

## FACEBOOK BEZPEČNOSTNÍ CHYBA

Jak jste si v mém statutu mohli přečíst, došlo postupně k napadení mých dvou facebookových profilů. O jeden účet jsem přišel úplně, záložní se mi podařilo zachránit. (Díky své přirozené obezřetnosti a nutkové potřebě mít vyřešené odpovědi na otázku “co kdyby“, mám všechna svá data zálohována.) Naštěstí.

Ač samotný Facebook používám výhradně na svém počítači i a mobilu (obě zařízení mám chráněna proti nezvaným návštěvníkům), mám nastaveno **dvoufázové zabezpečení** a nastaveny **oznámenky**, které musím v jednom či druhém zařízení potvrdit, podařilo se útočnickovi zcizit mi účet. Facebook pomocí svých algoritmů sice detekoval útok, útočnickovi se ale již podařilo převzít vládu nad mým účtem a níže napíšu jak k tomu došlo. A dopředu mohu rovnou napsat, že vám žádné zabezpečení nepomůže. **Chyba je totiž v logice potvrzování změn.**

### CO SE TEDY STALO?

Mnozí z nás to znají, Facebook posílá emailem oznámení o změnách na účtu, případně informace, které jste si nastavili, aby vám přicházely do emailové schránky.

Jednoho krásného dne mi přišlo oznámení o novém přihlášení z jiného místa. Prakticky ve stejnou chvíli dorazil také bezpečnostní kód a informace o možném napadení účtu. A jak vidíte, chodilo toho více.

|          |                |                                                                                                                                                                                |        |
|----------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| Facebook | Doručená pošta | Resetoval jste právě své heslo? - Zdravíme, Lukáš, Chceme vás informovat, že vaše heslo bylo právě resetováno. Informace o této změně Pátek 26. ledna 2024 v 0:19 (UT...       | 26. 1. |
| Facebook | Doručená pošta | Did you just reset your password? - Hi Lukáš, This is to let you know that your password was just reset. About this change Friday, January 26, 2024 at 12:19 AM (UTC+01) N...  | 26. 1. |
| Facebook | Doručená pošta | 462438 je kód pro obnovení vašeho účtu na Facebooku - Dostali jsme žádost o reset vašeho Facebook hesla. Zdravíme, Lukáš, Dostali jsme žádost o reset vašeho Faceb...          | 26. 1. |
| Facebook | Doručená pošta | Bezpečnostní kód je: Facebook - Bezpečnostní kód je: Facebook Hi Lukáš, Your security code is: 49672411 To help us confirm your identity on Facebook, we need to verify ...    | 26. 1. |
| Facebook | Doručená pošta | Someone may have accessed your account - We think your account was hacked. Secure your login details to get it back. Hi Lukáš, It looks like someone may have access...        | 25. 1. |
| Facebook | Doručená pošta | Your Facebook security code - Your Facebook security code Zdravíme, Lukáš, Bezpečnostní kód je: 68064618 Abychom mohli potvrdit vaši totožnost na platformě Faceboo...         | 25. 1. |
| Facebook | Doručená pošta | Přihlásili jste se ke službě Facebook z jiného místa? - Zdravíme, Lukáš! Podle všeho se někdo v 25. ledna v 23:14 pokusil přihlásit k vašemu účtu z Firefox pro Windows 10 ... | 25. 1. |

OK, není to poprvé, co něco podobného vidím, takže jsem zůstal v klidu. **Odmítl jsem změny**, tak jak mi **Facebook radil** a snažil jsem provést **krátký postup pro trvalé zabezpečení účtu**. Každá změna musí být potvrzena kódem, a také jsem tak učinil.

Zdravíme, Lukáš!

Podle všeho se někdo v **25. ledna v 23:14** pokusil přihlásit k vašemu účtu z **Firefox pro Windows 10**. Přihlášení jsmeablokovali. Chceme se jen ujistit, že jste to vy, kdo se pokusil přihlásit z nového m...

**Pokud jste to nebyl(a) vy, přihlaste se k Facebooku**, abychom vás mohli provést krátkým postupem trvalého zabezpečení účtu.

S přáním pěkného dne  
Tým Facebooku

**Your Facebook security code**

Zdravíme, Lukáš,

Bezpečnostní kód je:

**6 8 0 6 4 6 1 8**

Abychom mohli potvrdit vaši totožnost na platformě Facebook, potřebujeme ověřit vaši e-mailovou adresu. Kód zadejte v prohlížeči. Dá se použít jen jednou.

Pokud jste o kód nepožádal(a), je možné, že se k vašemu účtu snaží někdo dostat. [Zajistěte bezpečnost svého účtu pro jistotu tím, že se změníte heslo.](#)

Thanks,  
The Facebook Security Team

Poté, co jsem provedl veškeré kroky, **kterými mě Facebook prováděl**, **nedošlo k zabezpečení účtu** ani jsem se **ke svému profilu nedostal**. Naopak, přišel další email a tentokrát varování, že **můj účet byl napaden**. (Jak k tomu sakra mohlo dojít, když jsem si účet podle průvodce právě zabezpečil, napadlo mě.)

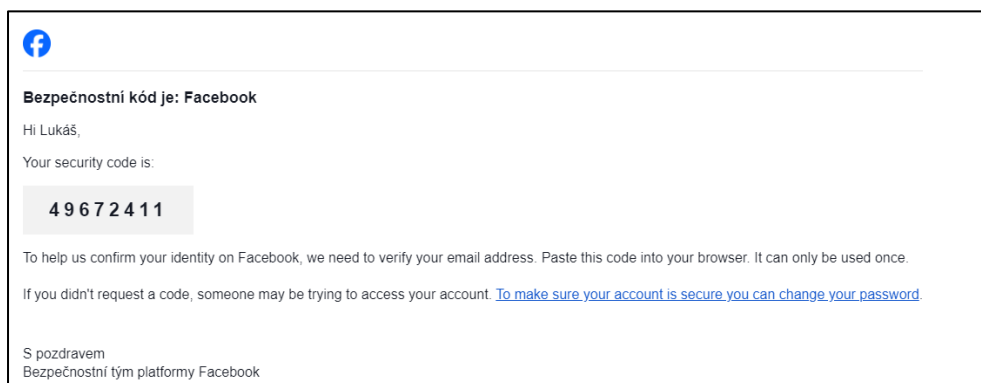
Hi Lukáš,

It looks like someone may have accessed your Facebook account. To secure your account, you'll need to answer a few questions and change your password the next time you go to Facebook.

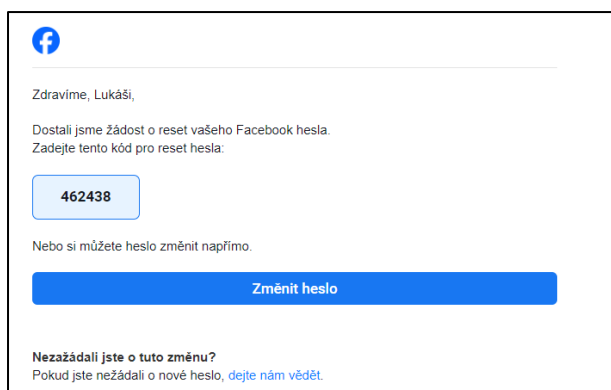
For your protection, no one can see you on Facebook until you secure your account.

[Secure Your Account Now](#)

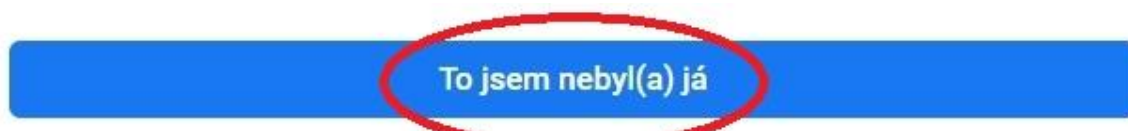
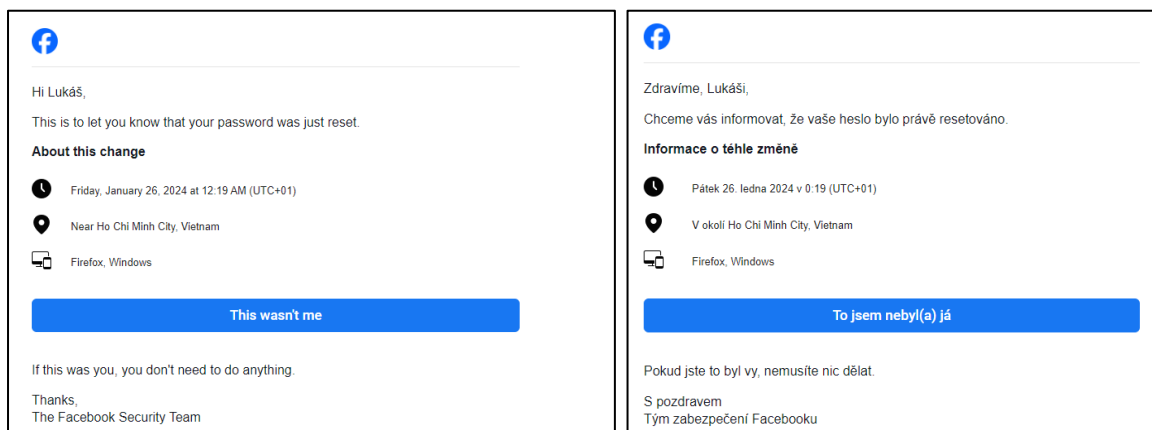
Postupuju i nadále podle návodu, [jak mi Facebook radil](#): **zadávám bezpečnostní kód** a snažím se opět **změnit heslo** a zabezpečit účet. **Aniž bych o tom věděl, právě v tento okamžik jsem předal útočnickovi kontrolu nad svým účtem.**



Vzápětí došel další email s požadavkem na změnu hesla. Změnu jsem **nepotvrzoval**, ale kliknul jsem na odkaz, že jsem **o nové heslo nežádal**. Nic naplat, toto nepomohlo.

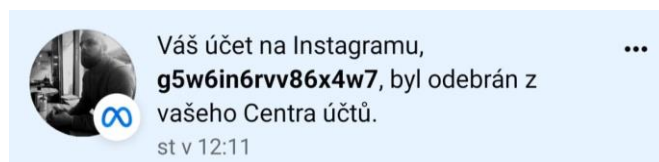


Ač jsem dělal, co jsem dělal a že jsem dělal všechno, [co mi samotný Facebook radil](#), útočnick z druhé strany planety již ovládl můj účet. (Jak je to sakra možné, když sedím v Ostravě!!!)



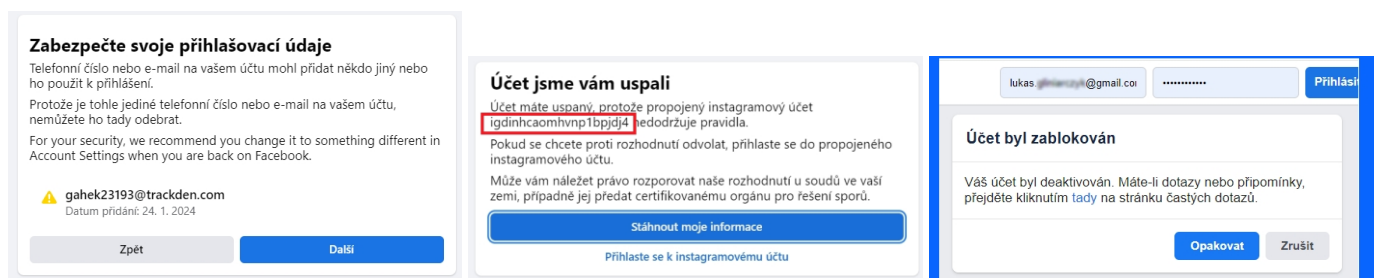
## PROČ MI Odstavili ÚČET?

Útočnick po převzetí mého účtu začal do **Centra účtu** (zastřešení FB a IG pokud máte více účtu nebo jste adminy stránek a skupin) své vlastní účty. Tyto jeho účty ovšem porušovaly podmínky Facebook, tak se Facebook rozhodl na věčné časy („definitivně“) **pro uspání mého účtu** (rozuměj, zrušení).



## Jak vypadal facebookový průvodce během pokusu o zabezpečení účtu?

Jak vidíte, viděl jsem zprávy o odebrání a nahrazení emailové adresy (vždyť jsem změnu přece zamítl?), uspání účtu i jeho následném zablokování.



## KDE SE STALA CHYBA?

Znovu si prohlédněte screeny emailových zpráv.

Myslíte si, že vás dvoufázové a další zabezpečení ochrání? **Tak to vůbec!** Pokud provádíte změny emailů, telefonních číslo nebo se jen pokoušíte obnovit zapomenuté heslo, **všechno se potvrzuje kódy**. Stále nic? Tak čtěte pozorně:

Všimli jste si, že některé emaily jsou v češtině a některé v angličtině? **Tak přesně tady je jádro pudla:** útočník vás nechá postupovat podle facebookového návodu a v pravou chvíli začne i on provádět změny a vy, aniž byste to tušili, **nepotvrzujete své změny, ale ty jeho!!!** Proto ty opakované emaily, to vy nic neděláte špatně, to on ve stejnou chvíli dělá to samé a čekám, že mu jeho požadavek na změnu potvrdíte!

Šílené? Ano!!! Tak jednoduše vás jde připravit o účet na facebooku.

## JAK TO SPRAVIT?

Toto nejde opravit. Zrušený účet, je zrušený účet.

Pokud jste v účtu měli platební kartu (třeba kvůli placeným reklamám), přihlašujete se do eshopů nebo jiných aplikací, všechno má pod kontrolou útočník. Všechny vaše údaje. Fotky, zprávy, status, přátelé. A pomoc se nedovoláte!

## CO DĚLAT?

Není žádná varianta jak se tomuto vyvarovat, pokud k útoku dojde.

Nezmatkujte. Nic nepotvrzujte, nezažívejte heslo, nesnažte se zachránit účet. **Zachovejte klid!**

**Vaše obezřetnost je v tuto chvíli to jediné, co vám pomůže zachránit váš účet.** Musíte počkat, až Facebook detekuje útok a útočníka odstaví.

**Pokud omylem potvrdíte útočníkovi jeho žádost, je s vaším účtem konec.**

**PAMATUJTE:** Raději týden bez facebookového účtu než na věčné časy odevzdat útočníkovi vaše data.

Pokud si nevíte rady nebo se bojíte, požádejte o pomoc důvěryhodnou osobu, která je technicky zdatná může vám pomoci.

**Dobrá rada:** V každém případě, mějte účet zabezpečený emailem i SMSkou.

---

Anticopyright | překlad žádoucí | psáno rodilým Ostravakem | Verze 1.0

CC BY-NC-ND 4.0 PRÁVNÍ UJEDNÁNÍ

Uveďte původ-Neužívejte komerčně-Nezpracovávejte 4.0 Mezinárodní

---

Z vlastní zkušenosti sepsal a bezpečnostní chybu odhalil Lukáš Gliniarczyk  
podpořit mě můžete zde zadáním práce 🙌 [www.elgesko.cz](http://www.elgesko.cz)