

## Prodávala dětský koberec, nakonec sama přišla o peníze

MĚLNÍK - Policisté řeší případ internetového podvodu a zjišťuje, která konkrétní osoba ho spáchala.

Prostřednictvím Pol Pointu - asistované digitální služby, oznámila mladá žena podvodné jednání, v důsledku kterého přišla o bezmála šedesát tisíc korun.

Jednalo se o naprosto běžnou záležitost, kdy žena prostřednictvím internetového portálu prodávala za tisíc korun dětský koberec. Ještě týž den přišla na její Whatsapp odpověď od neznámé ženy, že má o tento koberec zájem. Nicméně místo, aby za koberec získala požadovaných tisíc korun, sama přišla o několiknásobně vyšší částku. Z jejího účtu, díky předem promyšlenému jednání a splnění instrukcí "kupující" osoby, jí zmizelo bezmála šedesát tisíc korun.

Poté, co neznámá žena (alespoň se pod ženským jménem při whatsappové komunikaci vydávala) projevila o dětský koberec zájem, sama začala instruovat autorku inzerátu ke krokům, které má udělat. Obdržela odkaz na údajného dopravce z DPD s tím, že musí vyplnit veškeré údaje ke své osobě, účtu, ale i platební kartě. Tedy číslo karty, její platnost, číselný kód ze zadní strany karty. Pak už jen obdržela ověřovací PIN, který zadala. Současně jí přes whatsappovou komunikaci bylo doporučeno, aby v žádném případě stránky neopouštěla. Takto byla požádána o připojení a stejný postup ještě jednou.

Žena tak po splnění všech pokynů čekala, kdy jí bude účet vložena tisícikoruna za prodaný dětský koberec. Místo toho jí ale neznámý podvodník "odčerpal" z účtu přes třicet tisíc korun a na bankovním účtu jí zbylo pouhých 22 korun. Bohužel stejným způsobem jí podvodník připravil o peníze z kreditní karty, celkově tak žena přišla o bezmála šedesát tisíc korun.

Žena pochopila, že se jednalo o podvod a okamžitě kontaktovala bankovní ústav, u kterého má své účty. Tam jí jenom potvrdili, že díky sděleným údajům se mohl neznámý hacker pohybovat v prostředí jejích účtů a o peníze tak přišla.

Případ, který žena oznámila z domova, s videokonferenčním připojením, kdy žena nemusela nic podepisovat, neboť o jejím podání vysvětlení byla pořízena videonahrávka, budou řešit policisté z Kralup nad Vltavou. Ti již v dané věci zahájili úkony trestního řízení pro trestný čin podvodu podle § 209, odst. 1 a pro podezření z neoprávněného opatření, padělání a pozměňování platebního prostředku.

### INTERNETOVÁ KRIMINALITA NA VZESTUPU

Toto je jeden z typických případů internetové kriminality (tzv. IT), kterými se v posledních měsících zabývají policisté nejen ve středních Čechách, ale i v celé České republice. IT kriminalita je v současné době na vzestupu /viz tabulka a graf/. V době "covidu", tedy v roce 2020, řešila středočeská policie 1 903 případů v internetovém prostředí, následující rok - 2021 - stoupl počet těchto případů na 2 566 za celý rok (tedy o 663 případů více). Za letošní právě uplynulé čtyři měsíce letošního roku je počet oznámených případů 1 064 (průměrně tak měsíčně řeší policisté přes 260 případů, tedy denně přibývá cca 9 oznámených případů).

### NEJČASTĚJŠÍ PŘÍPADY V IT PROSTŘEDÍ

Policisté se nejčastěji zabývají ve virtuálním prostředí různým druhům podvodného jednání. Podvedení jsou většinou lidé, kteří prostřednictvím inzerátu na portálech k tomu určeným nabízeli k prodeji různé věci (pračky, ledničky, věci po dětech, boty, lyže, mobilní telefony). Za ně většinou požadovali malé částky, nicméně většinou sami přišli o téměř veškeré peníze na účtu, tedy někdy až statisícové částky. Celkově pak kriminalisté evidují - od ledna do dubna letošního roku - v souvislosti s veškerou kybernetickou kriminalitou škodu přesahující 176 miliónů korun (v této částce jsou zahrnuty jak skutky kvalifikované jako trestné činy, tak i přestupkové jednání).

## JAK SE BRÁNIT INTERNETOVÝM PODVODNÍKŮM

- V žádném případě nesdělujte k Vaší osobě žádné citlivé údaje ani bezpečnostní údaje z vaší platební karty, nebo přístupové údaje k online bankovníctví;
- Nikdy nikomu nesdělujte, a ani nepřeposílejte, bezpečnostní autorizační kód, který Vám přišel formou SMS zprávy;
- Myslete na to, že útočník dokáže napodobit jakékoliv telefonní číslo, odesílatele SMS zprávy, ale třeba i e-mailovou adresu;
- Nikdy nikomu podezřelému neumožňujte vzdálený přístup do Vašeho počítače;
- Sledujte a pečlivě čtěte informace od Vaší banky v internetovém bankovníctví;
- Při každém vstupu do internetového bankovníctví kontrolujte, zda odpovídá doména přihlašovací stránky. Toto platí vždy, když někam zadáváte své osobní nebo přihlašovací údaje;
- Aktualizovat software, antivirový program, firewall;
- Během, nebo po takovémto podezřelém hovoru, si zaznamenejte údaje, které Vám útočník sdělil (*jména, e-mailové adresy, čísla účtů, odkazy na webové stránky, apod.*)

mjr. Mgr. Vlasta Suchánková  
oddělení tisku a prevence  
KŘP Středočeského kraje

### VÝVOJ IT KRIMINALITY V RÁMCI STŘEDOČESKÉHO KRAJE

Vývoj nápadu IT KRPS		2020	2021	2022
	leden	172	217	342
	únor	143	176	256
	březen	138	212	275
	duben	155	217	191
	květen	150	209	
	červen	173	181	
	červenec	131	165	
	srpen	123	179	
	září	149	199	
	říjen	164	217	
	listopad	203	301	
	prosinec	202	293	
		1903	2566	1064
		2020	2021	2022
1 až 4	celkem	608	822	1064

## VÝVOJ IT KRIMINALITY V RÁMCI STŘEDOČESKÉHO KRAJE

