EUCPN
EUROPEAN CRIME PREVENTION NETWORK

Doporučující dokument

KLIKNĚTE ZDE, PROSTĚ MI VĚŘTE!

Jak se dělají online podvody a jak jim předcházet

EMPACT

Internetové podvody jsou v Evropě stále významným problémem a v dohledné budoucnosti jím zůstanou.

Tento článek předkládá některé široce použitelné koncepty a nástroje pro navrhování iniciativ v oblasti prevence kriminality.

Citace
EUCPN (2022). Klikněte zde, prostě mi věřte!-Jak fungují online podvody a jak jim předcházet. Brusel: EUCPN.

Autoři/redaktoři
Thomas Van den Berghe, referent pro praxi a politiku, sekretariát EUCPN.

Součást projektu "Sekretariát EUCPN", únor 2023, Brusel
S finanční podporou Fondu pro vnitřní bezpečnost Evropské unie - policie

Obsah

Dokument vznikl v rámci spolupráce EUCPN v rámci Evropské multidisciplinární platformy proti kriminálním hrozbám (EMPACT) z roku 2022. Tento krátký dokument zkoumá obecné mechanismy, díky nimž fungují schémata online podvodů, předkládá pokyny pro iniciativy v oblasti prevence.
a uvádí některé příklady osvědčených postupů. Jejím cílem je poskytnout solidní úvod a porozumění schématům online podvodů, ale nenabízí komplexní pokyny pro preventivní reakce na všechny online podvody.

Rádi bychom vyjádřili zvláštní poděkování těm, kteří se podíleli na tvorbě tohoto dokumentu, mimo jiné Švédskému národnímu centru pro podvody.

Společenské změny, jako je krize COVID-19 a přechod k bezhotovostní společnosti, vytvářejí nové příležitosti i pro pachatele trestné činnosti. aby se dostalo k více obětem.

Podvádění druhých není nový fenomén, zdaleka ne. Podvody existují tak dlouho, jak dlouho existuje soukromé vlastnictví a schopnost komunikace.[1] Rozsah těchto podvodů se však výrazně zvýšil. Široká popularita digitálních komunikačních technologií s sebou přinesla novou generaci podvodných schémat. Tyto "kyberneticky podporované" podvody se mohou šířit nepředstavitelnou rychlostí a zaměřit se na větší počet (potenciálních) obětí, přičemž zločinci mohou působit v anonymitě.[2]

Podvodníci využívají nejrůznější mody operandi (MO).[3] Používají různé techniky, z nichž každá má svá specifika: podvody s milostnými vztahy v online seznamovacích aplikacích, phishingové e-maily s podvodnými odkazy, investiční podvody s nejnovějšími kryptoměnami a mnoho dalších. Všechny tyto různé druhy podvodů však mají společný mechanismus: sociální inženýrství. Jedná se o techniku, která manipuluje s lidským chováním s cílem přimět lidi, aby vyhověli danému požadavku nebo poskytli důvěrné informace, které by jinak neudělali.[4]

Společenské změny, jako je krize COVID-19 a přechod na bezhotovostní společnost, také vytvářejí nové příležitosti pro pachatele, jak se dostat k většímu počtu obětí.
Podvodníci jsou flexibilní a ochotně přizpůsobují svůj způsob práce, aby zvýšili své šance na úspěch, jak to dělali i v minulosti. S tím, jak si občané stále více zvykají využívat on-line služby, jako je internetové bankovnictví a internetové obchody, roste i okruh potenciálních obětí.[5] Tento trend je již zřejmý, vzhledem k tomu, že
že online podvody jsou rok od roku rozšířenější.[6] Pravděpodobnost hromadného odchodu lidí z jejich života na obrazovce se zdá být poměrně malá, a proto bude nutné se připravit na boj proti typům online podvodů.

Pod pokličkou podvodných schémat

Lidský faktor

Kybernetičtí zločinci používají k podvádění svých obětí nejrůznější techniky, ale obecně je lze považovat za součást určitého spektra. Na jednom konci spektra jsou přístupy založené na technologiích. Ty využívají IT nástrojů, jako jsou key loggery, spyware, jiné typy malwaru a nástroje pro získávání citlivých informací (např. hesel, firemních záznamů nebo osobních údajů). Na druhém konci spektra se však zločinci zaměřují na lidské jednání a snaží se ho ovlivnit. Patří sem nejrůznější podvodná schémata, jako je phishing, investiční podvody, vydávání se za přátele/autority a další. Tato manipulace se běžně označuje jako **sociální** inženýrství[7].

Tento článek se zaměřuje na tento lidský prvek. Zaprvé proto, že přístup založený na technologiích má obecně také tendenci využívat lidské slabiny k průniku do jejich IT infrastruktury (např. připojením podvodných příloh k e-mailu s žádostí, aby je příjemce otevřel, a uvolněním škodlivého kódu, když tak učiní). Za druhé, zaměření na hackerské přístupy zahrnující lidský prvek má širší uplatnění vzhledem k jejich širokému využití.

Lidský faktor je slabinou, která otevírá dveře k online podvodům.[8] Odhaduje se, že se podílí na více než 80 % případů narušení bezpečnosti dat po celém světě a je považován za klíčový faktor, který se na mnoha z nich podílí.[9] Ačkoli je třeba poznamenat, že "lidský faktor" zahrnuje mnohem více než jen sociální inženýrství, slabiny, jako jsou špatná hesla nebo ztráta důležitého hardwaru, nejsou výsledkem sociálního inženýrství.

Sociální inženýrství funguje, protože (ne)využívá způsob, jakým lidé zpracovávají informace. Obvykle máme dva způsoby zpracování informací. První z nich je "centrální cesta", vyžaduje logiku a myšlení, které analyzuje příchozí informace. Je skeptičtější a žádá o doplňující informace, které by upřesnily a hledaly případné nesrovnalosti. Druhá, "periferní cesta", se mnohem více zaměřuje na samotný zdroj informací a individuální/osobní důvody, proč být přesvědčen. Pokud se nám zdroj líbí, popř. kontext, ve kterém je prezentován, je věrohodný, informace z něj vycházející budou také považovány za dobré.

a nebudeme se jimi zabývat příliš podrobně.[10] Podvodníci své oběti tlačí na tuto druhou cestu tím, že zneužívají lidského myšlení. Tím na oběti vyvíjejí nátlak a dostávají je do situace, kdy je mnohem těžší reagovat pomocí centrální cesty a použít kritické myšlení na danou situaci.[11]

Vlivné osoby Maleficent

Abyste pochopili, proč podvody fungují, musíte se také podívat na příběhy, které přinášejí svým obětem. Teprve pak můžete úspěšně pokračovat v jejich potírání. Na toto téma bylo provedeno poměrně velké množství výzkumů, které lze shrnout do seznamu pěti klíčových prvků podvodů.[12]

- **Autorita**: Podvodníci často vystupují z pozice autority. Ta může souviset s profesí (např. policisté) nebo znalostmi (např. investiční guruové). Lidé jsou během svého života podmíněni tím, že na postavy autority reagují spíše podřízeně.
- **Sociální důkaz**: Lidé jsou rádi součástí skupiny, takže mají tendenci následovat to, co dělají ostatní. Pokud něco vypadá, že to dělá mnoho lidí, instinktivně předpokládáme, že to musí být bezpečné, i když tomu tak ve skutečnosti není.
- **Oblíbenost, podobnost a klamání**: Lidé mají rádi lidi, kteří jsou jim podobní nebo kterými by chtěli být. Podvodníci předstírají, že jsou úspěšní investoři, krásní lékaři v zahraničí, kteří hledají pomoc/lásku, nebo prostě někdo, kdo má stejný vzhled/postoje jako my. Lidé podvědomě chtějí, aby se jim daná osoba líbila.
- **Závazek, vzájemnost a důslednost**: Lidé chtějí být vnímáni jako konzistentní a důvěryhodní. Podvodníci toho zneužívají tím, že vám poskytnou velmi malou laskavost a na oplátku požadují něco (ze strany oběti obtížnějšího). Oběť je tak nucena vyhovět, protože "něco za něco". Cílem podvodníků je také přimět vás k souhlasu, třeba s něčím velmi jednoduchým, než přejdou k podstatnějším požadavkům. Pokud chce oběť zůstat vnímána jako vstřícná, byť i podvědomě, musíte i nadále souhlasit.

- **Rozptýlení**: Lidé se rádi soustředí na jednu věc: něco, co mohou vyhrát, riziko, kterému se mohou vyhnout, nebo časově omezenou nabídku. Ty odvádějí jejich pozornost od jakéhokoli
jiné signály, které by jinak mohli vnímat, a zvyšují emocionální stav lidí, což je nutí ignorovat nelogické chyby. Vlivnými motivátory jsou zejména strach a chamtivost.

Ne všechny prvky jsou přítomny ve všech podvodných schématech. Výše uvedené prvky jsou pouze složky, které mohou být v některých schématech účinné, ale v jiných ne. Většina podvodů se omezuje na jeden nebo dva z výše uvedených principů. Zdaleka nejpoužívanější je "autorita" následovaná "sympatiemi, podobností a podvodem "[13].

Taftování krok za krokem

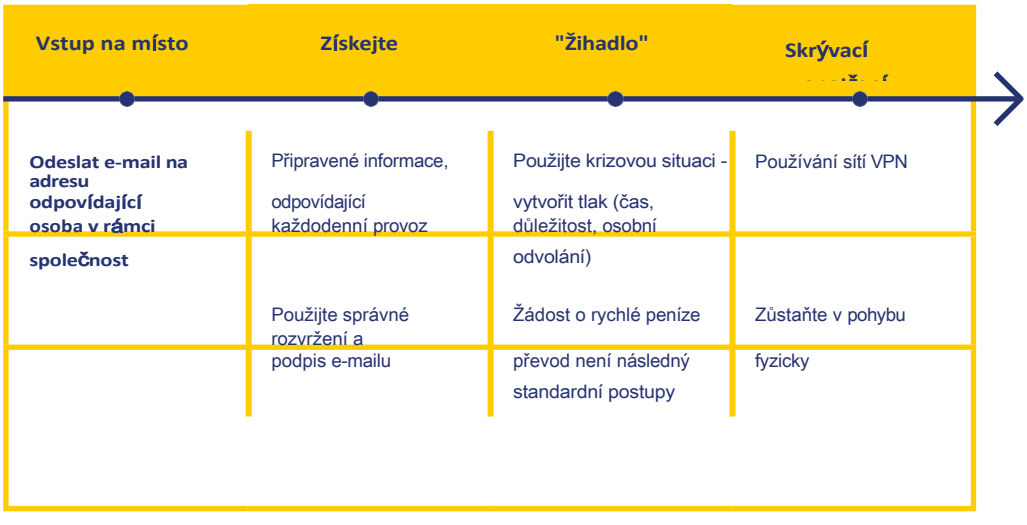
Nejen složky online podvodných schémat jsou si podobné. Navzdory podstatným rozdílům mezi mnoha MO v online podvodných schématech mají stále společné rysy.
proces, který je jejich jádrem. Tato společná cesta umožňuje využívat společné rámce pro všechny systémy online podvodů a preventivní iniciativy zaměřené na ně. Jedním z takových nástrojů je **Crime Scripting**, který organizuje informace o kroky, které pachatelé trestných činů činí při jejich provádění, a požadavky, které jsou k tomu nutné.[14]

Vytvoření kriminálního scénáře je dobrý způsob, jak analyzovat způsoby jednání používané v kriminálních scénářích. Umožňuje jasně uvést prostředky zločince, jeho prostředníky a ohniska jeho působení. Tyto informace vám umožní vytvořit přesnější a účinnější preventivní a rušivé akce. Pokud víte, jak podvodníci operují a
jaké informace potřebují, můžete snadněji připravit preventivní opatření, která se na ně zaměří. Ačkoli to může znít složitě a komplikovaně, ve skutečnosti tomu tak být nemusí.

Ano, kriminální scénáře mohou být založeny na hlubokých a důkladných vědeckých studiích. Velmi silný základ pro scénáře kriminality však mohou poskytnout i zkušenosti, a to tak, že se sejde skupina zkušených policistů, kteří diskutují o svém know-how týkajícím se konkrétního fenoménu kriminality.

Jak se tedy píše scénář kriminálního filmu? Nejdříve si rozdělíte proces páchání trestného činu na tři fáze: přípravnou fázi, fázi provedení a fázi, ve které se trestný čin stane.
fáze dokončení (která se zabývá opatřeními přijatými po spáchání trestného činu).
Pro každou fázi pak sestavíte časový plán/proces, který obsahuje všechny požadavky na provedení zločinu krok za krokem. Fáze přípravy a provedení se u různých typů podvodů značně liší, ale fáze dokončení je univerzálnější.

Zjednodušený příklad vizualizace přípravné fáze zločinného scénáře pro podvody typu BEC (Business E-mail Compromise) je následující:



Používejte falešná telefonní čísla
ber v případě kontroly
NEBO okamžitě uveďte že telefonní kontakt je není možné

Provoz ze zahraničí

Preventivní iniciativy

Stavební bloky

Lze navrhnout pět stavebních kamenů, které lze použít v úspěšných iniciativách prevence podvodů na internetu. I když tyto stavební prvky samy o sobě nestačí, lze je použít jako "model švýcarského sýra" a přidat nedokonalé vrstvy ochrany, které tvoří pevný celek.[15]

Cílem prvního bloku je **zvýšit úsilí, které** je třeba **vynaložit,** a ztížit pachatelům jejich podvody. V tomto případě je důležité rozlišovat mezi cílovými oběťmi a usnadňujícími oběťmi.
Usnadňující oběti jsou ti, kteří hostují informace a IT infrastrukturu (např. společnosti), které mohou být použity k podvodu na skutečných cílových obětech, na něž se zaměřují.
své finanční prostředky nebo z jiných důvodů. Zaměřením se na usnadnění obětí můžete zabránit tomu, aby se cílové oběti vůbec dostaly k vám. Pokud je například příliš obtížné proniknout do databází, nelze informace v nich obsažené využít k cílení na občany. Mnoho pachatelů také stále využívá starší nástroje, jako jsou telefonní seznamy. Na ty by se nemělo zapomínat, protože moderní řešení těchto starých problémů by mohla být obzvláště účinná. Preventivní techniky zahrnující kontroly přístupu, které ztěžují přístup k některým službám, by měly co nejvíce využívat také soukromé společnosti. Ty mohou sahat od (silných) hesel až po dvoufaktorovou autentizaci nebo za určitých okolností i prověřování pro účely, jako je získání přístupu k citlivým databázím.

Odborníci by také měli **zvýšit rizika spojená** s páchání podvodů, aby posílili odrazující účinek. Klíčový je zejména tok informací mezi veřejnými a soukromými subjekty. Sdílení poznatků o MO, preventivních opatřeních a prosazování práva vytváří společný pohled na problémy a společné způsoby jejich řešení a výrazně ztěžuje bezpečnou činnost pachatelů trestné činnosti.
Mnoho soukromých společností (např. ve finančním sektoru) již disponuje databázemi, které jsou zajímavé jako prostředek
monitorování a sledování situace. Technologie může být také nástrojem pro analýzu obrovského množství dostupných dat. Sledování situace s cílem identifikovat vysoce rizikové transakce (např. do zemí označených vlajkou nebo neregulérní nákupy) rovněž umožňuje proaktivní přístup. Tím lze také obejít stigma oběti podvodu a stále pomáhat uživatelům, protože nemusí vyvíjet iniciativu. Boj proti podvodům na internetu je obtížnější kvůli složitým postupům

hlášení, různým prioritám a

Snížení odměn by mělo být také předmětem preventivních iniciativ. "Povolání" podvodníka by nemělo být atraktivním prostředkem k získání stálého příjmu.

skutečnost, že v mnoha případech se na nich podílejí lidé z několika zemí. Proto může být obtížné zjistit, na koho se obrátit. Pro oběti by mělo být stanoveno a jasně sděleno jasné a snadno dostupné kontaktní místo, aby se zvýšila šance na dopadení podvodníků.

Snížení odměn by mělo být také předmětem preventivních iniciativ. "Povolání" podvodníka by nemělo být atraktivním prostředkem k získání stálého příjmu.
Při dopadení zločince se co nejdůkladněji zabaví jeho zisky a majetek, čímž se sníží jeho příjmy. Podobný účinek má i pronásledování jejich infrastruktury pro praní špinavých peněz (např. peněžních mul). Kontroly toku finančních prostředků na platformách pro online prodej by mohly mít silný dopad na zisky zločinců (např. služby, které drží peníze po určitou dobu, než je převedou prodejci).

Omezením provokací se snižuje pravděpodobnost, že se zločinci nechají inspirovat k páchání trestné činnosti. Ačkoli v případě online podvodů není mnoho možností, jak toho dosáhnout, určitý potenciál tu přece jen je. Tím, že pouze uvolnění omezených informací o přesných způsobech jednání podvodníků by bylo možné napodobitele zastavit ještě předtím, než začnou.

A konečně, preventivní iniciativy by měly **odstranit** i **výmluvy** pachatelů. Ti rádi tvrdí, že jejich oběti se ani nedozvědí, co se jim stalo. Informováním (potenciálních) obětí o tom, co se děje a jak se lze podvodům vyhnout, pachatelé využívají argument, aby přesvědčit sami sebe. Může mít podobu vyskakovacího okna při zadávání bankovní transakce na označený/vysoce rizikový účet, které oběť upozorní na riziko, nebo může mít podobu komunikačních kampaní zaměřených na rizikové skupiny, například na osoby, které se již dříve staly obětí podvodu.

Správné postupy

Podvody online jsou rozsáhlým problémem. Navrhování a realizace účinných iniciativ v oblasti prevence kriminality vyžaduje čas, výzkum a finanční prostředky. Naštěstí je již k dispozici několik příkladů, které můžete použít jako inspiraci nebo si je přizpůsobit podle svých potřeb.

Proaktivní narušování podvodů v oblasti kryptoinvestic ze strany Úřadu služby kriminální policie a vyšetřování je příkladem postupu, který zaujímá proaktivní přístup a jehož cílem je "zvýšit riziko" pro pachatele trestné činnosti. Jedná se o iniciativu zaměřenou na pachatele, která je konkrétně zaměřena na podezřelé bankovní účty a na narušování zisků z trestné činnosti. Když oběť nahlásí, že byla podvedena, škoda již byla způsobena a pachatelé již zahlazují stopy. Česká policie se vydává za potenciální oběti, které mají zájem investovat do kryptoměn, aby se sama obrátila na zločince. Při kontaktu s podvodníky je přiměje k odhalení bankovních účtů, které používají. Tyto informace pak předává národnímu orgánu pro boj proti praní špinavých peněz, který má pravomoc účty prošetřit. Kdykoli dojde k jakémukoli trestnému činu nebo podezřelému
se do odhalené činnosti zapojují vedle dalších policejních složek i samotné banky. Spolupráce s bankami je při kombinovaných akcích tohoto typu nezbytná. Byla navázána a udržována, protože všechny zúčastněné strany vnímají tento vztah jako oboustranně výhodný.

Podvody online jsou rozsáhlým problémem. Navrhování a provádění iniciativ v oblasti prevence kriminality vyžaduje čas, výzkum a finanční prostředky.

Projekt Sunbird je australská iniciativa, kterou lze považovat za zaměřenou na "zvýšení úsilí". Zaměřuje se na podvody, při nichž mají oběti posílat peníze do konkrétních západoafrických zemí. Projekt analyzuje finanční transakce remitenčních agentur, finančních institucí nebo bank mezi australskými územími a pěti západoafrickými zeměmi. Tyto údaje jsou analyzovány a využívány několika způsoby. Domácnostem podezřelým z podvodu, které posílají peníze do jedné z těchto zemí, jsou zasílány dopisy. z pěti zemí, jednu při zjištění podvodu a druhou o tři měsíce později, pokud budou platby pokračovat. Dopis obsahuje vysvětlení, proč je zasílán, a vyzývá je, aby se pro další informace obrátili na uvedené kontaktní místo. Propojené bankovní účty identifikovaných pachatelů a potenciálních obětí jsou rovněž potenciálně zablokovány, pokud budou pokračovat v zasílání finančních prostředků.
Při hodnocení projektu přestalo 72 % respondentů posílat peníze po jednom dopise a dalších 50 % těch, kteří obdrželi druhý dopis, přestalo posílat peníze. Malé procento respondentů po počátečním ukončení zasílání finančních prostředků obnovilo.[16]

Závěr

Internetové podvody jsou v Evropě stále významným problémem a v dohledné budoucnosti jím zůstanou. Naštěstí je k dispozici mnoho informací o tom, jak (online) podvody fungují a jak lze těmto podvodům předcházet. Chceme-li navrhnout účinné iniciativy prevence kriminality, je klíčové využít dostupné informace. Tento článek předkládá některé obecné koncepty a nástroje, které přesně toto umožňují. Jako zdroj inspirace může posloužit i několik nástrojů, které lze implementovat do iniciativ prevence kriminality
při budování nových projektů nebo je lze implementovat v rámci stávajících projektů. Online podvody se vyznačují vysokou mírou flexibility na straně pachatelů, která jim umožňuje přizpůsobit se měnícím se okolnostem. Informace v tomto dokumentu umožňují vypracovat vědecky podložené věcné reakce na ně.

Pokud chcete získat více (akademických) informací o podvodech online a další příklady z celé Evropy, přečtěte si **náš soubor nástrojů o jednotlivých podvodech** kliknutím sem.

Chceme-li navrhnout iniciativy v oblasti prevence kriminality, je klíčové využívat dostupné informace.

Poznámky na závěr

1 K. Crosman, Phone and Television Scams in the Age of the Internet, *Lewis & Clark Law Review* 21:3 (2017), 794.

2 Tamtéž; M. Button a C. Cross, Cyber Frauds, Scams and Their Victims, Oxon: Routledge, 794-5, 2017 #39.

3 Europol, Hodnocení hrozeb závažné a organizované trestné činnosti v Evropské unii: A Corrupting Influence, Lucemburk: Úřad pro publikace Evropské unie, 2021, 60, https://dx.doi.org/10.2813/02362; Europol, Internet Organised Crime Threat Assessment (Iocta) 2021, Lucemburk: Úřad pro publikace Evropské unie, 2021, 30-2.

4 Europol, Hodnocení hrozeb závažné a organizované trestné činnosti v Evropské unii: Kancherla, Motivational and Psychological Triggers in Social Engineering, Research Paper: Social Science Research Network, 2021, 1, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3750474#:~:text=Gragg%20(2002)%20extracted%20seven%20psychological,information%20that%20triggers%20strong%20emotions; A. Ferreira, L. Coventry a G. Lenzini (Eds.), *Principles of Persuasion in Social Engineering and Their Use in Phishing*, vyd. T. Tryfonas a I. Askoxylakis, Los Angeles: konferenční sborník, 2015, 36, https://.link.springer.com/chapter/10.1007/978-3-319-20376-8_4; F. Mouton, L. Leenen a H.S. Venter, Social Engineering Attack Examples, Templates and Scenarios, *Computers & Security* 59 (2016), https://dx.doi.org/https://doi.org/10.1016/j.cose.2016.03.004; J.-W.H. Bullée, L. Montoya, W. Pieters et al., On the Anatomy of Social Engineering Attacks - a Literature-Based Dissection of Successful Attacks, *Journal of Investigative Psychology and Oflender Profiling* 15:1 (2015), 20-1, https://dx.doi.org/https://doi.org/10.1002/jip.1482; X. Luo, R. Brody, A. Seazzu a S. Burd, Social Engineering: The Neglected Human Factor for Information Security Management, *Information Resources Management Journal* 24:3 (2011), 2.

5 Europol, Hodnocení hrozeb závažné a organizované trestné činnosti v Evropské unii: Whittaker a M. Button, Understanding Pet Scams: A Case Study of Advance Fee and Non-Delivery Fraud Using Victims' Accounts, *Australian & New Zealand Journal of Criminology* 53:4 (2020), 509-10, https://dx.doi.org/10.1177/0004865820957077.

6 S.N.C.f.C.P. (Brå), Fraud Crime in Sweden: Švédská národní rada pro prevenci kriminality (Brå), 2016, https://bra.se/down- load/18.7d27ebd916ea64de53037693/1582617820842/2016_9_Fraud_crime_in_Sweden.pdf.

7 Kancherla, Motivational and Psychological Triggers in Social Engineering, 2; M. Allen, Social Engineering a Means to Violate a Computer System: SANS institute, 2021, 4-5, https://sansorg.egnyte.com/dl/Y7NTZsCxKN; tamtéž, 6-7.

8 Bullée a kol., On the Anatomy of Social Engineering Attacks - a Literature-Based Dissection of Successful Attacks (Anatomie útoků sociálního inženýrství - literární rozbor úspěšných útoků), 21{Luo, 2011 #57.}

9 Verizon, Data Breach Investigations Report, 2021, 33, https://www.verizon.com/business/resources/reports/2022/dbir/2022-da- ta-breach-investigations-report-dbir.pdf.

10 M.T. Whitty, The Scammers Persuasive Techniques Model - Development of a Stage Model to Explain the Online Dating Romance Scam, *The British Journal of Criminology* 53:4 (2013), 668, https://dx.doi.org/https://doi.org/10.1093/bjc/azt009; J. Teeny, P. Biñol, and
R. Petty, *The Elaboration Likelihood Model:* Abingdon: Routledge, 2017, 393-8.

11 Luo a kol., Sociální inženýrství: Atkins a W. Huang, A Study of Social Engineeringin Online Frauds, *Open Journal of Social Sciences* 1:3 (2013), 23-4, https://dx.doi.org/http://dx.doi. org/10.4236/jss.2013.13004.

12 Ferreira a kol., *Principy přesvědčování v sociálním inženýrství a jejich využití při phishingu*, 39-40.

13 Bullée a kol., On the Anatomy of Social Engineering Attacks - a Literature-Based Dissection of Successful Attacks (Anatomie útoků sociálního inženýrství - literární rozbor úspěšných útoků), 34-5.

14 H. Dehghanniri a H. Borrion, Crime Scripting: A Systematic Review, *European Journal of Criminology* (2019), 2, https://dx.doi.org/10.1177/1477370819850943.

15 D.B. Cornish a R.V. Clarke, Opportunities, Percipators and Criminal Decisions: A Reply to Wortley's Critique of Situational Crime Prevention, 16 (2003), 41-96.

16 Button a Cross, Cyber Frauds, Scams and Their Victims, 205-8.

Kontaktní údaje

Sekretariát EUCPN E-
mail: eucpn@ibz.eu
Webové stránky:
www.eucpn.org

twitter.com/eucpn
facebook.com/eucpn
linkedin.com/company/eucpn