E-Bezpečí 2024, 9(1): Page 109-111. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=4080

JAK LIDÉ PŘICHÁZEJÍ O ÚČTY NA FACEBOOKU A JAKÉ TRIKY HACKEŘI POUŽÍVAJÍ

Kamil KOPECKÝ

Facebook je jednou z nejrozšířenějších sociálních sítí na světě, s miliardami uživatelů, kteří každý den sdílejí osobní informace, fotky a komunikují s přáteli a rodinou. Tato obrovská databáze osobních údajů přirozeně přitahuje pozornost hackerů a kyberzločinců. V následujícím článku se podíváme na nejčastější způsoby, jak lidé přicházejí o své účty na Facebooku, a jaké triky hackeři používají.

1. Phishingové útoky

Phishing je jedním z nejběžnějších způsobů, jak hackeři získávají přístup k účtům na Facebooku. Uživatelé dostanou e-mail nebo zprávu, která vypadá, jako by byla od Facebooku, a která je požádá, aby klikli na odkaz a přihlásili se do svého účtu. Tento odkaz však vede na falešnou stránku, která vypadá jako přihlašovací stránka Facebooku. Jakmile uživatel zadá své přihlašovací údaje, tyto údaje jsou odeslány hackerovi, který je pak může použít k přihlášení na skutečný účet uživatele.

2. Slabá hesla a jejich opakované používání

Mnoho uživatelů stále používá jednoduchá a snadno uhodnutelná

hesla, jako jsou "123456" nebo "password". Navíc často používají stejná hesla pro více účtů na různých platformách. Pokud je jedno z těchto hesel kompromitováno na jiné webové stránce, hackeři mohou toto heslo zkusit použít i na Facebooku.

3. Malware

Malware, nebo škodlivý software, může být nainstalován na počítač nebo mobilní zařízení různými způsoby, například prostřednictvím infikovaných e-mailových příloh nebo stažených souborů z nelegitimních webových stránek. Tento software může zaznamenávat stisknuté klávesy (keyloggery) a odesílat přihlašovací údaje hackerovi.

4. Sociální inženýrství

Sociální inženýrství je technika, při které hackeři manipulují s lidmi tak, aby jim dobrovolně poskytli své přihlašovací údaje. Může to zahrnovat předstírání, že jsou zaměstnanci Facebooku nebo přátelé oběti, kteří potřebují pomoc. Tímto způsobem mohou získat dostatečné množství informací k přihlášení na účet.

K oblíbeným trikům patří např. rozesílání upozornění, že váš účet porušuje komunitní pravidla Facebooku a bude zablokován či smazán, pokud nekliknete na konkrétní odkaz a nezažádáte o obnovení. Facebook je doslova zamořen tímto typem spamu, který dokáže uživatele vyděsit a přimět k ukvapené reakci.

5. Zranitelnosti v aplikacích a webových stránkách

Hackeři mohou také využívat bezpečnostní zranitelnosti ve třetích stranách, které jsou propojeny s Facebookem. To může zahrnovat aplikace, které uživatelé používají k přihlášení pomocí Facebooku. Pokud je taková aplikace kompromitována, hackeři mohou získat přístup k účtu uživatele.

Jak se bránit proti ztrátě účtu na

Facebooku

1. **Používejte silná a jedinečná hesla**: Každý účet by měl mít své vlastní heslo, které je složené z kombinace písmen, čísel a speciálních znaků.
2. **Aktivujte dvoufázové ověření (2FA)**: Tento bezpečnostní prvek vyžaduje kromě hesla také ověření pomocí telefonu nebo aplikace pro autentizaci.
3. **Buďte obezřetní vůči phishingovým útokům**: Nikdy neklikejte na podezřelé odkazy a vždy ověřte, zda jste na skutečné stránce Facebooku.
4. **Aktualizujte software a aplikace**: Ujistěte se, že váš operační systém, prohlížeč a aplikace jsou aktuální, což snižuje riziko využití známých zranitelností.
5. **Vyhněte se podezřelým e-mailům a zprávám**: Pokud něco vypadá příliš dobře na to, aby to byla pravda, pravděpodobně to tak je. Neposkytujte své přihlašovací údaje nikomu.

Odkazy pro hlášení napadených účtů na Facebooku

Pokud máte podezření, že váš účet byl napaden, můžete použít následující odkazy k nahlášení problému a obnovení vašeho účtu:

https://www.facebook.com/hacked
https://www.facebook.com/login/identify
https://www.facebook.com/help/285695718429403/
https://www.facebook.com/help/securitycheckup
https://www.facebook.com/help/105487009541643

Pro E-Bezpečí
Kamil Kopecký
Univerzita Palackého