

# „PHISHING“, „KEYLOGGERY“ A „TROJSKÉ KONĚ“

## CO JE „PHISHING“?

Čím více lidí používají internet, tím více spoléhají na jeho pohodlné zprostředkování služeb jako jsou např. bankovní služby, nákupy on-line a podobně. Bohužel však je internet též **zneužíván podvodníky**, kteří rozesílají e-maily, které mají vzbuzovat dojem, že pocházejí právě od této služby. Tyto e-maily vypadají neuvěřitelně věrohodně a běžně se jim říká „**Phishing**“ (název je odvozen od anglického slova „Fishing“ - Rybaření), a jejich jediným cílem je „ulovit“ Vás a Vaše osobní údaje.

## VAROVÁNÍ:

Bezpečné webové adresy mají na začátku předponu **https**: (v níž koncové „s“ značí, že jsou bezpečné - „secure“) a mají ikonu zámku v pravém dolním rohu. Hackeři jsou však schopni tyto vlastnosti věrohodně zfalšovat, a proto na ně nemůžete spoléhat bezvýhradně. Dvojitým kliknutím na symbol zámku otevře dialogové okno s určením toho, kdo je majitelem dané licence, např. „Issued to (vydáno pro): production.citibank.cz“. Avšak hackeři často používají podvodná vyskakující okna (tzv. „pop-up“ okna) společně s legitimními stránkami a snaží se zjistit Vaše osobní údaje. Někdy tato okna mohou vypadat jako přihlašovací obrazovky. Absolutní spoléhání na ikonu zámku proto může být riskantní.

## JAK ROZPOZNAT „PHISHING“ OD KOREKTNÍHO E-MAILU

Může se stát, že obdržíte neočekávaný e-mail z Vaší banky nebo od některého z poskytovatelů jiných služeb, které využíváte. Ve skutečnosti se však může jednat o odesílatele, který pouze předstírá, že je Vaší bankou nebo dodavatelem služeb. Obvykle jste požádáni o zaslání informací o Vašem účtu, někdy dokonce i o Váš PIN kód a jste vyzváni k tomu, abyste dotyčné informace zaslali odesílateli buď e-mailem anebo vstupem na jím uvedenou webovou stránku. Pro snazší navigaci může **podvodný e-mail dokonce obsahovat webový odkaz, na který stačí pouze kliknout a přímo se dostanete na dotyčnou stránku.**

Internetoví podvodníci se Vás pokoušejí rafinovaně obelstít používáním výrazů jako je „bezpečnost a údržba“ či „vyšetřování nesrovnalostí.“ Často uvádějí, že například „Váš účet byl zablokován“ nebo že „je potřeba znovu ověřit Vaše osobní údaje“, „Vaše kreditní karta byla zrušena“ anebo dokonce že „na Vašem kontě je velká částka peněz, potvrďte prosím výběry hotovosti“. A to jen proto, aby Vás navnadili a zvýšili pravděpodobnost Vašeho kliknutí na dotyčný hyperlink, pomocí něhož Vás přimějí navštívit žádoucí stránku.

## CO POTŘEBUJETE VĚDĚT

Jestliže Váš počítač není přiměřeně chráněn pravidelně aktualizovaným antivirovým softwarem a firewallem (Brána „firewall“ představuje software či hardware, který vytváří ochrannou hráz mezi Vaším počítačem a potenciálně škodlivým obsahem na internetu. Pomáhá počítač chránit před internetovými podvodníky a počítačovými viry a tzv. „červy“.) a neaktualizujete-li pravidelně svůj operační systém oficiálně vydávanými aktualizacemi (tzv. bezpečnostními „záplatami“), budete velice obezřetní a nikdy neotevírejte odkazy, jež jsou součástí obdrženého e-mailu. Používáte-li internet pro své bankovní operace nebo online nákupy, vždy zadávejte oficiálně uváděnou webovou adresu do prohlížeče ručně, předejdete tak případnému přesměrování.

Vaše banka po Vás nikdy nebude požadovat sdělování Vašich osobních údajů či kódu PIN prostřednictvím e-mailu, proto na email nereagujte. Odolejte pokušení odpovědět anebo provést pokyny zaslání e-mailem. Třebaže to někdy může být dost obtížné - zejména dozvíte-li se, že Váš účet byl „zmražen“ anebo „zrušen“, či když Vám někdo namlouvá, že se vystavujete peněžité pokutě či sankci.

**Nikdy neodpovídejte na „Phishingové“ e-maily. Máte-li podezření, že je e-mail podvodný, ověřte obdržený e-mail u firmy uvedené v e-mailu přes telefonní číslo o němž víte, že je autentické (v případě Citibank je to naše linka CitiPhone ☎ 233 062 222).**

## „KEYLOGGERY“ A „TROJSKÉ KONĚ“

Internetoví podvodníci neváhají použít tzv. keyloggery a trojské koně - malé programy, které Vám přijdou jako e-mail, spam či příloha e-mailu nebo mohou být ukryté ve webové stránce.

Otevřením takového webové stránky, e-mailu či přílohy se tento software skrytě a nepozorovaně nainstaluje do Vašeho počítače. Je přitom schopen zachytit a identifikovat Vámi provedené úderky na klávesnici počítače anebo prohledat Váš počítač a nalézt údaje o Vašem účtu nebo kreditní kartě. Vymazávejte veškeré podezřelé e-maily aniž byste je otevírali a nikdy neotevírejte podezřelé přílohy, třebaže mohou vzbuzovat dojem, že pocházejí od někoho, koho sami znáte.

## ANTIVIROVÁ OCHRANA

Chraňte svůj počítač nainstalováním účinného antivirového programu. Nezapomeňte jej však pravidelně aktualizovat!

## CHRAŇTE SVŮJ POČÍTAČ AKTUALIZOVANÝM ANTIVIROVÝM SOFTWAREM.

Citi never sleeps™

Pro získání dalších informací navštivte internetové stránky  
[www.citibankonline.cz](http://www.citibankonline.cz) nebo volejte CitiPhone ☎ 233 062 222.

**citibank**®