# Mám napadené zařízení

**Příručka pro identifikaci a odstranění malwaru**

Verze dokumentu: 1.0
Datum vytvoření: 22. ledna 2026
Architekt a iniciátor projektu: Milan Trnka

---

## Úvod

Jestliže máte podezření, že vaše zařízení bylo napadeno malwarem, připravili jsme pro vás přehledný seznam kroků, které vám pomohou situaci vyhodnotit a případně škodlivý software odstranit. Dodržováním těchto doporučení můžete minimalizovat riziko ztráty dat a ochránit své soukromí před kybernetickými hrozbami.

---

## Co mám tedy dělat?

Tyto jednotlivé kroky vám mohou pomoci malware nejprve identifikovat a poté i odstranit.

### 1. Odpojte počítač od internetu

Odpojením zařízení od internetu zabráníte malwaru další komunikaci se zařízením útočníka.

**Jak na to?**

- **Mobilní zařízení** – aktivujte režim „Letadlo". V tomto režimu se standardně vypne veškerá bezdrátová komunikace.
- **Počítač** – odpojte zařízení od internetu buď odpojením síťového kabelu, nebo vypnutím Wi-Fi. Využíváte-li jiné způsoby připojení, nezapomeňte je také deaktivovat.

### 2. Obnovte systém ze zálohy

Jestliže pravidelně zálohujete a víte, kdy mohlo dojít k infikaci vašeho zařízení, vraťte systém do stavu před infekcí nahráním dané zálohy. Pokud zálohy nemáte, pokračujte dále v našem návodu.

**Jak zjistím, jestli mám zálohy?**

- **Mobilní zařízení** – U mobilních zařízení obvykle nemáte systémové zálohy. Máte-li zapnuté zálohování, pravděpodobně se jedná o zálohu uživatelských dat (fotek, souborů...) do cloudu, nikoliv o kompletní zálohu systému.
- **Počítač** – Nemáte-li manuálně nastaveny zálohy systému na externí uložiště, pravděpodobně nevlastníte potřebné systémové zálohy.

### 3. Spusťte antivirový program

V případě počítače spusťte hloubkovou kontrolu systému. Odhalí-li váš antivir nějaké hrozby, odstraňte je.

### 4. Zkontrolujte běžící procesy a programy

Najděte ve svém zařízení systémovou aplikaci „Správce úloh" a zde zkontrolujte, zda na vašem zařízení neběží nějaká podezřelá aplikace. Nejste-li si jisti, jestli se jedná o podezřelou aplikaci, vyhledejte ji pomocí webového prohlížeče. Legitimní aplikace vždy budou mít oficiální stránky, kde se budete moci dočíst, k čemu daná aplikace slouží. Najdete-li podezřelý program, odstraňte jej.

**Jak na to?**

- **Mobilní zařízení** – V případě mobilního zařízení naleznete veškeré instalované aplikace v nastavení. Umístění tohoto nastavení se liší dle využitého operačního softwaru.
- **Počítač** – Umístění systémové aplikace „Správce úloh" se liší dle využitého operačního softwaru.

### 5. Změňte hesla k důležitým účtům

Jestliže jste zjistili, že vaše zařízení je/bylo napadeno, je potřeba také změnit hesla minimálně ke všem důležitým účtům, ke kterým jste se přihlašovali nebo máte heslo uloženo v napadeném zařízení. Útočník může tato hesla získat a zneužít.

### 6. Zvažte přeinstalaci systému

Jestliže si nejste jisti, zda jste malware opravdu odstranili, zvažte přeinstalaci samotného systému. Tímto krokem budou ze systému odstraněna všechna data a tím tedy i možný malware. Nezapomeňte si před tímto krokem zálohovat potřebná data jako jsou fotografie, dokumenty atd. – přeinstalací budou odstraněna.

**Jak na to?**

- **Mobilní zařízení** – Postup se liší podle operačního systému, obvykle však zahrnuje resetování zařízení do továrního nastavení, které naleznete v nastavení.
- **Počítač** – Pro stolní zařízení stačí využít nástroje pro obnovení nebo přeinstalování operačního systému pomocí instalačního média.

---

## Co můžu dělat, aby se situace neopakovala?

### Dávejte pozor na kybernetické hrozby

Buďte obezřetní při instalaci neznámého softwaru a vždy si ověřte jeho zdroj. Nikdy neotevírejte podezřelé e-mailové přílohy nebo odkazy, které vám přijdou od neznámých či nedůvěryhodných odesílatelů. Kromě toho používejte dostatečně silná a unikátní hesla pro všechny své účty a ideálně je spravujte pomocí správce hesel.

### Nezapomínejte na aktualizace systému a softwaru

Pravidelné aktualizace operačního systému, antivirového programu a dalšího vámi využívaného softwaru jsou

klíčové pro ochranu před novými hrozbami. Vývojáři často opravují bezpečnostní chyby, které mohou útočníci zneužít k napadení vašeho zařízení. Pokud je to možné, zapněte si automatické aktualizace, abyste měli vždy nejnovější ochranu bez nutnosti ručního zásahu.

---