje mnoho účinných programů, ze kterých je možno vybírat, ale k nejběžnějším komerčním produktům patří\* (v abecedním pořadí):

- Lavasoft Ad-aware
- McAfee
- Spy Sweeper
- Spybot-Search & Destroy
- Symantec

*\*Seznam dodavatelů výrobků je uveden pouze pro informaci a neměl by se považovat za doporučení ING Online. Pokud si zákazníci nejsou jisti vhodností jednotlivých produktů, měli by požádat o odbornou radu. Další informace je možno najít hledáním výrazů 'Antivirové programy' a 'Spyware' v internetových vyhledávacích.*

---

## Osobní firewally

Firewall je další malý program, který pomáhá chránit Váš počítač a jeho obsah před útoky z internetu. Když je nainstalovaný, brání neoprávněným datovým přenosům do Vašeho osobního počítače a z něho.

Existuje mnoho účinných programů, ze kterých je možno vybírat, ale k nejběžnějším komerčním produktům patří\* (v abecedním pořadí):

- BlackICE Defender
- Kerio Personal Firewall
- McAfee Personal Firewall
- Norton Personal Firewall
- Sygate Personal Firewall
- Tiny Personal Firewall
- Zone Alarm

*\*Seznam dodavatelů výrobků je uveden pouze pro informaci a neměl by se považovat za doporučení ING Online. Pokud si zákazníci nejsou jisti vhodností jednotlivých produktů, měli by požádat o odbornou radu. Další informace je možno najít vyhledáním výrazu „firewall“ v internetových vyhledávačích.*

---

## Slovníček pojmů z oblasti počítačové bezpečnosti

### Antivirové programy

Programy k detekci a odstraňování počítačových virů. Nejjednodušší programy prohledávají spustitelné soubory a blokuji známé viry ze seznamu. Jiné jsou neustále aktivní, pokoušejí se detekovat činnost virů. Antivirový program by měl vždy zahrnovat možnost pravidelné aktualizace, která mu umožní odhalit nejnovější viry, jakmile se objeví. Pro další informace, přejděte k části „*Antivirové programy*“.

### Back doors

Back doors (zadní dvířka) je skrytý hardwarový nebo softwarový vstup do počítačového systému, který může být použit k překonání bezpečnostní ochrany systému. Chcete-li získat další informace, přejděte k části „*Antivirové programy*“.

### Cookies

Cookies („koláčky“) jsou malé soubory uložené na pevném disku počítače. Cookies jsou obvykle neškodné a používají se k identifikaci zákazníka tak, aby mohl webové stránky používat efektivněji. Cookies mohou obsahovat informace o Vašich předvolbách, které umožňují přizpůsobení webových stránek Vaším potřebám.

### Firewall

Firewall je malý program, který pomáhá chránit Váš počítač a jeho obsah před útoky z internetu nebo sítě. Když je řádně nainstalovaný, brání neoprávněným datovým přenosům do Vašeho osobního počítače a z něho. Existuje mnoho účinných programů, ze kterých je možno vybírat. K nejběžnějším komerčním programům patří např. produkty společností Zone Labs, Symantec (Norton), McAfee a Computer Associates. V mnoha případech existuje verze komerčního programu, která je pro soukromé uživatele bezplatná. Chcete-li získat další informace, přejděte k části „*Osobní firewally*“.

### Phishing

Phisher je podvodník nebo webová stránka, kteří se snaží oklamat lidi a přimět je k tomu, aby prozradili své osobní informace. (např. hesla k účtům a čísla kreditních karet). Phisher obvykle používá podvodné e-mailové zprávy nebo online reklamy jako návnadu, aby nalákal nic netušící uživatele na podvodné webové stránky, kde je pak lstí přiměje k vyrazení osobních informací. Chcete-li získat další informace, přejděte k části „*Ověření, zda se jedná o ING Online*“.

### Prohlížeče

- IE5 a vyšší

## Secure Socket Layer (SSL)

Protokol Secure Socket Layer (SSL) poskytuje vysokou úroveň zabezpečení pro internetovou komunikaci. SSL zajišťuje šifrovanou komunikační relaci mezi Vaším internetovým prohlížečem a webovým serverem. SSL pomáhá zajistit zachování důvěrnosti citlivých informací (např. čísel kreditních karet, zůstatků na účtech a jiných soukromých finančních a osobních údajů) odesílaných při online transakcích přes internet mezi Vaším prohlížečem a webovým serverem.

## Spyware

Jakýkoli počítačový program, který tajně shromažďuje informace o klientech prostřednictvím jejich internetového spojení bez jejich vědomí, obvykle pro reklamní účely. Spywarové aplikace jsou obvykle připojeny jako skrytá součást programů, které lze stáhnout z internetu; je však třeba podotknout, že většina aplikací spyware neobsahuje. Spyware po instalaci monitoruje činnost zákazníka na internetu a odesílá tyto informace na pozadí někomu jinému. Spyware může také shromažďovat informace o e-mailových adresách a dokonce heslech a číslech kreditních karet.

Spyware se podobá trojskému koni v tom, že zákazníci tento produkt instalují nevědomky při instalaci něčeho jiného. Obětí spyware se obvykle stanete tak, že si stáhnete některý z dnes dostupných programů pro peer-to-peer výměnu souborů. Chcete-li získat další informace, přejděte k části „*Antivirové programy*“.

## Šifrování

Šifrováním se Vaše data ještě před odesláním přes internet převádějí do zakódované podoby, čímž se neoprávněným uživatelům zabrání v přečtení těchto informací. V ING Online používáme 128bitové šifrování Secure Socket Layer (SSL), které se v našem oboru považuje za standardní úroveň. Potvrzení že Vaše relace probíhá v bezpečném „zašifrovaném“ prostředí, poznáte podle toho, že v poli internetové adresy uvidíte https://, popř. symbol uzamčeného visacího zámku.

## „Time out“ relace

Jedná se o automatické ukončení zabezpečené relace z bezpečnostních důvodů po určité době nečinnosti serveru. Může k němu dojít, i když něco zapisujete na stránku nebo do datového pole, tuto událost aktivuje nulová komunikace s našimi servery, nikoli nečinnost klávesnice nebo myši. Tuto ochranu mají všechny naše služby internetového bankovníctví.

## Trojský kůň

Program, který se jeví jako legitimní, ale když je spuštěn, vykonává nějakou zakázanou činnost. Může se používat k lokalizaci informací o heslech nebo může způsobit větší zranitelnost systému při příštím vstupu nebo jednoduše ničit programy nebo data na pevném disku. Trojský kůň se podobá viru až na to, že se sám nereplikuje. Zůstává v počítači a škodí nebo umožňuje někomu ovládat počítač ze vzdáleného místa. Trojské koně se do počítačů často ukrádají spolu s bezplatnými hrami nebo jinými obslužnými programy. Chcete-li získat další informace, přejděte k části „*Antivirové programy*“.

## Virus

Počítačový program obvykle skrytý v jiném zdánlivě neškodném programu, který produkuje vlastní kopie a vkládá je do jiných programů a který obvykle vykonává škodlivou činnost (např. ničí data). Chcete-li získat další informace, přejděte k části „*Antivirové programy*“.

## Worm

Worm (červ) je program, který je vytvořen tak, aby se replikoval a rozšířil po celém počítačovém systému. Obvykle se skrývá v souborech a rozesílá tyto soubory prostřednictvím libovolných dostupných síťových spojení. Kromě toho se červy mohou rychle šířit prostřednictvím elektronické pošty. Chcete-li získat další informace, přejděte k části „*Antivirové programy*“.

## Zabezpečené relace

Když se přihlásíte k internetovému bankovníctví, bude Vám sděleno, že se jedná o „zabezpečenou relaci“. Technologie SSL se při Vaší relaci internetového bankovníctví používá k šifrování informací ještě předtím, než opustí Váš počítač, aby se zajistilo, že je nepřečte nikdo jiný. V závislosti na nastavení

Vašeho prohlížeče se může objevit vyskakovací okno, které Vás bude informovat o tom, že vstupujete na zabezpečenou stránku. To, že jste na „zabezpečené stránce“, poznáte podle toho, že před webovou adresou uvidíte „https://“. V pravém dolním rohu okna Vašeho prohlížeče také uvidíte symbol uzamčeného visacího zámku.

## **Zachytávání a zaznamenávání stisků kláves**

Cokoli na počítači napíšete, můžete být zachyceno a zaznamenáno. Takovou skrytou činnost může provádět hardwarové zařízení připojené k osobnímu počítači nebo program běžící téměř neviditelně přímo v počítači. Zaznamenávání stisků kláves často využívají podvodníci ke shromažďování osobních údajů včetně hesel. Některé současné viry jsou schopny instalovat takový program bez vědomí uživatele.

Riziko, že se setkáte se zaznamenáváním stisků kláves, je větší na osobních počítačích sdílených několika uživateli, např. na počítačích v internetových kavárnách a knihovnách. Přítomnost jakéhokoli takového programu na Vašem osobním počítači odhalí antispywarový program. Zákazníci si mohou anti-spyware bezplatně stáhnout z internetu; chcete-li získat další informace, přejděte k části „*Antivirové programy*“.

V brzké době zavedeme online klávesnici (Key Pad), která minimalizuje riziko, že by někdo cizí mohl zachytit a zaznamenat cokoli, co pomocí klávesnice do svého počítače napíšete.

## **Zranitelnost**

Bezpečnostní díry/chyby jsou vady, závady nebo programovací chyby. Ty mohou využít neoprávnění uživatelé k přístupu k počítačovým sítím nebo webovým serverům z internetu. Jakmile se tato zranitelná místa odhalí, vydavatel programu vyvine „záplaty“, „opravy“ nebo „aktualizace“, které si můžete stáhnout, a problém tak vyřešit. Chcete-li získat další informace, přejděte k části „*Aktualizace počítačových programů*“.