

/ Obsahuje-li tento dokument zmínky produktů, nejedná se o affiliate program, ale doporučení na základě nezávislých testů a zkušeností.

// Chybí vám nějaké informace? Potřebujete radu? Neváhejte mne kontaktovat na webu www.karolsuchanek.com

ZABEZPEČENÍ ZAŘÍZENÍ: ZÁMEK ZAŘÍZENÍ A ŠIFROVÁNÍ



Přečtěte si, jak zvolit a nastavit vhodnou formu zamykání a šifrování svého počítače a smartphonu.

OBSAH

- [Počítač s Windows 10](#)
- [Počítač MAC](#)
- [Smartphone s Androidem](#)
- [iPhone](#)

POČÍTAČ S WINDOWS 10

Možnosti přihlášení do Windows 10

Pro přístup k vašim možnostem přihlášení přejděte na **Start**  > **Nastavení** 
> **Účty** > **Možnosti přihlášení**

Na stránce Možnosti přihlášení jsou k dispozici následující metody přihlášení:

- Obličej ve Windows Hello
- Otisk prstu ve Windows Hello
- PIN ve Windows Hello
- Klíč zabezpečení
- Heslo
- Obrázkové heslo

Jsou tu i tato nastavení:

- Vyžadovat přihlášení: Vyžaduje, abyste se po nepřítomnosti znovu přihlásili do zařízení.
- Dynamický zámek: Automaticky uzamkne zařízení, když jste pryč.
- Ochrana osobních údajů: Zobrazí nebo skryje osobní informace na přihlašovací obrazovce a umožňuje vašemu zařízení používat vaše přihlašovací údaje k opětovnému spuštění aplikací po aktualizaci nebo restartování.



Změňte nebo spravujte heslo:


1. Přejděte na **Start**  > **Nastavení**  > **Účty** > **Možnosti přihlášení**
2. Vyberte **Heslo** a pak vyberte **Změnit**

Windows Hello

Windows Hello umožňuje přihlášení k zařízením, aplikacím, online službám a sítím pomocí rozpoznání obličeje, duhovky, otisku prstu nebo PIN kódu. I když vaše zařízení s Windows 10 může biometriku Windows Hello používat, můžete se rozhodnout, že ji

používat nebudete. Pokud to ale považujete za dobrou volbu, můžete být klidní, že informace, které identifikují váš obličej, duhovku nebo otisk prstu, nikdy vaše zařízení neopustí. Windows neukládá snímky vašeho obličeje, duhovky nebo otisků prstů na zařízení ani nikam jinam.



Chcete-li Windows Hello zapnout, přejděte na **Start**  > **Nastavení**  > **Účty** > **Možnosti přihlášení**. Vyberte metodu **Windows Hello**, kterou chcete nastavit, a poté vyberte **Nastavit**. Pokud se služba Windows Hello v části Možnosti přihlášení nezobrazí, nemusí být pro vaše zařízení dostupná.

Chcete-li ze zařízení odebrat Windows Hello a všechna související biometrická identifikační data, přejděte na **Start**  > **Nastavení**  > **Účty** > **Možnosti přihlášení**. Vyberte metodu Windows Hello, kterou chcete odebrat, a pak vyberte **Remove**.

Dynamický zámek

System Windows dokáže podle zařízení spárovaných s vaším osobním počítačem zjistit, že jste pryč, a zamknout počítač krátce poté, co se dostanete mimo dosah signálu Bluetooth. Díky tomu je pro jiné osoby obtížnější získat přístup k vašemu zařízení, pokud odejdete od počítače a zapomenete ho uzamknout.

Chcete-li dynamický zámek aktivovat:

1. Přejděte na **Start**  > **Nastavení**  > **Účty** > **Možnosti nastavení**
2. V části **Dynamický zámek** zaškrtněte políčko **Umožnit systému Windows automatické uzamčení zařízení, když jste pryč**
3. Spárujte telefon s počítačem pomocí Bluetooth. [Jak spárovat zařízení pomocí Bluetooth](#)

Jakmile jsou zařízení spárovaná, vezměte si při odchodu telefon s sebou a váš počítač se automaticky zamkne přibližně minutu poté, co se dostanete mimo rozsah signálu Bluetooth.


Co je šifrování zařízení?

Šifrování zařízení pomáhá chránit vaše data a je k dispozici na široké řadě zařízení s Windows. K datům na vašem zařízení, které má zapnuté šifrování dat, budou mít přístup pouze osoby, které jsou oprávněny. Pokud vaše zařízení nepodporuje šifrování dat, může se vám místo toho podařit zapnout standardní šifrování nástrojem BitLocker. Nástroj BitLocker není k dispozici v edici Windows 10 Home.

Je tato funkce k dispozici na mém zařízení?

Šifrování zařízení je k dispozici na podporovaných zařízeních se všemi edicemi systému Windows 10. Pokud chcete místo toho používat standardní šifrování nástrojem BitLocker, je tato možnost k dispozici na podporovaných zařízeních s edicemi Windows 10 Pro, Enterprise nebo Education. Některá zařízení mají oba typy šifrování. Například zařízení Surface Pro se systémem Windows 10 Pro má jak zjednodušené prostředí šifrování zařízení, tak i úplné možnosti správy nástrojem BitLocker. Nejste si jistí, kterou verzi Windows používáte? Podívejte se na článek [Který operační systém Windows používám?](#)



Jak zjistit, jestli můžete používat šifrování zařízení

1. Do vyhledávacího pole na hlavním panelu zadejte **Systémové informace**, klikněte pravým tlačítkem na položku **Systémové informace** v seznamu výsledků a potom vyberte **Spustit jako správce**. Můžete také vybrat tlačítko Start  a potom v části **Nástroje pro správu Windows** vybrat **Systémové informace**.
2. V dolní části okna **Systémové informace** vyhledejte položku **Podpora šifrování zařízení**. Pokud je tam uvedena hodnota **Splňuje požadavky**, znamená to, že vaše zařízení podporuje šifrování. Pokud šifrování není k dispozici, může se vám podařit použít standardní šifrování nástrojem BitLocker.


Zapnutí šifrování zařízení

1. Přihlaste se do Windows pomocí účtu správce (možná se budete muset odhlásit a znovu přihlásit kvůli přepnutí účtů). Další informace najdete v článku [Vytvoření](#)

[místního účtu nebo účtu správce ve Windows 10.](#)

2. Vyberte tlačítko **Start**  a potom vyberte **Nastavení**  > **Aktualizace a zabezpečení** > **Šifrování zařízení**. Pokud se nezobrazí možnost **Šifrování zařízení**, znamená to, že není dostupná. Místo toho se vám může podařit zapnout standardní šifrování nástrojem BitLocker.
3. Pokud je šifrování zařízení vypnuté, vyberte možnost **Zapnout**

Zapnutí standardního šifrování nástrojem BitLocker


1. Přihlaste se do Windows pomocí účtu správce (možná se budete muset odhlásit a znovu přihlásit kvůli přepnutí účtů). Další informace najdete v článku [Vytvoření místního účtu nebo účtu správce ve Windows 10.](#)
2. Do vyhledávacího pole na hlavním panelu zadejte **Spravovat BitLocker** a v seznamu výsledků pak vyberte stejnou položku. Nebo můžete vybrat tlačítko **Start**  a potom v části **Systém Windows** vybrat **Ovládací panely**. V **Ovládacích panelech** vyberte **Systém a zabezpečení** a pak v části **nástroj BitLocker Drive Encryption** vyberte **Spravovat nástroj BitLocker**. Tato možnost se zobrazí pouze v případě, že je nástroj BitLocker pro vaše zařízení k dispozici. Není k dispozici v edici Windows 10 Home.
3. Vyberte **Zapnout Bitlocker** a pak postupujte podle pokynů.

POČÍTAČ MAC

Jak nastavit zamykání počítače Mac

Počítače Mac mají již v továrním nastavení zapnuto přihlašování heslem.

Pokud váš Mac po zapnutí nebo probuzení z režimu spánku nevyžaduje heslo, znamená to, že máte aktivní funkci **Automatické přihlášení**. Pro lepší zabezpečení je potřeba tuto funkci vypnout:


1. Otevřete nabídku Apple  > **Předvolby systému** > **Uživatelé a skupiny** > **Přihlášení**
2. U položky **Automatické přihlášení** zvolte **Vypnuto**

Jak zapnout šifrování dat počítače Mac pomocí funkce FileVault

Funkce FileVault zašifruje data na vašem startovacím disku, takže neoprávnění uživatelé k nim nebudou mít přístup.

Poznámka: Pokud máte iMac Pro nebo jiný model Macu s čipem Apple T2, data na vaší jednotce jsou už zašifrována automaticky. Zapnutí FileVaultu však poskytuje ještě další ochranu, protože pro dešifrování vašich dat požaduje vaše přihlašovací heslo.

1. Na Macu vyberte nabídku **Apple**  > **Předvolby systému** > **Zabezpečení a soukromí** > **FileVault**

Pokud je zámek vlevo dole zamčený , kliknutím na něj [odemkněte panel předvoleb](#).

2. Vyberte **Zapnout FileVault**. Je možné, že budete vyzváni k zadání vašeho hesla.
3. Zvolte způsob odemknutí disku a obnovení přihlašovacího hesla v případě zapomenutí:
 - **Účet na iCloudu**: Pokud už účet máte, klikněte na **Povolit mému účtu na iCloudu odemýkat disk**. Pokud účet na iCloudu nemáte, klikněte na **Nastavit můj účet na iCloudu pro reset mého hesla**
 - **Klíč zotavení**: Klikněte na **Vytvořit klíč zotavení a nepoužívat můj účet na iCloudu**. Klíč zotavení si opište a uchovejte ho na bezpečném místě, ideálně ve správci hesel
4. Klikněte na tlačítko **Pokračovat**

Pokud váš Mac používají další uživatelé, budou zašifrovány i jejich údaje. Zašifrovaný disk uživatelé odemknou svým přihlašovacím heslem.

SMARTPHONE S ANDROIDEM

Nastavení zámku obrazovky

Pokud váš telefon nevyžaduje aktivaci otevřením zámku obrazovky, proveďte aktivaci této funkce:

1. Otevřete aplikaci **Nastavení**

2. Vyberte **Zabezpečení**. Pokud možnost Zabezpečení nevidíte, vyhledejte náповědu na [webu podpory výrobce telefonu](#).
3. Vyberte **Zámek obrazovky** (pokud tuto volbu vidíte)
4. Nebo přímo vyberte typ zámku obrazovky, který chcete použít a postupujte podle pokynů na obrazovce.

Možnosti zámku obrazovky

Naprostý základ, který byste měli vždy používat, je **PIN**.

Zadejte alespoň šest číslic. Delší kódy PIN bývají bezpečnější.

Abyste posílili bezpečnost funkce PIN, aktivujte si odemykání **rozpoznáním obličeje** nebo **otiskem prstu**.

V závislosti na modelu telefonu se dostupné možnosti mohou lišit. Další informace o zámku obrazovky zařízení najdete na [webu podpory výrobce](#).

Dále nabízejí telefony s Androidem pro odemykání možnost **Gesto** - načrtnutí jednoduchého obrazce prstem. Toto zabezpečení není příliš silné a nedoporučuji jej používat.

Šifrování dat v telefonu s Androidem

Před samotným šifrováním dat je vhodné pro prevenci nečekaných problémů provést kompletní zálohu.

1. Přejděte do **Nastavení > Osobní > Zabezpečení > Šifrovat telefon**. Budete informováni o průběhu procesu a vyzváni k připojení nabíječky.
2. Následně si budete muset zvolit heslo, bezpečnostní gesto nebo PIN kód pro zpětné dešifrování, které musí obsahovat specifický počet znaků a číslic. Potvrzením volby se zařízení začne šifrovat. Smartphone se bude několikrát restartovat a v průběhu operace ho nebudete moci používat.

Jakmile je šifrování dokončeno, automaticky se vygeneruje dešifrovací klíč, který je bezpečně uložen v Androidu. V případě potřeby můžete zašifrovat také připojenou SD kartu, aby z ní nebylo možné číst ani kopírovat data. Stačí v sekci Zabezpečení zvolit tuto možnost.

IPHONE

Jak zapnout nebo změnit odemykání obrazovky

1. Otevřete aplikaci **Nastavení**
2. Na iPhonech s Face ID vyberte **Face ID a kód**
Na iPhonech s tlačítkem plochy vyberte **Touch ID a kódový zámek**
3. Vyberte **Zapnout kódový zámek** nebo **Změnit kód**

Nastavením přístupového kódu zapnete ochranu dat, která šifruje data v iPhoneu. Po nastavení kódu můžete iPhone odemknout pomocí **Face ID** (odemykání obličejem) nebo **Touch ID** (odemykání otiskem prstu), v závislosti na modelu. Zvolte jednu z těchto variant a postupujte podle instrukcí na obrazovce iPhoneu.