

# Nebezpečné maily s viry a Phishing



Nebezpečné maily s viry a [Phishing](#) – Slyšíme o tom kolem sebe často, víme o tom skoro všichni, ale přesto se stále díky různým fintám daří útočnickům zavirovávat počítače, případně získávat citlivé přístupové údaje. A protože opakování je matka moudrosti, zopakujme si varování na nebezpečné maily s viry a maily s Phishing technikou.

Jelikož provozuji několik webů a pracuji na různých projektech, mám několik mailů a také na některých doménách kontroluji maily v tzv. doménovém koši, tak se probírám tunami spamu a tím také často narážím na nebezpečné maily s viry a Phishing maily. Poslední dobou se roztrhl pytel se škodlivými maily, proto bych rád opakoval varování pro všechny.

## **Nebezpečné maily s viry**

Nebezpečné maily s virem jsou buď s přílohou, nebo s odkazem. Zavirovaný mail může obsahovat přiložený soubor, který je zavirovaný a po spuštění, nebo otevření souboru se počítač zaviruje. Zavirovat počítač si můžete také mailem s odkazem, který vede na zavirovanou stránku. Proto dávejte pozor jaké přílohy v mailu otvíráte, nebo na jaké odkazy klikáte.

Co se týče přiložených souborů, dávejte si pozor na přípony souborů, a na odkazy v mailu se zaměřte na začátek adresy odkazu. Neotvírejte spustitelné soubory s příponou .exe, .bat,

.apk, .lnk, .msi. Viry mohou obsahovat také soubory Office .doc, .docx, .xls, .xlss. Takový soubor má v sobě obsažené škodlivé makro. Dobrá rada je mít nastavený Office tak, aby nespouštěl makra u souborů stažených z internetu.

## Nebezpečné maily s viry – vzory nebezpečných mailů s přílohou



## Nebezpečné maily Phishing

Phishing maily jsou maily tvářící se jako mail z oficiální adresy nějaké instituce, převážně banky, nebo internetové peněženky vyzývající k úpravě údajů.

Technika jak vás nalákat a přimět kliknout na odkaz, nebo přílohu je různá. Útočník může lákat na slevu, na výhodný nákup, na výdělek, na zajímavé video, zkrátka na cokoli

zajímavého. Může také působit jako update nějakého programu, nebo nastavení profilu. Stačí ale trochu pozornosti a trochu přemýšlet před tím, než na něco kliknete.

V případě, že podezřelé a nebezpečné maily obsahují odkazy, zkontrolujte odkaz a pokud odkaz vypadá podezřele neklikejte na něj. Podezřelý odkaz poznáte tak, že například v mailu se uvádí, že máte přejít na stránku například Komerční banky kliknutím na odkaz. Odkaz Komerční banky začíná <https://www.kb.cz/>. V podvodném mailu bude odkaz vypadat jinak. Bude začínat jinou doménou. Vždy je odkaz nějak jinak, než je opravdová adresa banky, nebo společnosti.

## Nebezpečné maily s Phishing – vzory nebezpečných Phishing mailů



•24 SERVIS 24 Internetbanking · x

← → C 🏠 [rodrigojucarep.com.br/Ref150101/](http://rodrigojucarep.com.br/Ref150101/)

Vážený uživateli, používáním SERVIS 24 souhlasíte s používáním cookies, které aplikace ke správnému fungování vyžaduje. [Souhlasím](#)

**SERVIS 24**  
INTERNETBANKING

Přihlášení SERVIS 24

Heslem | Klientským certifikátem

**UKÁZKA PODVODNÉ STRÁNKY**

Vždy pečlivě kontrolujte adresu, správná je „<https://www.servis24.cz/>!“

**Videoukázky**  
JAK BEZPEČNĚ NA INTERNETBANKING

**SERVIS 24 Internetbanking**

- [Demo](#)
- [Více informací](#)

Banka touto formou NIKDY po svých klientech nepožaduje sdělení jejich citlivých údajů.

**První přihlášení**

Klientské číslo

Heslo

Tajný kód

Úplné názvy

Datum narození

Adresa

PSČ

Mobilní číslo

Pevně telefonní

[Zapomenuté/zablokované heslo](#)

[Klíčovnice](#) [? Návrat k přihlášení](#)

Ukázka jak mohou stránky kam odkazují nebezpečné maily využívající metodu phishing. Kontrolujte adresy.

Dejte si opravdu pozor na co v mailu klikáte a jakou přílohu otvíráte. Dejte si pozor na **nebezpečné maily s viry a Phishing maily**. Mějte kvalitní a aktualizovaný [antivirový program](#), ale stejně se na něj nespolehejte na 100%. Vždy se chovejte obezřetně. A poslední rada na závěr. Zálohujte. Zálohujte si důležitá data, protože pokud si zavirujete počítač, tak ne vždy se podaří odvírovat bez ztráty dat. Některé viry zašifrují disk a pro vás data budou nečitelná. Takže zálohujte.