Zpravodajství

Policie České republiky – KŘP Královéhradeckého kraje

Ahoj Boženo, pošli mi své telefonní číslo…

KRAJ – Převlečení za přátele číhají na sociální síti.

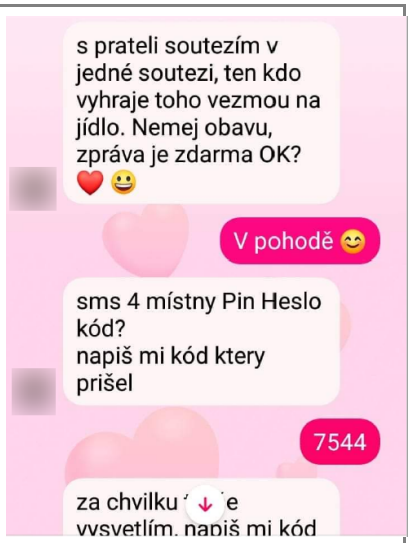
Když si Jiřina zřídila účet na jedné z nejpoužívanějších sociálních sítí a využívala pro komunikaci se všemi navázanými přáteli na její profil i přidruženou komunikační platformu, netušila, že do jejího virtuálního soukromí pronikne pachatel a jejím jménem začne oslovovat její přátele.

Vcelku nevinně a nenápadně se tak začíná odvíjet ne příliš příjemný příběh, na jehož konci je řetězově se množící a v daném okamžiku v čase de facto nezastavitelná sériová trestná činnost prováděná pachatelem ve virtuálním světě, a to velice sofistikovaným způsobem.

Přestože kriminalisté se každému takovému zjištěnému a následně nahlášenému případu intenzivně věnují, je velice obtížné tuto trestnou činnost objasnit a hlavně v čase páchání varováním zastavit. Pachatelé umějí dokonale „zamést“ téměř všechny stopy a opět těží z přílišné důvěřivosti svých obětí. Jednání pachatelů přesahuje hranice krajů a dost možná i kontinentů. Popíšeme Vám jeden takový nevinný příběh Jiřiny a Boženy, dvou důvěřivých kamarádek na sociálních sítích.

A jak to celé funguje?

Jednoduše. Jiřina profil běžně používá, komentuje příspěvky, těší se nad příspěvky svých přátel a samozřejmě používá i přidruženou komunikační platformu. Pachatel neoprávněně do jejího účtu vniká a začíná jejím jménem kontaktovat i Jiřiny přátele.

<table>
<tr>
<td>
</td>
<td>
</td>
</tr>
<tr>
<td>Falešná Jiřina žádá Boženu o telefonní číslo.</td>
<td>Božena ochotně posílá falešné Jiřině i PIN kód</td>
</tr>
</table>

Ahoj Boženo, pošli mi prosím tvé telefonní číslo…

Od Jiřininých přátel pachatel pod smyšlenou legendou (soutěž o večeři, příp. soutěž o vyšší finanční částku v řádech desetitisíců Kč), vyláká jejich telefonní číslo. Ano, jakkoliv se to zdá nereálné, Božena pachateli převlečenému za Jiřinu pošle své telefonní číslo, přestože ho s největší pravděpodobností opravdová Jiřina patrně už má, protože si kamarádky volají.

<table>
<tr>
<td></td>
<td></td>
</tr>
</table>



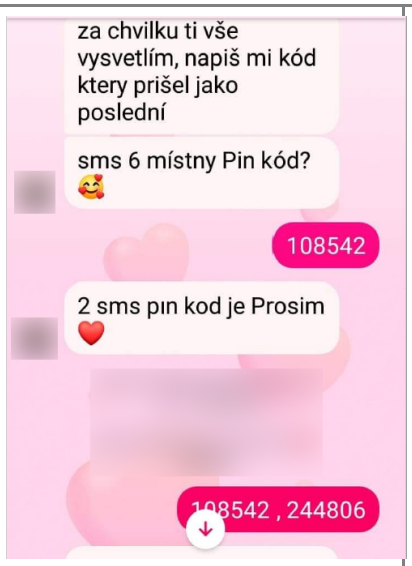
Pachatel používá smyšlené legendy.



Důvěřivá oběť pachateli posílá vše podle zadání.

Božena posílá své telefonní číslo falešné Jiřině...

Boženě to nepřijde divné a číslo pachateli převlečenému za Jiřinu ochotně posílá. Falešná Jiřina pak požádá sociální síť o změnu hesla Boženy k jejímu účtu a následně přichází v mezičase PIN kód Boženě na mobil a pachatel převlečený za Jiřinu od Boženy vyláká cestou komunikace v aplikaci i tento PIN kód a v tu chvíli se Boženy profilu zmocňuje pachatel převlečený za Jiřinu. První krok, který pachatel ke své trestné činnosti potřebuje, je za ním.



Pachatel naléhá, oběť plní jeho přání.

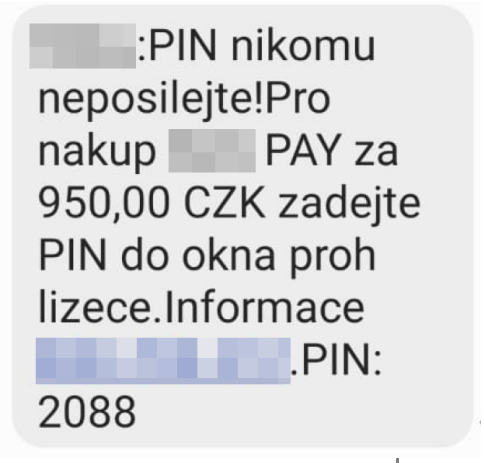


Pachatel naléhá a oběť plní jeho přání.

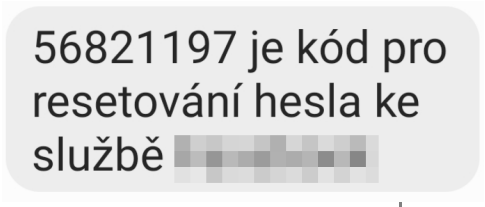
Svůj účet už Božena nevědomky předala pachateli

Pachatel pokračuje a prostřednictvím telefonního čísla Boženy provede například objednávky herních kódů v různých částkách na různých internetových portálech cestou „M-platby“, což obnáší opět zaslání PIN kódů od majitelů telefonních čísel, tedy přítelkyně Boženy a dalších přátel, které jsou zapotřebí k potvrzení „M-platby“ za nákup těchto herních kódů.

Hesla k dokončení plateb cestou "M-platby" ochotně přítelé zasílají, přestože je mnohdy operátoři varují například takto: *„Dobry den, nenechte nikoho zneuzit sve heslo, nikomu ho nesdelujte. K dokončeni m-platby z Vaseho kreditu/faktury u Vaseho cisla +420xxx na castku xxx Kc u xxx je heslo xxx. Vas operátor“*.



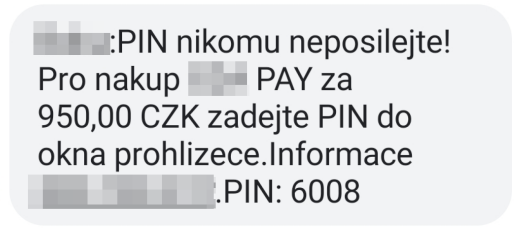
Vzor zaslané SMS zprávy od operátora.



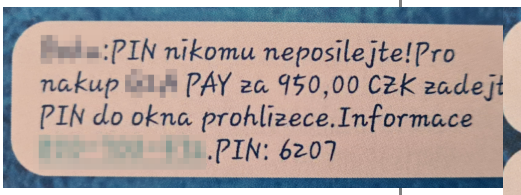
Vzor zaslané SMS od poskytovatele sociální sítě.



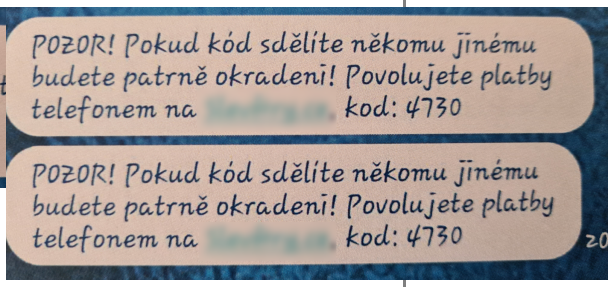
Příchozí SMS zprávy od operátora.



Příchozí SMS od operátora.



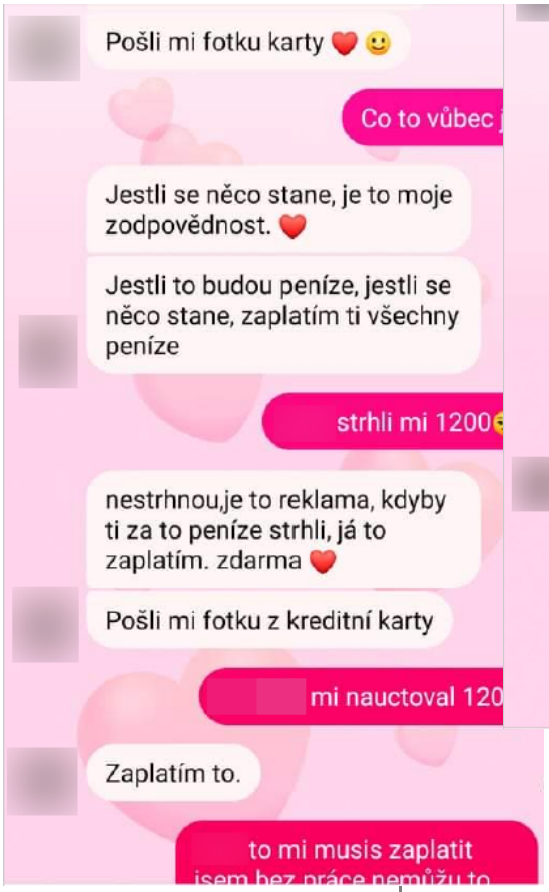
Příchozí SMS od operátora.



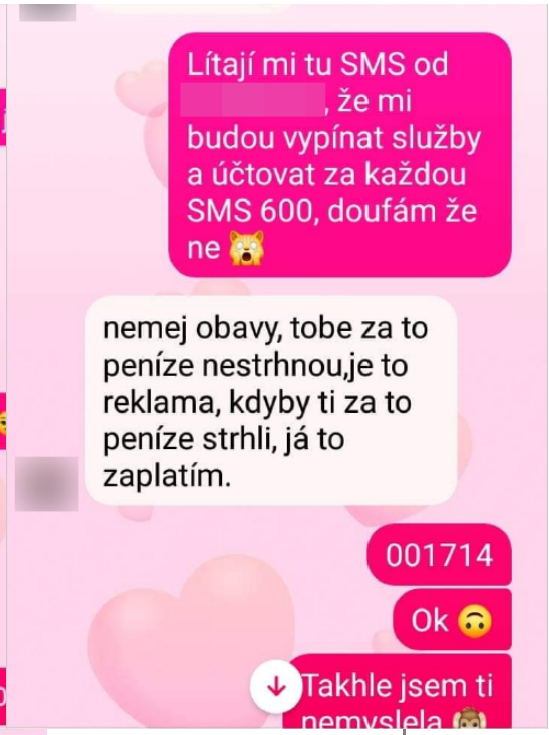
Příchozí SMS od operátora.

Z ničeho nic několikanásobný účet od mobilního operátora

Boženě a všem přátelům, kteří falešné Jiřině uvedené údaje zaslali, se navýší o danou částku paušální vyúčtování od jejich operátora mobilních služeb.
V takovém případě už není cesty zpět. Božena a další přátele Jiřiny přicházejí o virtuální identitu v podobě jakési zajištěné „intimity“ či „soukromí“ svého účtu na sociální síti a nenávratně i o své peníze.



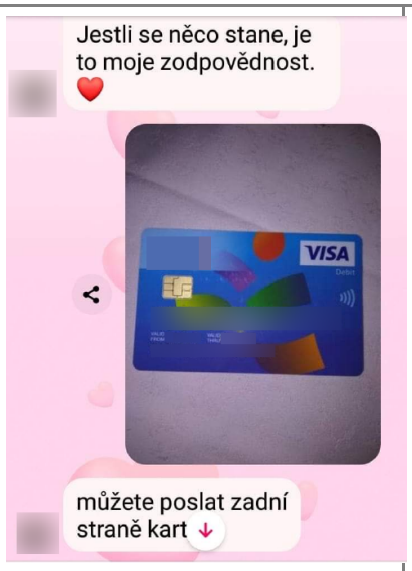
Oběť už má jisté pochybnosti.



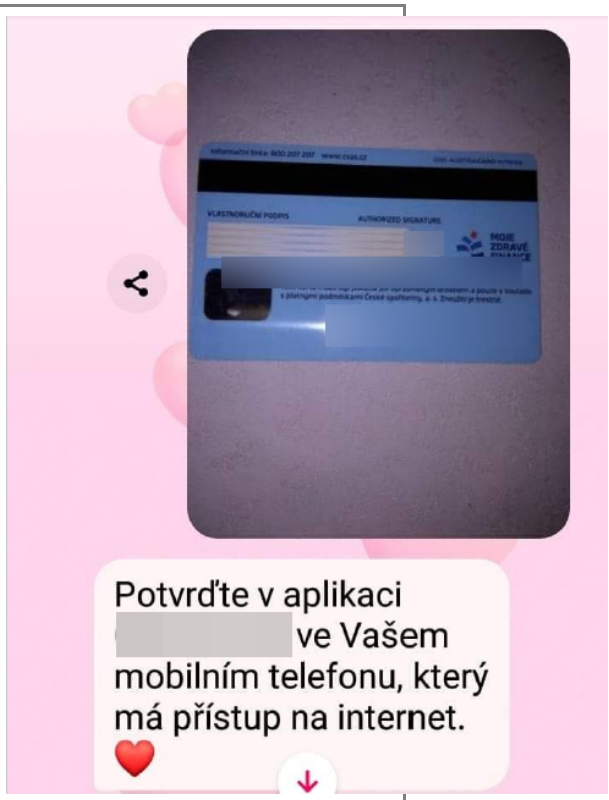
Operátor komunikuje s obětí.

Falešná Jiřina však pokračuje v drzosti

Oslovuje i osoby z rodiny Boženy (manžel, děti, sestra, bratr) a žádá fotografii platební karty příp. i zaslání přihlašovacích údajů k internetovému bankovnictví. Pomocí platební karty pak odcizí finanční prostředky z účtu. Bohužel falešná Jiřina občas získá tyto údaje i od osob mimo rodinu.



Oběť ochotně posílá fotografii platební karty.



Oběť na výzvu pachatele pošle i číselný kód ze zadní strany platební karty.

Výsledek?

Pachatel se ve výše uvedeném příběhu, v němž jsme pozměnili jména poškozených, dopustil několika trestných činů, přičemž v případě uznání viny mu může soud uložit trest až do výše osmi let odnětí svobody.

Ale to už je pro oběti pozdě…. Jak a kdo to může zastavit?

"Vzhledem k tomu, že Policie ČR se o těchto případech nemá šanci dozvědět online v čase, je pouze na veřejnosti, aby se nestala oběťmi podvodníků a zareagovala obezřetně a správně včas. Trestná činnost ve virtuálním prostředí je ex post obtížněji objasnitelná. Opět jedinou šancí je obezřetné chování všech, kteří by se mohli stát obětí takových pachatelů a šíření tohoto způsobu páchání trestné činnosti. Na konci celého poměrně krátkého procesu je nejen ztráta soukromí a případně celého účtu, ale pachatelé by mohli touto cestou obecně své oběti například vydírat, vyhrožovat jim a samozřejmě odčerpávat nezanedbatelné finanční částky," říká kriminalista Ladislav, který se problematice dlouhodobě na našem Krajském ředitelství policie Královéhradeckého kraje intenzivně věnuje.

Na co si dát tedy pozor?

- Na druhé straně sociální sítě nemusí být v danou chvíli online vůbec Váš přítel, může to být pachatel, který se naboural do účtu vašeho kamaráda či kamarádky, přičemž oni o tom vůbec nemusejí vědět – při pochybnostech si s přáteli, kteří Vám podobné zprávy posílají, raději zatelefonujte,
- neposílejte žádné údaje bez předchozích telefonického ověření ani svým přátelům, s nimiž jste běžně v kontaktu,
- neklikejte raději ani na žádné linky, jež Vám od přátel mohou přijít cestou komunikačních platforem, mohou to být v lepším případě reklamní triky, ale v horším Vás mohou tyto adresy cíleně přesměrovat na vzdálené servery, což může být začátek dalších nepříjemností,
- zablokujte si „M-platby“ u operátora telefonních služeb,
- nikomu nesdělujte žádné PIN kódy,
- nezasílejte ofocené platební karty a přihlašovací údaje k internetovému bankovnictví,
- a informujte své přátele o tom, co se může stát i jim, protože ani Váš profil a účet nemusí být vůbec před podvodným jednáním uchráněn…

A jak konkrétně vypadá první a zcela nevinně vypadající zpráva, která Vám může od přítele přijít?



Takhle nevinně začíná konverzace...

plk. PhDr. Ondřej Moravčík
mjr. Ing. Magdaléna Vlčková, MBA
4.4.2021

© 2021 Policie ČR, všechna práva vyhrazena