Informace Policie ČR k problematice podvodného jednání v kyberprostoru

V poslední době se v České republice stále více šíří podvodné jednání, které je realizováno v kyberprostoru a které může mít mnoho podob. Jde zejména např. o **spoofing** (podvodníci maskují pravé telefonní číslo, e-mail, IP adresu či věrohodně vypadající webovou stránku), **phishing** (podvodné zprávy a e-maily) a **vishing** (podvodné volání „bankéřů“), což jsou metody sociálního inženýrství užívaná útočníky v rámci kybernetické kriminality. Tato činnost spočívá v oklamání konkrétní oběti pomocí e-mailu, telefonního hovoru, kdy cílem pachatele je vylákání různých informací, které mohou být následně zneužity (informace k osobní identitě, k platební kartě, k bankovnímu účtu aj.). V těchto případech pachatelé dokáží napodobit prakticky jakékoliv e-mailovou adresu či telefonní číslo a mohou se tak vydávat například za oficiální pracovníky různých finančních institucí (např. za pracovníky klientské linky té které banky). Např. pod legendou napadení účtu a nutnosti rychlého převodu peněz na jiný zabezpečený účet z důvěřivé oběti telefonicky vylákají informace o platební kartě a znění příchozí potvrzovací SMS zprávy. Oběť až následně zjistí, že byla podvedena a okradena, protože odsouhlasila převod finančních prostředků z vlastního bankovního účtu. K podvodnému jednání mohou být zneužity i některé osobní informace oběti, které mohly v minulosti uniknout např. z databáze e-shopu, která byla pachateli získána jinými hackerskými útoky. Dále se může jednat např. o různé falešné odkazy na založení bitcoin účtu, převod peněz na bitcoin, podvodné vyděračské e-maily, podvodné e-shopy, aukce apod. Podvodná jednání jsou stále sofistikovanější a pro laickou veřejnost obtížně odhalitelná.