Přes systém „přátel“ na facebooku můžete přijít o peníze

Kriminalisté z odboru analytiky Krajského ředitelství policie kraje Vysočina prověřují od začátku letošního roku již čtyřicet případů podvodného jednání při získání a poté zneužití osobních údajů pomocí sociální sítě facebook. Všechny zadokumentované případy prověřují pro podezření se spáchání trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací. V případě zadržení pachatele a prokázání viny by za tento skutek hrozil trest odnětí svobody až na tři roky.

Ve všech prověřovaných případech jednal pachatel s úmyslem a cílem obohatit se, neboť po získání potřebných osobních údajů přišel poškozený o finanční prostředky, které pachatel získal prostřednictvím elektronické platby uskutečněné přes mobilní telefon. Většinou se jednalo v jednotlivých případech vždy o částku ve výši kolem 1 400 korun.

„Celé podvodné jednání pachatele většinou začíná tím, že se na facebookovém profilu od některého z přátel, tedy od osoby, kterou majitel účtu na sociální síti zná a nemá tedy důvod být nedůvěřivý, objeví vzkaz se žádostí o zpřístupnění osobních údajů, včetně mobilního telefonního čísla. Důvody pro tuto žádost bývají velice různorodé, ale vždy poměrně věrohodné,“ upozorňuje kpt. Bc. Václav Hess, vrchní komisař z oddělení informační kriminality Krajského ředitelství policie kraje Vysočina.

Poté probíhá další komunikace na facebooku, kterou ale nevede nikdo ze skutečných „přátel“, ale kterou vede pachatel s jasným cílem tyto údaje získat. Když se dostane až k číslu mobilního telefonu, zneužije tento telefon k provedení podvodné elektronické platby. Pro její uskutečnění ale znovu potřebuje spolupráci majitele mobilního telefonu, který musí platbu SMS zprávou sám potvrdit. I tato komunikace probíhá nejprve přes facebook, kdy pachatel se snaží pod časovým tlakem donutit poškozeného k rychlému jednání, což má za následek, že si majitel mobilního telefonu vůbec nepřečte obsah SMS zprávy, ve které je jasně a zřetelně uvedeno, že příslušná platba proběhne. Až ale tuto zprávu potvrdí, následně z další SMS zprávy zjistí, že mu byla z jeho paušálního účtu odečtena neoprávněně finanční částka, kterou už ale podvodně získal

pachatel.

Kriminalisté tedy znovu upozorňují majitele účtů na sociálních sítích, aby nezveřejňovali a nezpřístupňovali svoje osobní údaje, hesla a mobilní telefonní čísla, a to ani na žádosti, které se mohou na první pohled tvářit jako věrohodné. Často se stává, že o tyto osobní údaje je majitel také požádán v odkazech na různé výhry například elektronických přístrojů. V praxi se uživateli počítače objeví na monitoru okno s informací, že uživatel byl vylosován jako výherce nějaké hodnotné ceny. Podmínkou bývá zodpovězení jednoduché anketní otázky s tím, že uživatel se má na výherní stránku přihlásit přes svůj facebookový profil. Zadané přihlašovací údaje jsou automaticky odeslány pachateli, který je následně může zneužít. Po přihlášení k napadenému účtu pachatel pošle přátelům majitele facebookového profilu, které najde na jeho účtu, zprávu s informací, že ztratil jejich telefonní kontakty. Ve zprávě je požádá o jejich zaslání. Po získání telefonických kontaktů pak již sleduje aktivitu přihlášených přátel na facebooku.

„Pokud je někdo z nich on-line a pachatel zná jeho telefonní číslo, pak zadá na internetu platební příkaz pomocí m-platby. Toto je služba, která umožňuje provádět platby na internetu pomocí mobilních telefonů, kdy zaplacená částka za zboží nebo služby se objeví ve vyúčtování za poskytnuté telefonické služby. Jako telefonní číslo, ze kterého má platba proběhnout, uvede telefonní kontakt získaný od právě aktivního přítele na facebooku," popisuje postupy pachatele mjr. Mgr. Martin Vaněček, vedoucí odboru analytiky Krajského ředitelství policie kraje Vysočina.

Majiteli telefonu poté přijde SMS zpráva o m-platbě. V tuto chvíli s ním již pachatel komunikuje pomocí facebooku a v časové tísni pod různými smyšlenými legendami se z něj snaží vylákat potvrzující kód platby, který je součástí SMS zprávy. Pachatel například uvádí, že zkouší nějakou novou počítačovou hru a do tří minut musí napsat kód, který si nechal poslat v SMS zprávě na jeho telefon, neboť jeho vlastní telefon je rozbitý a podobně. V okamžiku, kdy pachatel získá potřebný kód, přijde již poškozenému pouze SMS zpráva, že platba proběhla v pořádku a peníze byly odečteny z jeho účtu za telefon.

V rámci předcházení této trestné činnosti musí uživatelé facebooku a jiných sociálních sítí dodržovat několik základních bezpečnostních zásad:

· V žádném případě nepište své uživatelské jméno a heslo někam jinam než při přihlášení na svůj facebookový profil. Totéž platí i pro přihlašování na ostatní sociální sítě.

· Nikomu neposkytujte svoje osobní údaje. Na svém facebookovém profilu těchto osobních informací zveřejňujte co nejméně. Jsou pak velmi snadno zneužitelné. V tomto případě se to týká i telefonních čísel.

· Mějte na paměti, že v prostředí sociálních sítí netušíte, zda ten, s kým komunikujete, je skutečně tím, za koho se právě vydává.

· Vždy mějte na zřeteli, že osoba, která s vámi komunikuje pomocí internetu, se může za vašeho přítele pouze vydávat.

· Pozorně si přečtěte každou SMS zprávu, která vám přijde a týká se plateb přes mobilní telefon. Jakékoliv autorizační kódy k platbám nesdělujte žádné třetí osobě.

Dana Čírtková