



Tomáš Šalmon



(Ne)bezpečný internet



Sprievodca
pre používateľov
internetu
od 10 do 99 rokov

viac >

V KNIHE NÁJDETE:

- > ako sa brániť kyberšikanе
- > ako bezpečne nakupovať v e-shopoch
- > ako rozoznať hoax alebo fake news
- > ako odhaliť internetových podvodníkov a útočníkov
- > ako sa nepopáliť na zoznamke a sociálnych sieťach
- > a mnoho ďalšieho

Ljndeni

HOAX

(Ne)bezpečný internet

Vyšlo aj v tlačovej podobe

Objednať môžete na
www.lindeni.sk
www.albatrosmedia.sk

Lindeni

Tomáš Šalmon
(Ne)bezpečný internet – e-kniha
Copyright © Albatros Media a. s., 2020

Všetky práva vyhradené.
Žiadna časť tejto publikácie nesmie byť rozširovaná
bez písomného súhlasu majiteľov práv.

ALBATROS  **MEDIA**

Tomáš Šalmon

(Ne)bezpečný internet



Spríevodca
pre používateľov
internetu
od 10 do 99 rokov

Ljndeni

Obsah

Predslov	11
Upozornenie	13
Štítky s odporúčaním „PRE KOHO“	14
O autorovi	15
Prehlásenie	15
KAPITOLA 1	
Internetové stránky a diskusie	17
Internetové stránky sa venujú všetkému, aj zlu...	17
Čím si otvárame a pozeráme internetové stránky?	18
Nebezpečný obsah na internete a sťahovanie	19
Vírusy na webe	21
Rizikové typy súborov	22
Spravodajstvo, magazíny a blogy	23
Skrývanie reklamy znižuje kvalitu obsahu	26
Konšpiračné portály	30
„Doktor Google“	32
Falošné stránky a magazíny	35
Podvodné reklamy a nebezpečné predaje	37
Pozor na falošných lekárov	39
Recenzie a overovanie	41
Hejtovanie, hejteri a svet nenávisťi	42
Cookies	46
Ako je to so sťahovaním z internetu?	49
Neverte (všetkému), ale overujte (čo overiť ide)	55
Kryptomeny	56
Obete vydierania s nahými fotkami a výkupné v BTC	60
Ako sa brániť pred vydieraním na Facebooku pomocou kryptomeny?	62
Nie ste si istí? Kde hľadať pomoc?	63

KAPITOLA 2

Kyberšikana 65

Šikana a jej online podoba – kyberšikana 65

Rozdelenie kyberšikany podľa typov agresorov 66

Rozdelenie kyberšikany podľa typov technológií 73

Ako riešiť kyberšikanu a na čo sa pripraviť? 77

Ako spoznať, že je dieťa obeťou kyberšikany? 77

Dospelý človek ako obeť kyberšikany 78

KAPITOLA 3

Sociálne siete 81

Sociálne siete 81

Neprehrádzajte o sebe priveľa 82

Neznámi „priatelia“ 84

Deti na sociálnych sieťach 86

Ochrana detí na sociálnych sieťach 87

Čo urobiť v rámci prevencie? 91

Čo je to viralita? 92

Osobný profil ako vlastná vizitka 92

Hacknutie účtu na Facebooku 93

Ideálna obeť? Outsider, hendikepovaný a sociálne slabší 96

Vydieranie a obchodovanie s fotkami 97

Máj 2019: Stovky obetí a ich nahé fotografie 97

Súťaže na Facebooku 99

Súťaže na Instagrame 102

Oznámenia o výhre 103

Verejné zbierky na sociálnych sieťach 109

Modlitba za „like“. Áno, čítate správne 110

Podvodné správy a reklamy 111

KAPITOLA 4

Zoznamky a „chat“ 113

Falošné zoznamky 114

Phishing prostredníctvom odkazu 118

Nebezpeční ľudia a pedofília 119

Dievčatá sú najčastejšou obeťou obťažovania 121

Fotografie a sexuálne narážky	122
Vydieranie a útoky	123
Deti sa ocitnú v pasci najčastejšie, keď...	125
Kultúra príspevkov, ktoré sú adresované ženám	129
Deviácie ako neznáma hrozba	131
Ako bojovať proti pedofilom?	136
KAPITOLA 5	
E-mail	137
E-mail v súčasnosti	137
Zabezpečenie e-mailu	140
Neporiadok a riziká v e-mailovej schránke	142
Zabudnuté heslo alebo zneužitie hackerom	145
Trestná činnosť cez e-mail	146
Prečo to nerobiť	147
Vydieranie cez e-mail	148
Phishing a popularita BitCoinu	149
E-maily s faktúrami a klamanie účtovníčok	151
Odkazom a prílohám v neznámych e-mailoch sa vyhýbajte	152
KAPITOLA 6	
Spam	155
Zopár šokujúcich čísiel	155
SPAM a jeho podoby	157
SPAM v e-mailovej schránke	157
SPAM v internetových diskusiách	157
SPAM v komentároch v článkoch	157
SPAM na ďalších miestach	158
Prečo ste dostali spam a kde ste pochybili?	158
Inzerát: Predám databázu e-mailových adres	160
Protiútok	161
Falošné zbierky pre chorých a v núdzi	163
Trolling	164
Falošné upozornenia na expiráciu domény	168
Pozor na falošné faktúry za „viditeľnosť stránky“	168
Katalógy stránok ako hrozba	170

KAPITOLA 7

Hoax a fake news 173

Ako spoznám hoax? 173

- Stručná typológia hoaxu 174
- Primitívne reťazové správy 177
- Hoax vzniká pre zábavu aj nevedomosť 178
- Hoax s mincami 179
- Hoax s koronavírusom 180

Reklamný a nákazlivý hoax na Facebooku 181

Fake News 183

- Vymyslené novinky ako kreatívna „oddychovka“ 185

KAPITOLA 8

Osobná bezpečnosť 187

- Osobné údaje a chúlостivé dáta 188
- Nedávajte o sebe vedieť všetko a všade 190

Heslá 191

- Funkcia zapamätania hesla 194

Mobil 195

- Ochrana mobilného telefónu 197
- SMS z inzerátov a platených služieb 198
- Absolútna bomba je, keď predávaš, aj platíš 204

Platobná karta 206

- Čo za žiadnych okolností nikdy nerobte 207

Fotografie 209

- iCloud hacking a celebrity online 211
- Autorské práva 212

Dokumenty, dáta, doklady, posudky... 213

Nepáči sa vám niečo? Bojujte! 217

KAPITOLA 9

Osobný počítač alebo mobil 221

Počítačové vírusy a ďalší nebezpečný software 222

- Malware alebo tiež „vírusy“ a ich podoby 223
- Antivírus 227

Wi-Fi 228

- Verejná Wi-Fi tam vonku 230
- Je webkamera na počítači rizikom? 231

Stahovanie súborov	233
Spôsoby šírenia súborov	235
Legálne prístupy k filmu, hudbe či softwaru	238
Záchrana zmazaných súborov	239
Predávate mobil, počítač alebo disk? Bacha!	241
KAPITOLA 10	
Zárobky, zisk a kryptomeny	243
Naozaj fungujúce systémy zárobku	244
Práca na doma	244
Hazardné hry	249
Provízne systémy a zisk z vášho webu	251
KAPITOLA 11	
Platené služby, nákupy a platby	255
Vaše nákupy = príležitosť pre podvodníka	255
Preverujte, za čo platíte	256
Internetové obchody a nakupovanie	257
Nákupy na eBay, Amazon a AliExpres	259
Falošní predajcovia hier	261
Pozor na pravidelné platby	262
Zneužitá platobná karta. Čo teraz?	263
Malware hrozby (vírusy), ktoré vyžadujú platby	264
KAPITOLA 12	
Návody a nástroje	267
Ako zistiť, či je fotografia originál a odkiaľ pochádza?	267
Reverzné vyhľadávanie obrázkov cez mobil	268
Ako vytvoriť to najlepšie heslo, ktoré existuje?	268
Kde získať bezplatné fotografie?	269
Nieкто vytvoril profil s vašimi fotografiami	270
Nahlásenie podvodnej súťaže / stránky na Facebooku	271
Nevhodné správanie používateľov je možné nahlásiť	272
Ako vytvoriť screenshot / snímku obrazovky	273
Ako zistiť vlastnú IP adresu	275
Trestné oznámenie	275

Slovník zo sveta online bezpečnosti	277
Záver	285
Nikdy sa nesmejte z menej skúseného používateľa počítača	285
Podakovanie	287
Register	289

Predslov

Internet je skvelý sluha, ale zlý pán. Pánom sa nad niekým môže stať práve vtedy, ak ho ovládne svojimi možnosťami a neobmedzenosťou, alebo ak ho ovládne niekto na druhej strane linky. Niekto bez mena a bez tváre, no s jasnými úmyslami. Aby sme mohli považovať internet za bezpečné prostredie, musíme ho poznať a vedieť sa v ňom pohybovať. Pre zdanlivú jednoduchosť má tento pocit každý. Možno aj vy. Len preto, že vám kedysi kamarát ukázal, ako si na YouTube nájdete video a ako prepnete na ďalšie, alebo si prečítate správy na Facebooku, už máte pocit, že to zvládáte.

Pravdou však je, že ani internet nebol vybudovaný pôvodne na to, na čo sa používa dnes. Na prvý pohľad je nástrojom úžasným, na pohľad druhý nekonečným... a na pohľad tretí nebezpečným.

Príliš prístupný internet odhalil nepripravenosť ľudí

Moderné technológie, výhodné dátové balíčky mobilných operátorov, ale pokojne aj rodičia, ktorí sa naučili zbaviť sa svojich detí pripojením k internetu, spôsobili jeden veľmi vážny problém. Internet sa stal dostupnejším. Súčasná moderná rodina už nechodí k babičke tak často, pretože jej pod vianočný stromček kúpili už tretí tablet, pripojili na internet a naučili ju komunikovať na Skype. Babička objavila kúzlo Facebooku, surfovania na Googli a rovnako tak veľké množstvo detí v mobile sleduje správy a statusy svojich priateľov. Pripojený je každý, no pripravený je možno každý desiaty. Rovnako tak, ako všetci na Slovensku majú pripojenie, internet objavilo aj mnoho živlov. Jednotlivcov, ktorí prišli na nedokonalosti nejakého systému, alebo zločincov, pre ktorých je internet zlatou baňou. V prvom rade sú to ľudia, ktorí z neho robia nebezpečné prostredie. Vyhľadávajú medzery a príležitosti, ako okradnúť ostatných. Internet na to ponúka výnimočné príležitosti a aj oveľa slabší pocit viny, ako keby ste okradli niekoho na ulici. Nevidieť obeti tvár, takže neprichádzajú žiadne výčitky. Je ňou ale vždy niekto živý. Možno ste to vy alebo niekto z vašich priateľov a blízkych. Lenže nie každý si prizná, že sa nechal oklamať. Znamenalo by to poníženie pred ostatnými. Naj-

mä v mladom kolektíve. Stať sa obeťou podvodníka, klamstva, hackera alebo nebezpečného útoku je dnes také bežné, ako zabudnúť niekde kľúče alebo sa ocitnúť v zápche.

Kde hľadať pomoc?

Na Slovensku neexistuje vážny inštitút pomoci, záchranná linka a ani polícia niekedy nie je to najvhodnejšie miesto, kde hľadať pomoc. Sú tu len projekty ako **zodpovedne.sk** alebo **pomoc.sk** a pridružené projekty. Za niekoľko rokov som zažil neuveriteľné množstvo prípadov, osudov, nešťastí alebo útokov. Vždy s rôznou intenzitou, v rôznom štádiu pokusu, ale aj takých, kde už bolo neskoro. Aj preto bolo mojou snahou priniesť materiál, ktorý by mohol upozorniť na všetko to nečisté a nebezpečné, ktorému sa odmietajú mnohé médiá venovať. O mnohých problémoch verejnosť nevie. Zrejme ste ani len netušili, aký nebezpečný vie byť napríklad Facebook. Inak nebezpečný pre toho, kto má v profile uvedený vek 16 rokov, a celkom inak nebezpečný pre toho, kto si vyplnil rok narodenia 1956. Práve na našich starých rodičov číha na internete nepredstaviteľné množstvo hrozieb. Šmejdi sa presúvajú na internet už dlhšie, no so silou, akou cieľia reklamy dnes, prekonávajú očakávania.



Foto: pixabay.com, RobinHiggins, caffeinesystem

Upozornenie

Táto publikácia nie je dielom psychológa ani policajného vyšetrovateľa. Je dielom niekoľkoročného úsilia pomôcť ľuďom, ktorí o ňu žiadali a ktorí ju potrebovali. Je súhrnom mnohých skúseností a snahy o upozornenie na problémy, ktoré dodnes nemusia mať riešenia a verejnosť ich v niektorých prípadoch stále nerozoznáva. Ak vám táto knižka umožní pochopiť hrozby a inšpiruje vás akokoľvek pomáhať ďalším, jej účel a môj cieľ sa tým pádom začal naplňovať. Cieľom tejto publikácie je upozorniť na problémy, ktoré ste možno doteraz za ne ani nepovažovali. Rád by som vám nasadil vylepšené „okuliare“, pomocou ktorých rozoznáte hrozbu oveľa ľahšie, ale rovnako tak nájdete riešenia. Popisované postupy, akými konajú podvodníci a útočníci, nemajú slúžiť na ich kopírovanie. Sú predstavené a vysvetlené, aby vám umožnili praktiky jasne identifikovať. Zároveň postupy a kroky páchatelov pochopiť. Každá obeť sa môže brániť a takmer vždy existuje riešenie, ako páchatela potrestať. Práve o tom je táto kniha. Jej cieľom je pomôcť a možno zachrániť viac ako len peniaze.

Kniha vychádza z osobných skúseností a praxe autora. Jednotlivé navrhované postupy a odporúčania mohli byť výsledkom výraznej improvizácie pre chýbajúce iné dostupné riešenia. Túto improvizáciu bolo možné neustále zdokonaľovať priamo v praxi. Poznatky a fakty v tejto knihe zväčša nevychádzajú z prekladanej literatúry a iných zdrojov, ale priamo zo slovenského prostredia. Z diania sledovaného stále rovnakými očami a zaznamenávané pomyselným „rovnakým perom“ s odstupom rokov.

Kniha a jej obsah nenahrádza odbornú právnu pomoc, činnosť polície a ňou poverených odborníkov.

Štítky s odporúčaním „PRE KOHO“

Táto kniha je v celom rozsahu určená čitateľom všetkých generácií. Jednotlivé časti však vyslovene odporúčam konkrétnym generáciám alebo skupinám ľudí. Primárne určená cieľová kategória čitateľa môže byť uvedená ako štítok s odporúčaním.

- ▶ **DETI** – téma vhodná pre začínajúcich používateľov a deti do 14 rokov
- ▶ **MLÁDEŽ** – téma vhodná pre mládež od 13 do 20 rokov
- ▶ **DOSPELÍ** – odporúčanie tém vhodných pre ľudí v produktívnom veku, dospelých, rodičov aj nerodičov. Obsah sa venuje hrozbám, ktoré sa môžu týkať priamo ich pôsobenia a cielenia hrozby
- ▶ **SENIOR** – téma označené pre seniorov približuje pozadie hrozieb, ktoré môžu byť cielené práve na starších ľudí
- ▶ **PODNIKATEĽ** – témy popisujúce ohrozenia podnikania, stabilitu používaného systému či ohrozenie financií firmy
- ▶ **VŠETCI** – témy určené všetkým bez rozdielu veku

O autorovi

Tomáš Šalmon sa pohybuje v prostredí internetu od roku 2001. Je autorom viacerých stránok a niekoľkých aplikácií. V priebehu rokov 2004 až 2007 sa výraznejšie zaoberal skúmaním internetu, zárobkových systémov a zrodu prvých veľkých hráčov v internetovej komunikácii. Pred niekoľkými rokmi odovzdával na hodinách informatiky vedomosti žiakom na dvoch základných školách. Na cestu boja proti internetovým hrozbám sa vydal po niekoľkých prípadoch zneužitia a vážneho ohrozenia ľudí v jeho blízkosti. V záujme vyriešiť to, čo bolo nad sily akéhokoľvek úradu a možnosti obyčajného človeka, ako aj v záujme zamedziť, aby sa podobné prípady neopakovali, začal sa venovať téme, ktorej rozsahu a bezohľadnosti ani po rokoch celkom neporozumel. Od roku 2008 sa pre takéto prípady zamerával na slovenské zoznamovacie prostredie. Pre jeho pôsobenie v rôznych internetových komunitách si ho začínali všímať a vyhľadávať prvé obeť rôznych hrozieb. Prelom prišiel v roku 2012, keď prenikol do tajomstiev oveľa väčších hrozieb, ako sa bežne spomínajú. V priebehu posledných rokov prispieva na slovenské portály zaoberajúce sa internetom alebo kybernetickou bezpečnosťou. Spolupracuje príležitostne s médiami, s redaktormi televízie Markíza, s portálom hoax.sk a ďalšími miestami. Rovnako tak odpovedá na žiadosti o informácie vyšetrovateľov a obetí kyberšikany, útokov, podvodov, zneužitia a vydierania.

Prehlásenie

Autor publikácie nie je súčasťou žiadnej ilegálnej komunity. Nie je prechováateľom a šíriteľom žiadnych nezákonných materiálov. Nevyužíva ilegálne nástroje, prípadne postupy, ktoré by boli v rozpore s platnou legislatívou, dobrými mravmi a zákonmi. Jednotlivé prípady a ukážky uvádza na základe dôkazov a výpovedí poškodených, prípadne uvádza zdroje. Za svoju činnosť počas celého trvania neprevzal ako odmenu žiadne finančné alebo hmotné dary. Autor publikácie nie je vlastníkom žiadnej programovej výbavy, používateľom ilegálneho softwaru alebo scriptov zasahujúcich akokoľvek do onli-

ne prostredia alebo počítačov. Autor dokonca v súčasnosti nie je vlastníkom vlastného počítača a postupne opúšťa online prostredie, ktorému sa plánuje venovať len príležitostne.

KAPITOLA 1

Internetové stránky a diskusie

Ak by som mal definovať odborne a oficiálne, čo je webová alebo internetová stránka, ide o online prístupný dokument uložený na serveri, ku ktorému prístupuje používateľ pomocou konkrétnej IP adresy alebo dnes už takmer výlučne len pomocou doménovej adresy. Dokument obsahuje hypertext, obrázky a rôzne ďalšie prvky. Vybavený je scriptmi, ktoré reagujú na používateľa, jeho potreby. Stránky prispôsobujú podľa toho, či prichádza používateľ cez mobil alebo počítač, či prichádza opakovane. Stránky pozeráme v aplikácii, ktorá sa volá internetový prehliadač.

Internetové stránky sa venujú všetkému, aj zlu...

Súčasná ponuka internetu prináša všetko. Vieme si na internete objednať aj zaplatiť hotel kdekoľvek na svete, spojiť to s dopravou, transfermi, službami, požičať si auto, vybaviť si niektoré typy dokladov, zabezpečiť si u lekára očkovanie, zmeniť poisťovňu, investovať peniaze na burze, komunikovať s priateľmi, pracovať, pripájať sa do práce z pohodlia domu (takzvaný homeoffice), sťahovať hudbu, komponovať hudbu, vytvárať grafiku, hrať sa online... Bolo by to však 1 888 strán navyše, ktoré nebudem zaplňať popisom všetkých činností. Na internete je dnes naozaj všetko. Aj návod na bomby a svetlice sa mi podarí nájsť v priebehu 60 minút, kým v roku 2001 na to stačilo pár sekúnd. Za posledné roky vznikli rôzne zabezpečenia. Aj Google robí veľa pre ochranu ľudí pred nebezpečnými stránkami. V minulosti bolo ľahké dostať sa na stránky zaplnené vírusmi či na stránky, ktoré nemali potrebné zabezpečenia. Dnes vás veľmi rýchlo na taký web upozorní už webový prehliadač.

Prvé zoznámenie sa s internetom sa tak pre mnohé deti neodohráva na hodinách informatiky, ale v tabletoch a mobiloch doma. Odrazu je povinnou aplikáciou Facebook, lebo každý z triedy ho už má a byť výnimkou znamená byť „out“. Odrazu je to Facebook, čo dieťa ovláda lepšie ako vlastný rodný jazyk či techniku umývania zubov. Pre ľudí v produktívnom veku číha najviac rizík na zoznamkách, v emailoch a pri surfovaní. Aj keď je pravdou, že ženy a dôverčiví ľudia sú ľahšou obeťou v každom veku.

VŠETCI

Čím si otvárame a pozeráme internetové stránky?

Internetové stránky dokážu čítať internetové prehliadače. Internetový prehliadač, alebo ak chcete „browser“, je aplikácia s niekoľkými nástrojmi (nastavenia hesiel, domovská adresa, záložky, rôzne funkcie ladenia a podobne), no hlavne s políčkom pre zadanie adresy a priestorom pre zobrazovanie samotnej stránky. Každý počítač s Windowsom má od výroby **Internet Explorer** (charakteristické modré malé „e“). V mnohých svojich verziách na mnohých počítačoch je v žalostne zlom stave, nefunkčný a pomalý. Windows 10 má rýchlejšiu a o trochu bezpečnejšiu verziu s názvom **Microsoft Edge**. Internet Explorer radi celé roky nahradzujeme **Google Chrome** alebo prehliadačom **Mozilla Firefox**. Počítače s operačným systémom od Apple sú vybavené prehliadačom **Safari**. Princíp fungovania je však stále rovnaký. Všetky sú bezplatné a tie lepšie sa udržiavajú aktuálne samé. Odporúčam nesťahovať si žiaden z týchto prehliadačov z iných miest ako tých oficiálnych. Objavuje sa aj slovenská verzia Firefoxu zo stránok, ktoré si z Firefoxu urobili hračku na propagáciu svojich stránok a rôznych partnerov. Nič, čo by sa dalo nazvať užívateľským komfortom.



Chrome



Safari



Firefox



Microsoft Edge

Oficiálne stránky pre jednotlivé prehliadače:

- ▶ Google Chrome: <https://www.google.com/intl/sk/chrome/>
- ▶ Mozilla Firefox: <https://www.mozilla.org/sk/firefox/new/>
- ▶ Opera: <https://www.opera.com/sk>

VŠETCI

Nebezpečný obsah na internete a sťahovanie

Internet je obľúbený nástroj pre prístupnosť čohokoľvek. Skrátka si to stiahnete. Láka sťahovanie celkom nových hier, ilegálnych prídavkov, elektronických kníh, skúšanie nových aplikácií alebo erotické videá nejakej známej celebrity. Pokiaľ ide o niečo mimoriadne lákavé a populárne, je to príležitosť pre hackerov, aby do súborov ukryli skrytý kód (malware či hovorovo „vírus“). Pozmenili súbory a nachystali pascu. Horlivo si milióny ľudí stiahnu hernú novinku a plní nadšenia si ju zahrajú, no ani len netušia, že s hrou inštalujú niečo navyše.

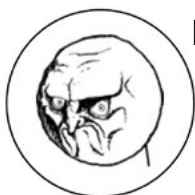


Dobre zabezpečený počítač vám nedovolí vstúpiť na podozrivé a infikované stránky. Objaví sa upozornenie pred hrozbou. Buď priamo komunikuje s databázou prehliadača a zobrazí varovanie, alebo zareaguje antivírus svojím upozornením.



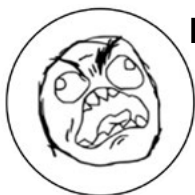
Kedy ste menej ohrození?

Relatívne bezpečné môže byť správanie, kedy na stránky prichádzate cez Google, navštevujete bežné známe portály, nezachádzate do neznámych vôd a nenakupujete v neznámych obchodoch. V počítači by ste mali mať minimálne aspoň nejaké antivírusové riešenie. Freeware či priamo to, ktoré je súčasťou aktualizovaného OS Windows. Platí, že nesťahujete filmy, hry, software, neprechádzate po neznámych stránkach, fórach a neklikáte na odkazy. Poštu zároveň nesťahujete Outlookom do počítača.



Kedy ste viac ohrození?

Viac sa vystavujete hrozbám, keď máte počítač zabezpečený bezplatným antivírusovým riešením, internet používate v neprehnanej miere na surfovanie, sem-tam si stiahnete nejaký film, hru, klikáte aj na neznáme stránky a na email sa prihlasujete jedine priamo na gmail.com alebo v inej službe bez používania Outlooku. Pri veľkom šťastí sa pokojne stane, že vás nič po celý čas používania počítača neohrozí. Opakujem – pri veľkom šťastí.



Kedy ste najviac ohrození?

Pri používaní internetu a surfovaní sa najviac vystavujete nebezpečenstvu, ak v sebe kombinujete slabú antivírusovú ochranu, používate posťahovaný ilegálny software, v ktorom sa hravo skryje trójsky kôň či mallware, sledujete fóra, internetové stránky, klikáte na odkazy v stiahnutých súboroch, sťahujete poшту cez Outlook priamo do počítača a na sťahovanie súborov používate P2P klientov pre sťahovanie torrentov. To je ideálny spôsob, ako k sebe dostať spiaci vírus cielene a ešte s pomocou viacerých rovnako oklamáných „seederov“.