

Bezpečnost vašich účtů

Jak jde o přihlašování do důležitých internetových účtů, měla by být vždy na prvním místě bezpečnost. Mezi tyto důležité účty patří bezesporu emailová schránka a všechny účty, na kterých máte peníze. To se bezesporu týká také účtů na portálu GLOCIN. Pokud je to možné, rozhodně si zapněte dvou faktorové ověření při každém přihlášení.

V praxi potom přihlašování probíhá tak, že kromě hesla musíte zadat další kód, které je automaticky generován pomocí aplikace Google Authenticator. Vy poté během přihlašování tento kód zadáte. Dále v portálu Glocin tento kód zadáváte při potvrzování transakcí a změn. Nový kód se generuje každých 30sekund. Nemusíte se však bát, že by jste to nestihli. Každý vygenerovaný kód platí ještě 30sekund po svém vypršení.

Samotný proces přihlašování zabere o několik vteřin déle, na druhou stranu je váš účet mnohem lépe zabezpečen a i kdyby se teoreticky někdo dostal k vašemu heslu, tak mu nebude k přihlášení stačit.

Jak funguje Google Authenticator

Aplikace Google Authenticator automaticky generuje šestimístné kódy, které jsou potřeba k přihlášení do různých účtů.

Tyto kódy se pravidelně mění a jsou napevno spojeny přímo s vaším telefonem.

Aby se tedy někdo dostal k vašemu účtu, potřeboval by jak znalost vašeho hesla, tak fyzický přístup k vašemu telefonu. Tím se k zabezpečení přidá další vrstva a jakýkoliv pokus o získání kontroly nad vaším účtem je pro případné útočníky značně zkomplikováno.

Dvoufázové ověření s aplikací Google Authenticator

Kde stáhnout aplikaci Google Authenticator?

Aplikace Google Authenticator je dostupná pro mobilní zařízení se systémy Android a iOS a je dostupná jak na Google Play tak na App Store:

[Stáhněte aplikaci Google Authenticator z Google Play](#)

[Stáhněte aplikaci Google Authenticator z App Storem](#)

Jak zapnout dvoufaktorové ověření (2FA)

Zapnutí dvoufaktorového ověření je velmi snadné. Postupujte takto:

1. Po přihlášení na Glocin portál jděte do svého profilu a na záložce zabezpečení zvolte možnost zapnutí dvoufaktorového ověření. Tato možnost je obvykle nabízena už při samotné registraci, jinak jí najdete obvykle pod záložkou "Security"/"Zabezpečení".
2. Zobrazí se vám QR kód, který slouží k propojení vašeho účtu s telefonem.

3. Stáhněte a zapněte aplikaci Google Authenticator na svém telefonu a vpravo dole klikněte na červené kolečko se symbolem +.
4. Zvolte možnost skenování čárového kódu, čímž se zapne fotoaparát, který je potřeba namířit na QR kód.
5. QR kód se načte do aplikace Google Authenticator a účet je propojen přímo s vaším telefonem.
6. Při přihlašování na Glocin portál nebo do jiné služby je potřeba zapnout aplikaci Google Authenticator a zadat vygenerovaný kód.

Co když ztratím mobil nebo vymažu aplikaci Google Authenticator?

Aplikace Google Authenticator není přímo propojena s vaším Google účtem a není synchronizovaná se žádným zařízením. Tím se zaručuje bezpečnost, kdy je k získání kódu opravdu potřeba mít mobil fyzicky u sebe a opsat kód. Na druhou stranu, pokud se mobil ztratí nebo se aplikace vymaže, tak nelze opětovným nainstalováním snadno vrátit propojené účty.

Při zapnutí dvoufázového ověření pomocí Google Authenticator vám bude generován soukromý kód, který lze zadat přímo do Google Authenticator. Pokud se vrátíte k návodu, tak v bodě 4 byste místo QR kódu vybrali možnost Zadání dodaného klíče.

Vygenerovaný soukromý kód 2fa si poznamenejte na bezpečné místo a nejlépe je napište na papír a dobře uschovejte. Pokud si smažete aplikaci a nemáte přístup k tomuto kódu, je obvykle zpřístupnění Glocin portálu nebo jiné služby velmi komplikované a bude potřeba opravdu dokázat, že majitelem účtu jste právě vy.

Co když si zakoupím nový mobil nebo potřebuji přenést aplikaci Google Authenticator do jiného telefonu?

V těchto dvou případech kdy máte původní telefon s funkční aplikací Google Authenticator je možné postupovat následovně.

- První a nejjednodušší způsob je přihlásit se do portálu Glocin jít do svého profilu a na kartě/záložce zabezpečení vidíte ve spodní části volbu zobrazení svého stávajícího klíče. Opište zde kód z aplikace Google Authenticator příslušící k danému účtu v portálu a klikněte na zobrazit soukromý klíč. Portál vám zobrazí váš soukromý kód tak QR kód a vy si tak můžete přenést přihlašování do jiného telefonu nebo na další telefon.
- Druhý o trochu složitější způsob je že do nového zařízení ručně opíšete svůj soukromý kód, který jste si před tím pečlivě opsali a bezpečně uložili.

Bezpečné uložení není uložení do emailu, fotografií, na plochu počítače, do

peněženky, do diáře a podobně. Myslete bezpečně nebo o své peníze přijdete.