NetAgent

NetAgent

MONITOROVACÍ SLUŽBA NA OCHRANU OSOBNÍCH DAT NA INTERNETU

CRIF CZECH CREDIT BUREAU
Together to the next level

kolikmam.cz

Obsah

Úvodní slovo

Počítačová kriminalita je rychle rostoucí oblast trestné činnosti. Zločinci stále více zneužívají rychlost, pohodlí a anonymitu internetu k páchání pestré škály trestných činností, které neznají hranice. V minulosti byla počítačová trestná činnost byla páchána hlavně jednotlivci nebo malými skupinami. V současné době jsme svědky velmi složité kyberkriminální sítě sdružující jednotlivce z celého světa k páchání trestné činnosti nebývalého rozsahu. Zločinecké organizace se obracejí k internetu, aby si usnadnily činnost a maximalizovaly svůj zisk v co nejkratším čase. Samotné zločiny nejsou nové, ale zločinecké organizace je vyvíjí v souladu s příležitostí, kterou on-line svět nabízí. Kyberyber kriminalita má rostoucí tempo a stále masivnější dopady. Je těžké si pamatovat všechny on-line účty a jejich přihlašovací údaje. Uživatelé internetu běžně používají stejné jméno a heslo do všech portálů a emailových schránek. Neuvědomují si však, že tímto chováním otvírají dveře podvodníkům. Jakmile dojde k prolomení jednoho z takových webů, pak podvodníkům zpřístupní i emailové schránky a jejich obsah.

Romana Knyblová
Projektová manažerka portálu kolikmam.cz

Služba NetAgent

NetAgent je první české řešení pro veřejnost, které aktivně detekuje ukradené osobní údaje a narušená důvěrná data na internetu. Pročesává blogy, webové stránky, nástěnky, fóra, sociální sítě, peer to peer sítě a chatovací místnosti, kde dochází k nelegálnímu obchodování a prodeji osobních údajů. Jedná se o jediné monitorovací řešení určené k proaktivní kybernetické detekci na mezinárodní úrovni, bez jazykových bariér, a odhalování krádeží identity po celém světě. Nabízí možnost neustálého sledování pohybu osobních a finančních údajů na internetu, aby se zabránilo jejich použití k nezákonným účelům a umožnilo uživateli rychle reagovat a přijmout nezbytná ochranná opatření.

Odkud pochází informace naší NetAgent služby?

Tyto údaje pocházejí z vyhledávání na veřejném webu a z databáze darkweb serverů, anonymních webových služeb atd.

Co to znamená, když obdržím nějaké upozornění?

NetAgent sleduje internetovou aktivitu kolem vámi nadefinovaných osobních údajů. Toto oznámení značí, že naše monitorovací technologie objevila na internetu informaci, která se shoduje s vámi monitorovanými údaji a poskytuje v detailu informace i zdroj kompromitace.

Co když notifikační zprávy zahrnují jen některé z monitorovaných osobních údajů službou NetAgent?

Pokud vás informujeme, že jen některé z vašich osobních dat, které si monitorujete, byly detekovány službou NetAgent jako narušené, doporučujeme obrátit se na příslušnou instituci, aby informace o vašem účtu změnila nebo si změňte informace o účtu sami, pokud je to možné. Dále **lze předpokládat, že pokud jsou ohrožené pouze některé informace, může se to týkat i všech. V takovém případě je vhodné zakoupit si i výpis z registrů a zkontrolovat, zda nedošlo k nějakému úvěrovému podvodu na vaší identitě. Zkontrolovat své bankovní účty a projít uvedené transakce, zda všechny transakce znáte a nemohlo dojít např. k nelegálním transferům, nákupům nebo výběrům z kreditních karet.**

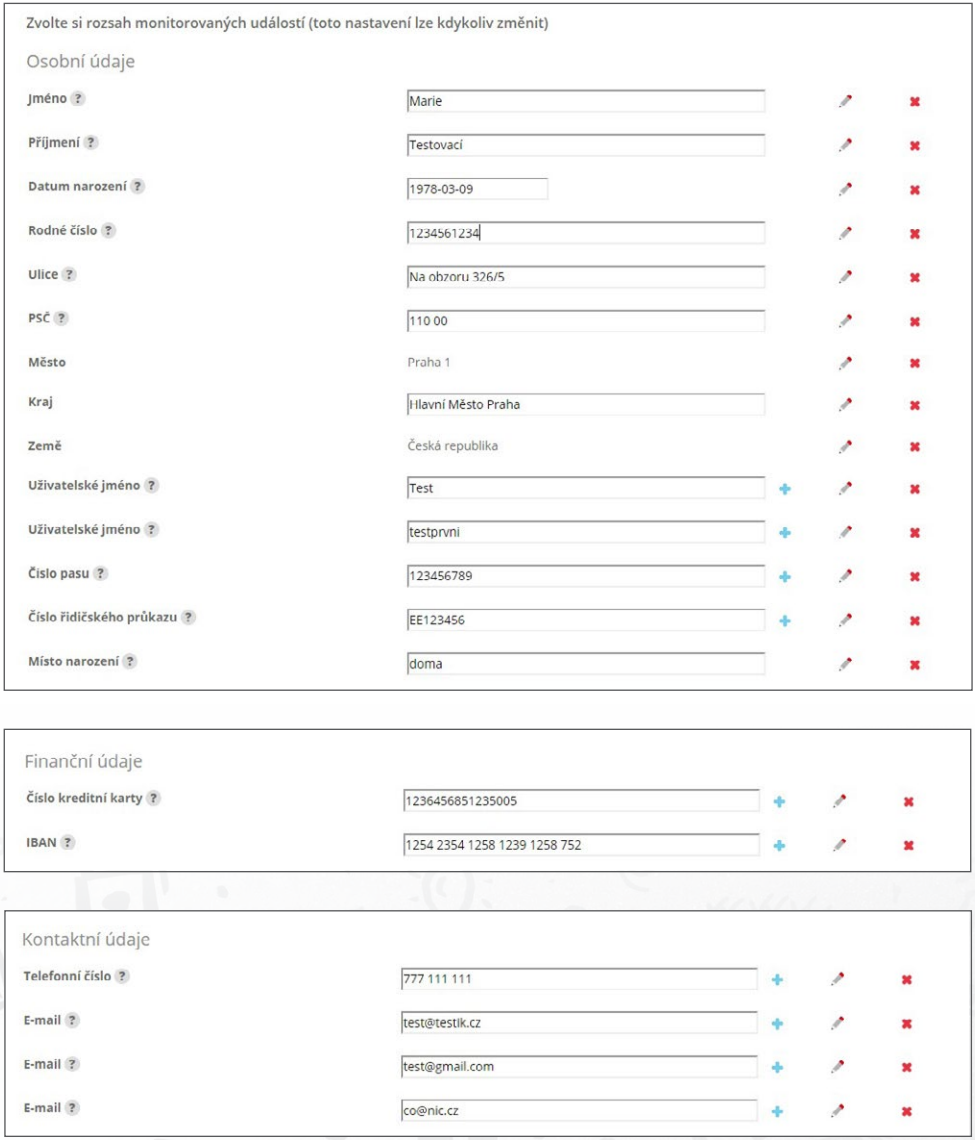
Mohu se stát obětí krádeže identity, i když jsem si předplatil službu NetAgent?

NetAgent výrazně snižuje riziko krádeže identity tím, že se s předstihem dozvíte, pokud jsou vaše osobní údaje nějak ohroženy. Služba umožňuje prevenci a rychlé řešení pro případ krádeže identity. Je vhodné si aktivovat také službu Hlídám si, kolik mám. Ta sleduje pohyby v registrech (BRKI a NRKI) a monitoruje, zda nevznikla nová událost nebo nebyla podána žádost o úvěrový produkt v některém z registrů. Kromě toho vám služba Hlídám si, kolik mám pomáhá sledovat stav v registrech, jestli nevznikla žádost o úvěrový produkt. Bohužel žádný nástroj na ochranu identity nemůže zabránit krádežím identity úplně.

Vaše osobní údaje jsou velmi cenné, a to především pro ty, kteří je chtějí používat k různým podvodům a nelegálním obchodům.

Výhody služby:

1. NetAgent monitoruje, zda nezaznamená osobní identifikační údaje uživatele na globálních webových stránkách na černém trhu, v internetových chatech a na sociálních sítích, jako jsou jméno a příjmení, datum narození, rodné číslo, číslo bankovního účtu, čísla kreditních a debetních karet, e-mailové adresy a hesla, telefonní čísla, čísla pasů nebo mezinárodní čísla bankovních účtů, záleží jen na rozsahu definovaném uživatelem. Umožňuje včas reagovat a podniknout kroky k ochraně osobních údajů.



2. NetAgent vás upozorní, pokud zaznamenáme nějakou činnost s vašimi daty. Ne vždy je možné poskytnout zdroj, kde byla data vystavena. Hackeři jsou vynalézaví a nabízí své zcizené seznamy na sociálních sítích, různých dark webech nebo je obchodují P2P a někdy není tedy možné zjistit, kde údaje zcizili, kterou stránku vykradli. NetAgent uvádí rozsah, který byl nalezen právě při zveřejnění jejich seznamů. Jestliže zdrojová stránka nebyla uvedena, znamená to, že touto informací nedisponujeme.
3. Nepřetržitě monitorujeme tisíce webových stránek sociální sítě, darkweby, atd.

Co dělat, když ztratím nebo mi byl zcizen občanský průkaz?

1. OZNÁMIT UDÁLOST

Nejprve situaci oznamte nejbližšímu místně příslušnému úřadu nebo Policii ČR, kde získáte potvrzení o ztraceném dokladu.

2. POŽÁDAT O NOVÝ

Musím jít požádat o novou, a to u kteréhokoliv obecního úřadu obce s rozšířenou působností, v Praze u kteréhokoliv úřadu městské části Prahy 1 - 22. Při ztrátě nebo odcizení občanského průkazu v zahraničí se tato skutečnost nahlásí místnímu oddělení policie, které o ztrátě vydá potvrzení a následně je nutné nahlásit na zastupitelském úřadě ČR v zahraničí. Pokud v zemi není ČR zastoupena, je možné se obrátit na zastupitelský úřad některého členského státu EU, který má v dané zemi zastoupení. V zahraničí nelze zažádat o vydání nového občanského průkazu. Pokud byl ztracený či odcizený OP zároveň cestovním dokladem, je občanovi vydán tzv. cestovní průkaz sloužící k návratu do ČR.

Proč si mám chránit svůj občanský průkaz?

V případě zcizení občanky může docházet ke zneužití vaší identity, k úvěrovým podvodům, zakládání bankovních účtů, které následně slouží k nelegálním převodům peněz.

3. CO S SEBOU:

a. **Jiný doklad totožnosti** - v případě, že občan ohlašuje ztrátu, odcizení či poškození občanského průkazu na úřadě a současně chce podat žádost o vydání nového občanského průkazu, předkládá doklad prokazující jeho totožnost (rodný list, cestovní pas, oddací list, řidičský průkaz, apod.

b. **Potvrzení o ztrátě** - formulář, ve kterém jsou uvedeny okolnosti ztráty, odcizení či poškození se vyplňuje přímo na přepážce při ohlášení této skutečnosti.

c. **Peníze** - za vydání nového občanského průkazu za průkaz ztracený, odcizený nebo poškozený se hradí správní poplatek ve výši **100 Kč**. Správní poplatek se hradí při podání žádosti o nový občanský průkaz přímo na přepážce.

A pokud žádáte o vydání OP bez strojově čitelných údajů, tak je nutné s sebou mít:

d. **Vyplněný tiskopis** žádosti o vydání občanského průkazu; příslušný tiskopis je k dispozici na oddělení osobních dokladů a evidence obyvatel.

e. **Dvě fotografie o rozměru 35 mm x 45 mm**, odpovídající současné podobě občana, zobrazující občana v předním čelném pohledu, v občanském oděvu, bez pokrývky hlavy, bez brýlí s tmavými skly, s výjimkou nevidomých, s výškou obličejové části hlavy od očí k bradě minimálně 13 mm, které splňují technické provedení, stanovené vyhláškou č. 400/2011 Sb., v platném znění.

Co dělat, když ztratím řidičský průkaz?

1. OZNÁMIT UDÁLOST

Nejprve jste povinni tuto skutečnost neprodleně oznámit příslušnému obecnímu úřadu obce s rozšířenou působností podle místa svého obvyklého bydliště a Policii ČR (ohláška policii není povinná, ale doporučujeme tak učinit);

2. POŽÁDAT O NOVÝ

Musím jít požádat o nový a v případě odcizení osoba předloží obecnímu úřadu obce s rozšířenou působností nebo magistrátu města na území ČR **oznámení o odcizení** z oddělení Policie ČR,

3. CO SI VZÍT S SEBOU:

a. **doklad totožnosti** (občanský průkaz, popř. cestovní pas společně s potvrzením o občanském průkazu, které je vydáno v případě ztráty nebo odcizení občanského průkazu), v případě poškození ŘP nebo mezinárodního ŘP i poškozený průkaz,

b. **jednu barevnou či černobílou průkazovou fotografii,**

c. **vyplněnou žádost o vydání ŘP nebo MŘP** při poškození průkazu i poškozený ŘP nebo MŘP

d. **peníze** – správní poplatek za vydání nového ŘP nebo mezinárodního ŘP je zákonem stanoven ve výši **50 Kč**

Proč si mám chránit svůj řidičský průkaz?

V případě zcizení řidičského průkazu může docházet k žádostem o vytváření nových falešných dokladů totožnosti s jinou fotografií, následně pak k úvěrovým podvodům a dalším nelegálním činnostem.

Co dělat, když ztratím pas?

Oznámení ztráty, odcizení nebo nálezu cestovního pasu může učinit v České republice na kterémkoliv obecním úřadu obce s rozšířenou působností nebo matričním úřadu nebo nejbližším útvaru policie České republiky. V zahraničí je držitel povinen ohlásit neprodleně ztrátu, odcizení, zničení cestovního dokladu nebo jeho nález nejbližšímu zastupitelskému úřadu. Zastupitelský úřad vystaví držiteli potvrzení o ztrátě, odcizení nebo zničení cestovního dokladu a současně bezodkladně oznámí tuto skutečnost orgánu příslušnému k vydání cestovního dokladu.

Proč si mám chránit svůj pas?

V případě zcizení pasu může docházet stejně jako v případě OP ke zneužití identity k úvěrovým podvodům, zakládání bankovních účtů určených k nelegálním převodům peněz.

K žádosti o vydání cestovního pasu je třeba předložit:

- **doklad totožnosti** například občanský průkaz (u občanů, kteří nemají občanský průkaz, jiné doklady, např. rodný list nebo oddací list), doklad o státní občanství (doklad o státním občanství se vyžaduje při vydání prvního cestovního pasu občanovi, který nemá trvalý pobyt na území České republiky)
- **žádost o vydání nového dokladu**, osobně
- **správní poplatky:**
  - **za vydání cestovního pasu**

    vydání cestovního pasu **600 Kč**
    - občanům mladším 15 let **100 Kč**

    vydání cestovního pasu ve zkrácené lhůtě **4 000 Kč**
    - občanům mladším 15 let **2 000 Kč**

  Tyto správní poplatky se platí při podání žádosti.

  - **za převzetí cestovního pasu**

  Za převzetí cestovního pasu se platí správní poplatek **100 Kč**, pokud občan převezme cestovní pas vydaný ve lhůtě 30 dnů u jiného úřadu, než podal žádost o jeho vydání. **Správní poplatek zaplatí před převzetím cestovního pasu.**

Co dělat, když obdržím informaci o pravděpodobném zneužití mé kreditní karty nebo jsem dokonce kreditní kartu ztratil?

Zneužití platební karty je obecný termín používaný k popisu celé řady trestných činů zahrnujících krádeže a podvodné používání údajů z účtu platební karty. Časté typy podvodů s platebními kartami zahrnují:

1) **podvodné aplikace** - typ krádeže identity, ve kterých jsou platební karty získány podvodným aplikačním procesem pomocí odcizených nebo padělaných dokladů.
2) **převzetí účtu** – jiný typ ID krádeže, to obvykle zahrnuje podvod finanční instituce, převydání platební karty a její přesměrování na jinou adresu.

Proč chránit číslo mé kreditní karty?

Zločinci kradou číslo vaší karty tím, že napadnou webové stránky, kde jste ji použili nebo napadají počítače se speciálním malwarem (což je počítačový program určený ke vniknutí nebo poškození počítačového systému), který zachycuje zadané kódy.

3) **ztracená/odcizená karta** - jak již název napovídá, tento typ podvodu se týká zneužití skutečných karet, které jsou buď ztracené nebo ukradené od skutečného držitele karty.

4) **padělané karty** - tento podvod se provádí pomocí plastových karet, které byly speciálně vyrobené nebo stávajících karet, které byly změněny. Tyto karty jsou kódovány pomocí nelegálně získaných dat z účtu platební karty, aby se dalo zaplatit za zboží a služby nebo slouží k výběru hotovosti.

5) **bez přítomnosti karty (CNP)** - tento typ podvodů spáchaných za použití dat účtu platebních karet na provádění transakcí, kde není face-to-face kontakt mezi prodávajícím a kupujícím. Obvykle se tento typ podvodu děje na internetu, u zásilkového obchodu nebo telefonicky. CNP podvody jsou v současné době nejrychleji rostoucím typem podvodů.

6) **ATM cash-out podvody** - u tohoto typu zločinu, zločinecká organizace napadají platební sítě, kradou čísla karet a odstraňují všechny výdajové nebo výběrové limity na kartách. Čísla karet jsou zasílána členům sítě po celém světě, kteří je překoduji do prázdných karet a používají je pak k výběrům obrovského množství hotovosti z bankomatů (ATM).

V takovém případě se neprodleně obraťte na svoji banku, kontakty na jejich karetní oddělení, kde provedou blokaci platební karty naleznete níže.

Co dělat, abych předešel zneužití mé kreditní karty při výběru z bankomatu? (SKIMMING)

Je potřeba být obezřetný, opatrný a při jakémkoli podezření na nestandardní chování bankomatu doporučujeme vůbec kartu nevkládat a informovat danou banku nebo policii.

- prohlédněte si vždy bankomat, ze kterého chcete vybírat
- při zadávání PIN dbejte na to, aby nikdo za zády či odjinud nemohl PIN odpozorovat
- pokud se bankomat chová nestandardně nebo je na něm připevněno nějaké neobvyklé přídavné zařízení, informujte banku nebo policii. Z bankomatu nevybírejte.
- v případě problémů při výběru nepřijímejte v žádném případě „pomoc“ cizích osob (např. rady na opakované zadání PIN)
- v případě, že bankomat nevydá bankovky, zkontrolujte pro jistotu, zda nebyl na výdejní otvor instalován falešný kryt

Proč chránit číslo mé kreditní karty?

Ke zneužití kreditní karty může dojít i při výběru z bankomatu. V případě zcizení údajů vaší kreditní karty může docházet k nelegálním nákupům v e-shopech apod.

Banky

Komerční banka, a.s.
blokace KK: +420 955 512 230

Raiffeisen stavební spořitelna a. s.
blokace KK: +420 800 900 900

Fio banka, a.s.
blokace KK: +420 224 346 777

Air Bank, a.s.
blokace KK: +420 547 134 134

Waldviertler Sparkasse Bank
blokace KK: +420 495 800 111

mBank S.A., organizační složka
blokace KK: +420 844 777 000

Citibank Europe plc, org. složka
blokace KK: +420 233 062 222

Česká spořitelna
blokace KK: +420 800 207 207

UniCredit Bank Czech Republik and Slovakia, a. s.
blokace KK: +420 800 140 014

MONETA Money Bank, a.s.
blokace KK: +420 224 443 636

Raiffeisenbank, a.s.

Expobank CZ, a. s., LBBW Bank CZ a.s.
blokace KK: +420 272 771 111

Equa bank a.s.
blokace KK: +420 222 010 222

Sberbank CZ, a.s.
blokace KK: +420 495 800 111

Zuno Bank AG
blokace KK: +420 245 699 999

Československá obchodní banka, a.s.
blokace KK: +420 495 800 111

Oberbank AG pobočka Česká republika
blokace KK: +420 495 800 111

Centra pro blokace karet
VISA* - Global Customer Assistance Service:
800 142 121 / +1 410 58113836

MasterCard* - MasterCard Global Service:
800 142 494 / +1 636 7227111

Diners Club:
+420 267 197 450

Global Payments Europe:
+420 272 771 111

Co dělat, když obdržím informaci, že moje emailová adresa byla zneužita?

Neprodleně změňte heslo do své emailové schránky. Nové heslo by mělo mít alespoň 8 znaků, použijte alespoň jedno velké písmeno, alespoň jeden znak a alespoň jedno číslo. Vyhněte se vytváření hesel ze jmen svých dětí, manželek/manželů, zvířecích miláčků, data narození a dalších snadno dohledatelných údajů na internetu. Zároveň zkontrolujte schránku, zda nedošlo k odeslání nevhodných emailových zpráv vašim kontaktům.

Mnohdy vaším jménem požadují od vašich blízkých peníze, mohou ukrást osobní data nebo instalovat škodlivý software příjemci vašich zpráv. Bez ohledu na skutečnost, že využíváte emailové adresy jako uživatelské jméno do sociálních sítí a aplikací.

Proč chránit e-mailový účet?

Díky vaší emailové adrese mohou podvodníci přistupovat k emailovým účtům a tím vám vytvářet problémy, protože obsahují spoustu informací o vás a vašich blízkých. Dochází pak k rozesílání phishingových zpráv z vašeho účtu.

Co dělat, když obdržím informaci, že moje uživatelské jméno či heslo bylo zneužito?

Neprodleně změňte heslo. Nové heslo by mělo mít alespoň 8 znaků, použijte alespoň jedno velké písmeno, alespoň jeden znak a alespoň jedno číslo. Vyhněte se vytváření hesel ze jmen svých dětí, manželek/manželů, zvířecích miláčků, data narození a dalších snadno dohledatelných údajů na internetu.

Proč bych měl chránit své uživatelské jméno?

Uživatelské jméno je základním nástrojem, který umožňuje podvodníkům útočit na váš bankovní účet nebo jiné účty. Zcizením uživatelského jména, „pouhé“ emailové adresy, jsou ohroženy všechny informace a osobní data ve všech takových aplikacích.

Co dělat, když zjistím, že bylo zneužito číslo bankovního účtu, ať už v národním či mezinárodním formátu IBAN?

Neprodleně se obraťte na svoji banku a nechte prověřit transakce na svém bankovním účtu, případně v internetbankingové aplikaci prověřte sami historii plateb, zda nedocházelo k neznámým platbám. Zároveň doporučujeme založit účet nový a napadený účet co nejdříve zrušit, aby nemohlo docházet k nelegálním přesunům plateb nebo podvodným platbám a nákupům z vašeho účtu.

Proč si chránit číslo svého bankovního účtu ať již v národním či mezinárodním formátu?

IBAN je mezinárodní formát čísla účtu, a tedy pro IBAN platí to stejné jako pro číslo bankovního účtu v národním formátu. Číslo účtu v domácím formátu se skládá ze dvou částí, oddělených pomlčkou, přičemž první část je nepovinná. V případě, že dojde ke zcizení bankovního účtu, pak přes něj mohou být prováděny nelegální přesuny peněz, nákupy v e-shopech bez vašeho vědomí a další podvodné aktivity.

Zásady bezpečného chování na internetu

Internet a technologie pronikly téměř do každého aspektu našeho každodenního života. To vytvořilo řadu pozitivních vymožeností, ale také nabízí zločincům příležitosti, jak oslovit nové oběti.

Je důležité chránit sebe a své zařízení před zločinci, kteří si přejí jejich využití. Nicméně technologie se neustále vyvíjejí a zločinci vždy hledají nové způsoby, jak s nimi manipulovat, takže musíte vždy zůstat ostražití a přijímat pravidelně nová bezpečnostní opatření.

Zde je několik tipů, jak zůstat v bezpečí. Existuje mnoho hodnotných zdrojů, které nabízejí on-line bezpečnostní poradenství, a doporučujeme použít všechny dostupné informace k ochraně sebe, svojí identity a svých aktivit.

- snížit spam (který může obsahovat viry nebo může být použit pro phishing)
- udržujte svůj spamový filtr zapnutý
- buďte podezíraví u nevyžádaných reklamních kampaní a nabídek
- buďte ve střehu, pokud neznáte odesílatele
- důvěryhodné webové stránky nebo on-line platební zprostředkovatel od vás nikdy nebude požadovat potvrzení citlivých informací, jako jsou hesla nebo podrobnosti o účtu
- okamžitě odstraňte všechny podezřelé spamy a neotvírejte žádné přílohy.

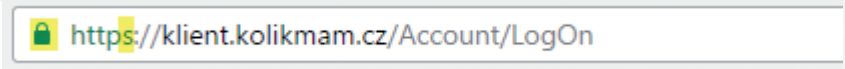
Dávejte si pozor na phishing

Podvodný email se může jevit jako, že pochází z důvěryhodného zdroje. Některé varovné příznaky jsou obsaženy přímo v e-mailu:

- je odeslán z volné emailové adresy, a ne z oficiálního sídla organizace
- uvítání v emailu začíná obecným pozdrav, a není přizpůsoben vašemu jménu
- obsahuje hrozbu, například, že váš účet není zabezpečený nebo se může vypnout
- požaduje osobní informace, jako je uživatelské jméno, heslo nebo bankovní spojení
- obsahuje odkaz na webové stránky s URL (webovou adresu), který je odlišný od oficiální adresy dané organizace.

„Brouzdejte“ bezpečně

- zkontrolujte URL adresu v adresním řádku prohlížeče a podívejte se na případné pravopisné chyby nebo neočekávaná jména či názvy
- buďte podezřívaví, pokud webové stránky neposkytují žádné kontaktní údaje
- dřív než někam vložíte osobní nebo finanční údaje, zkontrolujte, zda jste na zabezpečené lince. Podívejte se na „s“ v https a symbol visacího zámku.



Udržujte svůj počítač v bezpečí před viry a dalšími technickými problémy pomocí následujících nástrojů:

- firewall
- anti-virus software
- OS Update (pro bezpečnostní záplaty a opravy chyb)
- anti-spyware nástroje.

Další kroky, které můžete přijmout v rámci vlastní bezpečnosti online

- pokud máte bezdrátovou síť, zkontrolujte, zda je šifrována
- blokujte v prohlížeči vyskakovací okna nebo zkuste používat různé prohlížeče
- otevírejte přílohy pouze v případě, že jsou zasílané lidmi, které znáte a důvěřujete
- vytvořte silná hesla - alespoň osm znaků dlouhé a obsahující směs velkých a malých písmen, číslic, interpunkčních znamének nebo symbolů
- udržujte vaše hesla v tajnosti, nikdy je nikomu nedávejte.

Slovník pojmů

Adware neboli software podporující reklamu, je software, který automaticky vykresluje reklamy s cílem vytvářet příjmy pro jeho autora. Tyto funkce mohou být navrženy tak, aby analyzovaly, které internetové stránky uživatel navštěvuje a prezentuje mu tak relevantní reklamy o různém typu zboží nebo služeb.

Bitcoin je internetová platební síť a také v této síti používaná kryptoměna.Hlavní unikátností Bitcoinu je jeho plná decentralizace, tedy je navržen tak, aby nikdo, ani autor nebo jiní jednotlivci, skupiny či vlády, nemohl měnu ovlivňovat, padělat, zabavovat účty, ovládat peněžní toky nebo způsobovat inflaci. V síti neexistuje žádný centrální bod, ani nikdo, kdo by mohl o síti rozhodovat. Konečné množství bitcoinů je předem známo a uvolňování bitcoinů do oběhu je definováno ve zdrojovém kódu sítě. V síti probíhají platby za minimální nebo žádné náklady. Bitcoiny mohou být uloženy v osobním počítači ve formě souboru s peněženkou nebo uchovávány pomocí služby třetí strany.

Black market je online tržiště nejčastěji používané pro nelegální prodej drog provozované jako skrytý web, což umožňuje anonymní využití. Mezi takové např. patřil např. Silk Road tedy česky hedvábná stezka.

CryptoLocker je trojský kůň, který cílí na počítače s operačním systémem microsoft Windows. Tento typ malware se šíří infikovanými emailovými přílohami a zašifruje obsah na lokálních nebo připojených síťových discích přičemž vydírá uživatele, aby zaplatil např. prostřednictvím bitcoin , jinak se ke svým datům nedostane. Doporučuje se, žádnou platbu neprovádět, neboť ani tak není jisté, že budou data dešifrována případně, že se situace nebude opakovat.

Dark web je www obsah, který existuje na tzv. darknets (síť, která je přístupná jen se speciálním software, často využívá nestandardní protokoly a porty, typicky takovou sítí bývají P2P sítě), který využívá veřejný internet, ale k jeho přístupu je nutný speciální software, konfigurace a autorizace. Dark weby formují deep web, což je část webu, která není indexovaná vyhledávači.

Ddos útok je realizovaný tak, že směrem k napadanému serveru je vysláno obrovské množství požadavků např. o zobrazení webové stránky. K serveru, pokud přímo nezkolabuje, se pak nedostanou legitimní uživatelé (například uživatelé internetového bankovnictví). Útok DDoS je provedený z velkého množství míst, takže není možné útočníka snadno odříznout. A bohužel ani poznat: využívá „anonymitu davu“.

Internetová fóra nebo nástěnky jsou online diskusní stránky, kde lidé nechávají svou konverzaci ve formě zaslaných krátkých zpráv a bývají alespoň po minimální čas archivovány a diskutují v takzvaných vláknech.

IRC neboli Internet Relay Chat je protokol aplikační vrstvy, která usnadňuje komunikaci ve formě textu. Proces chatu pracuje na síťovém modelu klient/server. IRC klienti jsou počítačové programy, které uživatel může nainstalovat do svého systému. Tito klienti komunikují s konverzačním serverem pro přenos zpráv s ostatními klienty. IRC je určen především pro skupinové komunikace v diskuzních fórech, nazývaných kanály, ale také umožňuje one-on-one komunikace prostřednictvím soukromých zpráv, jakož i chatu a přenosu dat, včetně sdílení souborů. Vzhledem ke skutečnosti, že IRC spoje jsou obvykle nešifrované, tak jsou atraktivním cílem pro DoS/DDoS útočníky a hackery.

Malware krátké označení pro škodlivý (**malicious software**), je software používaný k narušení nějaké počítačové operace za účelem získání citlivých informací, přístupů k soukromým počítačům nebo rozesíláním nechtěné reklamy. Malware může být nenápadný, jeho cílem je ukrást informace nebo špehovat uživatele počítačů po delší dobu bez jejich vědomí nebo to může být navrženo tak, aby způsobil nějakou škodu, nebo k vydírání plateb (CryptoLocker). Malware je zastřešující termín používaný pro různé formy škodlivého nebo dotěrného softwaru včetně trojských koní, virů, spyware, adware, scareware a dalšími škodlivými programy.

P2P neboli peer-to-peer označení se dnes vztahuje hlavně na výměnné sítě, prostřednictvím kterých si mnoho uživatelů může vyměňovat data. Dnešní anonymní výměnné sítě umožňují (legální i nelegální) výměnu souborů s prakticky nulovou mírou odpovědnosti jednotlivých uživatelů.

Phishing je pokus získat citlivé informace, jako jsou uživatelská jména, hesla a informace o kreditních kartách či bankovních účtech (a někdy i nepřímo i peněz) vydáváním se za důvěryhodnou entitu v elektronické komunikaci. Phishingové e-maily mohou obsahovat odkazy na webové stránky, které jsou infikovány škodlivým softwarem. Phishing se obvykle provádí pomocí e-mailového spoofingu nebo instant messagingu, jež často směruje uživatele k zadání podrobností na falešné webové stránky, jejichž vzhled a chování jsou téměř totožné s legitimním webem např. jejich internet bankingových aplikací. Uživatelé by neměli používat stejné heslo kdekoli na internetu. Phishing je neustálá hrozba a riziko je ještě větší na sociálních sítích, jako je Facebook, Twitter a Google+.

Scareware je forma škodlivého softwaru, který se využívá k navození šoku, úzkosti nebo pocitu ohrožení tak, aby se uživatel nechat manipulovat ke koupi nežádoucího softwaru. Dále se označení scareware může vztahovat i na všechny aplikace nebo viry, které svými žerty mohou uživatelům úmyslně způsobit úzkost nebo paniku.

Skimming kopírování platebních karet pomocí speciálního snímacího zařízení, které pachatelé umísťují přímo na bankomaty peněžních ústavů. Zloději pak získají informace, díky kterým se mohou pokusit odcizit peníze z účtu poškozeného.

SMiShing SMS phishing nebo-li smishing je forma kriminální činnosti, jejímž cílem je stejně jako u internetového phishingu získat osobní údaje jako např. hesla a další údaje formou krátkých textových zpráv.

Spyware je software, který si klade za cíl shromáždit informace o osobě nebo organizaci bez jejich vědomí a to tak, že mohou posílat tyto informace na jiný subjekt bez souhlasu daného uživatele. „Spyware“ se většinou dělí do čtyř typů: sledování systému, trojské koně, adware a tracking cookies. Spyware se nejčastěji používá pro účely sledování a ukládání pohybu uživatelů Internetu na webu a následném servírování pop-up reklamy. Funkce spyware však mohou přesahovat toto jednoduché sledování. Spyware může shromažďovat téměř jakýkoliv typ dat, včetně osobních informací nebo zvyklostí při internetovém surfování, uživatelské účty a hesla nebo informace o bankovních účetech nebo kreditních kartách

TOR je software umožnující anonymní komunikaci. Tor směruje internetový provoz prostřednictvím bezplatné dobrovolnické sítě. Tor je využíván k zabezpečení soukromí uživatelů, stejně jako jejich svobody a schopnosti vést důvěrnou komunikaci tím, že drží své internetové aktivity mimo sledování a odposlech. Tor může také poskytnout anonymitu webových stránek a dalších serverů. Servery nakonfigurováne pro příjem příchozích připojení pouze přes Tor se nazývají skryté služby. Jednou z anonymních/skrytých webových stránek byl např. black market reloaded, přes který se prodávaly drogy a jiné nelegální zboží **včetně kradených kreditních karet**.

CRIF – Czech Credit Bureau, a. s.
Štětkova 1638/18
140 00 Praha 4
Česká republika

Tel.: +420 844 111 777
info@kolikmam.cz

netagent.kolikmam.cz