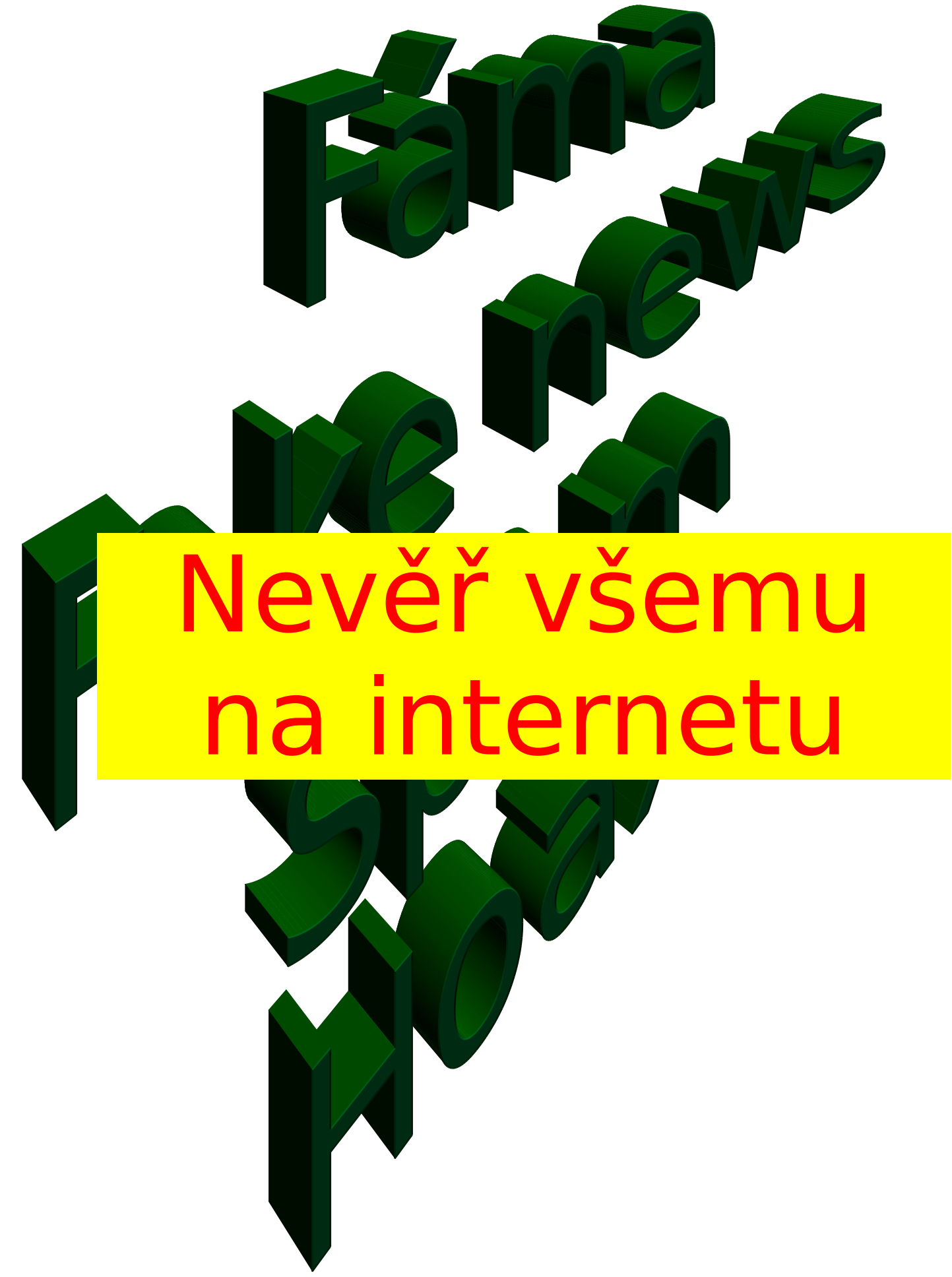
Fake news
Fáma
Nevěř všemu
na internetu

Fáma

Fáma (také **domněnka** či **zvěst**, anglicky *rumour* či *rumor*) je téměř vždy smyšlená, polopravdivá či nepravdivá informace o člověku, jevu či události ze všech sfér soudobého či současného života.

Definice fámy

Fáma je uvěřitelná informace nejistého původu, která se spontánně šíří mezi lidmi, a která se zpravidla vztahuje k nějaké aktuální události, diskusi či otázce. Různí se definice etnologů, sociologů či psychologů. Někteří tvrdí, že ji jednoznačně definovat nelze.

- G. W. Allport, L. Postman: „Fáma je sdělení, které se týká aktuálních událostí, kterému se má věřit a které se šíří od osoby k osobě zpravidla ústně. Neobsahuje údaje, podle nichž by se dala posoudit jeho pravdivost.“
- R. Knapp: „Fáma je informace předkládaná k věření. Souvisí s aktuálním děním a je rozšiřována bez oficiálního ověření.“
- W. Peterson, N. Gist: „Fáma je neověřená zpráva nebo vysvětlení rozšířené mezi lidmi. Týká se předmětu, události nebo otázky veřejného zájmu.“
- T. Shibutani: „Fáma je výsledkem společného intelektuálního úsilí společenské skupiny dospět k uspokojivému výkladu události.“

Historie

Fáma je podle Jeana-Noëla Kapferera nejstarším sdělovacím prostředkem. Fáma jako narativní žánr byl znám již ve starověkém Řecku. Pod jménem Pheme se zde vyskytuje postava bohyně nejistého původu, která dodává naději. V antickém Římě najdeme zmínky o této bytosti zejména u Vergilia a Ovidia, v satirické formě také u Petronia. Římané jí již připisují také negativní vlastnosti.

Publius Vergilius Maro popsal fámu v díle Aeneis takto:

Pověst, jíž žádná z příšer se rychlostí nemůže rovnat,
poněvadž rychlostí roste a chůzí nabývá síly,
nesmělá zprvu a malá, však záhy se do výše zvedne,
nohama po zemi kráčí a v mracích ukrývá hlavu.
Neboť prý rodička Zem, jsouc na bohy zjitřena hněvem,
po Koiu, po Enkeladu ji zrodila, poslední sestru,
nohou nadmíru rychlých a křídel hbitosti velké,
netvor to velký, hrozný – a kolik má po těle peří,
tolik – divocí div – má nad nimi slídivých očí,
jazyků v mluvících ústech a tolikéž vztyčených uší.
Uprostřed nebe a země se temnem za noci vznáší,
šustí a k sladkému spánku svá víčka nesklání nikdy.
Za světla sedí a slídí buď na střechách vysokých domů
anebo na vrchu věží a děsí veliká města,
výmysly mluví i lež, však také zvěstuje pravdu.

Publius Ovidius Naso ji ve svém díle *Proměny* popisuje jako příbytek, kde je vše vidět a slyšet. Bytosti, které tento příbytek obývají, vždy vše, co uslyší, pozmění a pošlou dále.

Personifikace

Od starověku byla fáma – podobně jako pomluva – personifikována jako negativní činitel, nejčastěji zlou starou ošklivou ženou s klubkem hadů ve vlasech či jedovatým hadem v ústech. Jindy má dlouhé uši, aby vše slyšela. Jindy mívá křídla, aby se mohla rychle rozlétnout, a vytrubuje své zvěsti na trubku. Nejoblíbenější bývala její vyobrazení v době renesance a baroka, například v Kuksu je socha od Matyáše Bernarda Brauna.

Fáma ovšem může mít také pozitivní smysl. Pak bývala - opět často v době barokní, ale i v 19.století - vyobrazena jako okřídlená vznášející se mladá žena s trubkou u úst, ztotožněná někdy s Nesmrtelností. V tom případě jejím protějškem bývala *Sláva* s věncem v rukou věnčící triumfujícího (a nejčastěji zemřelého) hrdinu. Tak například anonymní veršovaná kniha z roku 1641, oslavující mučedníka Jana Nepomuckého, nese titul *Fama posthuma* - *Posmrtná pověst*.

Od 1940 do současnosti

Systematický výzkum fámy začal v období druhé světové války v USA, kdy se především zkoumala nepřátelská propaganda. V roce 1944 vyšla kniha Roberta Knappa Psychologie fámy. Knapp v ní rozdělil fámy, které se v USA vyskytovaly v průběhu druhé světové války, na tři základní skupiny:

- Bogies („strašáci“) – fámy, které předpovídaly útok Japonců na území USA atd. Ze všech fám tvořily bogies 25%.
- Pipe dreams („vzdušné zámky“) – fámy ohlašující brzký konec války atd. Celkem 5%
- Wedge drivers („rozdělující“) – fámy, které „rozdělovaly“ obyvatele. Obviňovaly evropské přistěhovalce z kolaborantství atd. Celkem 65% všech fám.
- + 5% neklasifikovaných fám.

Jako první také zdůraznil, že fáma je schopna ventilovat a uspokojovat emoční potřeby obyvatelstva.

V roce 1988 byla založena Mezinárodní společnost pro výzkum současné pověsti (International Society for Contemporary Legend Research – ISCLR), která se studiem fám zabývá vedle jejích příbuzných žánrů, především pak tedy současné pověsti.

Prvními vědci, kteří se studiem fámy zabývali, byli psychologové. Následovali sociologové, od 80. let pak etnologové, kteří navázali na své dřívější výzkumy městských legend.

V současnosti fáma převládá jako forma folkloru. Je to šíření neověřené informace o aktuálních problémech ze všech společenských vrstev a ze všech sfér našeho života. Od městské pověsti (z anglického *urban legend*) se liší stručností (nemá děj), naléhavostí a rychlostí. Účelem fámy je varovat (často falešně) nebo diskreditovat. Oproti tomu současná pověst většinou vypráví příběh, který má za úkol pobavit či šokovat. Obě pocházejí z neověřených zdrojů (někdy z oficiálních médií, bulvárního vysílání, tisku apod.) Fáma se šíří jednak orálně, významným médiem je také internet, nejčastěji sociální sítě.

Některé současné fámy v Česku

- O škvorovi, který vleze člověku do ucha a pomocí zadečkových klíštěk prokousne bubínek.
- O injekčních stříkačkách umístěných v madlech eskalátorů nebo v sedadlech autobusů, které nakazí lidi virem HIV.
- O Romech, kteří na koupalištích lepí na tobogany žiletky. Zajímavé je, že stejná fáma se s obměnou aktérů vyskytuje i v zahraničí: V Británii je lepí Pákistánci, v USA Mexičané, v Německu Turci…
- O romských rodinách, které dostávají zadarmo léky v lékárně, kočárky atd.
- Ekologové uměle chovají zmije a vysazují je z letadel.

Fake news

Fake news (česky „**podvržené zprávy**“) jsou žánr tzv. žluté žurnalistiky (bulvární či neetické novinařiny) úmyslně šířící dezinformace či hoaxy za účelem ovlivnit a zmanipulovat příjemce. Do žánru fake news nepatří parodie či satira. Doménou fake news v současné době bývají dezinformační weby, sociální sítě, šířeny ale mohou být prostřednictvím všech mediálních platforem. Původem tak sahají i do doby vynalezení knihtisku.

Vznik fake news

Spojení „fake news“ je neologismus. Jeho používání, které je často i chybné, může přinášet i problémy. Fake news jsou smyšleným dílem. Každá fake news musí být uvěřitelná, proto se musí zakládat na částečně věrohodných informacích. To také zahrnuje její přizpůsobení místu kulturnímu kontextu zveřejnění. Na obdobných principech se tvoří i tzv. urban legends, které ale na rozdíl od fake news mají primární cíl pobavit, nikoliv zmanipulovat příjemce. Sdělení fake news mají většinou bulvární charakter a jsou formulována tak, aby vzbudila emoce.

První, kdo podvrženou zprávu zveřejní je typicky nepříliš známé internetové médium, respektive dezinformační web. Autor doufá, že zpráva se z jeho webu dostane do mainstreamových médií. Současně jsou fake news sdíleny na sociální síť (typicky facebook). Na sociální síti pak dezinformační web šíří fake news nejen za pomoci své vlastní stránky, ale také přes několik spřízněných stránek s názvy jako např.: milujeme svět, sdílíme pravdu, ty nejlepší typy, které se starají o šíření fake news. Tyto tři konkrétně jmenované stránky využívá pro šíření svých zpráv český dezinformační web AC24.cz.

Studie z MIT, která zkoumala šíření ověřeně nepravdivých městských legend na sociální síti twitter, prokázala, že se

EU chce zrušit písmeno Ř, prý kvůli zjednodušení

Řehořové, Bedřišky a Jindřichové se budou muset připravit na velké změny, letní jazykové kotrmelce se však budou týkat každého z nás. Evropská lingvistická rada spadající pod EU jednohlasně rozhodla, že od letošního července ruší písmeno Ř.“ A to proto, že „téměř nikdo tohle písmeno v Evropě nepoužívá a pro každého, kdo neovládá češtinu, je jeho výslovnost extrémně obtížná. ELR chce zjednodušit komunikaci tím, že problematické znaky a hlásky bude postupně eliminovat,“ vysvětluje jazykovědec František Měch.
Vedle odstranění problematického písmene má ale celá akce ještě jeden důvod. Evropská unie chce pečlivě sledovat reakce Čechů a podle toho urychlit, oddálit, nebo třeba i úplně zastavit snahu odstranit E s háčkem. Jeho eliminace sice není na pořadu dne, ale v roce 2020 by mělo na půdě europarlamentu proběhnout další jednání Evropské lingvistické rady a je velká šance, že se bude probírat i tenhle český potížista.
(Jedná se o satirickou zprávu z webu www.pravdive-zpravy.cz, kterou však převzala velká část českých médií a která byla sdílena také vrcholnými politiky – např. senátorem Jaroslavem Doubravou. Ten sdělení nijak neověřoval, ani jej to nenapadlo.)
Fake news často pracují s mediálními stereotypy a zjednodušeným – generalizovaným – výkladem světa. Využívají stereotypy náboženské (muslimové jako teroristé), rasové a národnostní (Romové jako zloději, černoši jako sexuální predátoři, Vietnamci jako prodejci na tržnici), genderové (hloupé blondýny, pracující muž, žena v domácnosti), stereotypy vázané na vzdělání (povýšení vysokoškoláci), stereotypy vázané na bydliště (vidláci z venkova), stereotypy vázané na sexualitu, sociální statut rodiny, politické zaměření apod. Fake news rovněž využívají závažných celosvětových témat, jako jsou např. migrace a terorismus (hordy migrantů čekají za hranicemi).

falešné zprávy šířily rychleji než pravdivé. Některé zprávy se šířily až 6x rychleji. Zatímco podvržené zprávy z oblasti vědy, podnikání nebo zábavy se šířily jen o trochu rychleji než pravdivé zpravodajství, skokový rozdíl v množství sdílení byl zaznamenán, pokud se zprávy týkaly politiky.

Podle studie Kolumbijské univerzity lidé, pokud jsou (i nepřímo) ve skupině, mají tendenci si příliš neověřovat zprávy. To vede například právě k šíření dezinformací na sociálních sítích. Fake news ale šíří menšina uživatelů a více k tomu tíhnou starší lidé nad 65 let věku. Před sdílením fake news by tak pomohlo, kdyby si každý informaci nejprve ověřil.

Příklady fake news

Komentátor v *Guardianu* a vysoce postavený člen královské rodiny Kataru označili za *fake news* tvrzení Spojených států a jejich spojenců z roku 2003, že Irák krátce před Američany vedenou invazí do Iráku vlastnil zbraně hromadného ničení. Později se toto tvrzení americké vlády a amerických tajných služeb ukázalo jako nepravdivé. Za *fake news* bylo v roce 2016 komentátorem ruské státní televizní stanice RT Neilem Clarkem označeno také tvrzení, které se objevilo před vojenskou invervencí v Libyi, že se libyjský režim chystal zmasakrovat obyvatelstvo Benghází. Tvrzení o chystaném masakru bylo později označeno za nepodložené Dolní sněmovnou Spojeného království.

Dezinformační web po demonstraci na Národní třídě dne 17. listopadu 2014, kdy účastníci demonstrace vystavili prezidentu Miloši Zemanovi červenou kartu, vytvořil článek o tom, že zmíněnou demonstraci organizovalo velvyslanectví USA v ČR. Tvrzení bylo vystavěno na základě fotografie účastnice demonstrace rozdávající červené karty kamarádkám. Dezinformační web z profilu účastnice na facebooku zjistil, že žena pracovala jako lektorka angličtiny pro velvyslanectví USA v Praze. Na této informaci dezinformační web vystavěl fake news o organizaci demonstrace americkou ambasádou.

V roce 2014 Rusko použilo státem kontrolovaná média, například síť RT, k rozšiřování dezinformací o okolnostech ruské okupace Krymu a sestřelu letu Malaysia Airlines 17 proruskými povstalci.

Volby prezidenta Francie 2017, ve kterých zvítězil Emmanuel Macron, také byly ovlivňovány fake news. Tchajwanská prezidentka Cchaj Jing-wen obvinila vládou placené trolly z Číny označované jako 50-cent army z šíření *fake news* na sociálních sítích ve snaze podpořit před tchajwanskými volbami v listopadu 2018 kandidáty nakloněné Pekingu. Saúdská Arábie byla obviněna z šíření falešných zpráv, které se týkaly sporu s Kanadou a zavražděného saudského novináře Džamála Chášukdžího.

Koncem roku 2018 sám týdeník *Der Spiegel* odhalil, že jeden z jeho novinářů Claas Relotius, který za své články získal v průběhu předchozích let mnohá ocenění, například cenu CNN „Novinář roku 2014“, si ve skutečnosti řadu svých článků zásadním způsobem domýšlel a dokresloval, vymýšlel si celé pasáže a příběhy a citoval vymyšlené osoby. Pro *Spiegel* Relotius napsal od roku 2011 téměř 60 článků. Rok před vypuknutím aféry se několik občanů amerického města Fergus Falls snažilo kontaktovat redakci *Der Spiegelu* na Twitteru, aby upozornili na spoustu nepravd v Relotiusově článku o jejich městě. Redakce nedostatky v Relotiusových textech přiznala pět týdnů po internímu upozornění jeho kolegy Juana Morena, který musel několik týdnů

čelit hrozbám a nátlaku, a vlastním rešerším, autor manipulace se přiznal a redakci opustil.

Americký prezident Donald Trump opakovaně obvinil z šíření *fake news* některá americká média, například televizi CNN či deníky *The New York Times* či *The Washington Post*. Amerického prezidenta podpořil polský prezident Andrzej Duda, který napsal: „Musíme nadále bojovat proti tomuto jevu. Polsko zažívá moc falešných zpráv z první ruky. Mnoho evropských a dokonce i amerických úředníků utváří své názory na Polsko na základě neúprosného toku falešných zpráv.“ V prosinci 2016 byl za šíření *fake news* kritizován americký deník *Washington Post*, poté co otiskl nepravdivou zprávu, že hackeři z Ruska pronikli do centrální elektrizační soustavy Spojených států. Naopak západní média za jedny z častých šiřitelů *fake news* uvádějí zpravodajské zdroje rozšiřující ruskou propagandu.

Umělá inteligence je schopna rozpoznávat i generovat uvěřitelná fake news.

Reakce

Proti fake news se staví například Wikitribune. V Česku se jimi zabývá Centrum proti terorismu a hybridním hrozbám či projekt Manipulátoři.cz. Proti šiřitelům dezinformací a falešných zpráv (v tomto kontextu označeným jako „trollové“) rovněž začali vystupovat někteří anonymní samozvaní bojovníci nazývající se po vzoru fantasy žargonu za „elfy“.

Podle skupiny analytiků z Yaleovy univerzity jsou opatření Facebooku nedostatečná.

V roce 2017 byl výraz *fake news* vyhlášen Collinsovým výkladovým slovníkem za slovo roku.

Vláda Sociálních demokratů ve Švédsku varovala před šířením dezinformací a propagandy ze strany Ruska před parlamentními volbami ve Švédsku v roce 2018. Vyškolila proto úředníky a do švédských domácností distribuovala miliony letáků varujících před hrozbou. Po volbách provedl Oxford Internet Institute, který je součastí Oxfordské univerzity, analýzu šíření falešných zpráv a dezinformací ve Švédsku a zjistil, že okolo 80% hlavních zdrojů bylo domácího švédského původu a ruské zdroje představovaly pouhé 1% URL adres, ze kterých byly šířeny falešné zprávy.

Americká kyberbezpečnostní firma New Knowledge, jejíž zprávu o údajném ruském působení a ovlivňován voleb zveřejnil zpravodajský výbor amerického Senátu jako důkaz vlivu ruských *fake news* a dezinformací ve Spojených státech, byla v prosinci 2018 obviněna, že ve spolupráci se společností napojenou na Demokraty vytvořila tisíce falešných ruských trollů na Facebooku a Twitteru, kteří měli během senátních voleb v Alabamě vytvořit dojem, že Rusové podporují republikánského kandidáta Roye Moora. Moore nakonec volby do Senátu prohrál.

Spam

Spam je nevyžádané sdělení masově šířené internetem. Původně se používalo především pro nevyžádané reklamní e-maily, postupem času tento fenomén postihl i ostatní druhy internetové komunikace – např. diskuzní fóra, komentáře nebo instant messaging. Používá se též zkratka **UBE/UCE** (Unsolicited Bulk/Commercial Email).

Pro opak spamu, tj. poštu, která je zaslána konkrétní osobou se specifickým jednorázovým účelem a adresát ji považuje za žádoucí, se řidčeji používá termín ham (anglicky šunka).

Původ (etymologie) termínu

Název pochází ze značky amerických konzerv lančmítu. Slovo vzniklo jako zkratka ze slov spiced ham - okořeněná šunka a tyto konzervy se vyrábí od 30. let 20. století dodnes. V současnosti ale výrobce trvá na psaní velkým písmem - SPAM. V období 2. světové války byla hojně rozšířená a stále méně oblíbená ve Velké Británii.

Proto se spam objevuje v závěrečném skeči 25. dílu televizního seriálu *Monty Pythonův létající cirkus*, kde všechny položky jídelního lístku v restauraci obsahují spam, i mnohokrát opakovaně, a spory zákazníků s číšnicí o objednávky přerušuje skupina Vikingů zpívajících „Spam, spam, spam…“

Označení tak bylo přijato nejprve pro praktiku mnohonásobného rozesílání téže zprávy na Usenetu, ale pak se význam posunul pro zneužívání skupin k šíření různých nepřípadných textů a přímo reklamy a zachoval se i poté, co se těžiště takových aktivit přesunulo do e-mailu.

V jiných výkladech je uváděn výraz SPAM jako zkratka z anglického *Shit Posing As Mail*, což v nevulgárním překladu znamená *Odpad jevící se jako zpráva*.

Historie spamu

Historie spamu (zahraničí)

Spam existuje déle nežli internet. První zmínka o spamu pochází z 19. století. V tomto období povolila telegrafická firma Western Union zasílání zpráv do více destinací. V roce 1864 byl zaznamenán první hromadě odeslaný nežádoucí telegram. To mělo za následek, že až do období velké hospodářské krize byli bohatí obyvatelé Severní Ameriky zahlcováni nejasnými investičními nabídkami. V Evropě tento problém neexistoval v takovém měřítku jako v Americe, jelikož telegrafii zde regulovaly národní poštovní kanceláře.

Internet byl původně armádní projekt a nikdo nepředpokládal, že bude určen k vydělávání peněz. Zřejmě první internetový spam napsal zaměstnanec Digital Equipment Corporation. Byl zaslán 1. května 1978 na adresy tehdejší sítě ARPANET a obsahoval informace o prezentaci produktů této společnosti. Dalším spamem byla zpráva podepsaná jistým Davem Rhodesem a rozeslaná do diskusních skupin sítě USENET. Předmětem této zprávy bylo MAKE.MONEY.FAST!! (vydělávej rychle peníze).

Roku 1993 se muž jménem Richard Depew rozhodl představit svoji novou představu o fungování USENETu. Tato idea nebyla na první pohled špatná.

Navrhoval přidat moderátorům konferencí možnost stanovit pravidla a zrušit příspěvky, které je poruší. Koncem března si Richard hrál se svým programem nazvaným ARMM, jehož úkolem bylo spravovat diskuse podle jím navrženého způsobu. Došlo k nehodě a jeho software zahltil diskusní skupinu news.admin.policy více než 200 příspěvky. Samotný Richard Depew se za své počínání omluvil s tím, že se skutečně jednalo o nehodu.

Jedním z dalších spamů byla zpráva zaslaná 18. ledna 1994 s předmětem Global Alert For All: Jesus is Coming Soon (Upozornění pro všechny: Ježíš brzy přijde). Jednalo se o nábožensky laděný text, který ukazoval souvislosti mezi zemětřesením v Los Angeles v Kalifornii, záplavami v Evropě, válkou v Jugoslávii a dalšími katastrofami.

Skutečně masivním spamem byla nevyžádaná zpráva Green Card Lottery, kterou zaslali 5. března 1994 právnická společnost Cantor a Siegel. Zpráva zahltila 6 000 diskusních skupin. V jejich stopách později kráčel další spammer Michael Wolff, který pomocí nevyžádaných zpráv nabízel svoji knihu o internetovém chatu. Každý výskyt spamu doprovázely mohutné diskuse o etice chování na Internetu (tzv. Netiketa).

Historie spamu (Česko), příklady

Tvujdum.cz

Zřejmě největší negativní reakci uživatelů vyvolal hromadný spam společnosti Media Online, s. r. o. Firma provozující server o bydlení Tvujdum.cz v něm oznamovala novinky a seznamovala čtenáře se svým webem. Spam obsahoval přílohu ve formátu HTML, což snížilo reklamní dopad celé akce. Uživatele také pobouřila výmluva uvedená v textu e-mailu:

Tento e-mail je Vám zasílán na základě pečlivého výběru a globální rešerše uživatelů, kteří své webové stránky věnují tematice bydlení, stavebnictví. Předem se omlouváme za nevyžádaný e-mail.

Ředitel společnosti se původně pokoušel masivní spamování obhajovat: „Dovoluji si Vás ujistit, že v žádném případě nešlo o masové rozesílání spamů, jak některé servery uvádějí, neboť množství připravených e-mailů bylo vůči českému internetu zanedbatelné.“ Později vydala společnost tiskovou zprávu, v níž se omluvila všem uživatelům. Výkonný ředitel společnosti navíc přislíbil finanční dar v hodnotě 50 000 Kč nadaci Člověk v tísni.

Přesto se uživatelé českého internetu semkli v boji proti spamu a podle serveru Lupa.cz zaslalo 30 lidí stížnost na společnost Media Online. Některé stížnosti adresované živnostenskému odboru Magistrátu hlavního města Prahy byly podepsány jen přezdívkou. Úřad nakonec udělil spamující firmě pokutu ve výši několika desítek tisíc korun.

Aleš Slabý

Jedním z dalších prvních českých rozesilatelů nevyžádaných zpráv byl student a podnikatel Aleš Slabý. Veřejnost poprvé masivně oslovil s nevyžádanou nabídkou na klonování SIM karet. Reklamu na svůj produkt také zřejmě vkládal do diskusí na známých českých serverech. Nebyl rozhodně prvním ani posledním spammerem, který opakovaně porušoval tehdejší Zákon o regulaci reklamy, nikdy mu to však nebylo prokázáno. Aktuálně nyní již

spam podle svého tvrzení v rozhovoru na Živě.cz (rok 2004) nerozesílá a věnuje se jiné oblasti obchodu a vlastní několik velkých společností.

Zákony proti spamu

Nynější zákony

Od 7. září 2004 začal platit nový Zákon o některých službách informační společnosti (č. 480/2004 Sb.), který problematiku spamu upravuje a vyžaduje prokazatelný souhlas příjemce zprávy. Dohledem nad dodržováním zákona byl pověřen Úřad pro ochranu osobních údajů. Tento zákon byl postupně novelizován, a to v letech 2005, 2006, 2007 a naposledy v roce 2011.

Zákon byl vytvořen podle směrnice Evropského společenství č. 2000/31/ES. Spam definuje jako obchodní sdělení, což jsou *všechny formy sdělení určeného k přímé či nepřímé podpoře zboží či služeb nebo image podniku fyzické či právnické osoby*. Zákon řeší nejen internetový spam, ale také jiné formy elektronické komunikace (SMS, telemarketing).

Podle zákona se za obchodní sdělení nepovažují údaje umožňující přímý přístup k informacím o činnosti fyzické či právnické osoby nebo podniku, zejména doménové jméno nebo adresa elektronické pošty; za obchodní sdělení se dále nepovažují údaje týkající se zboží, služeb nebo image fyzické či právnické osoby nebo podniku, získané uživatelem nezávisle.

Obchodní sdělení může prodejce zaslat, když:

a) je adresátem jeho zákazník, i) který zasílání podobných sdělení v minulosti neodmítl, ii) sdělení týká obdobného zboží či služeb,

b) adresát obchodníkovi poskytl informovaný souhlas.

Informovaný souhlas

Informovaný souhlas prodejce nemůže získat zasláním e-mailu obsahujícího jeho základní informace. Tento způsob informování byl sice zákonem vyňat z definice obchodního sdělení, ale podle současné legislativy neobsahuje taková zpráva dostatek informací. Informovaný souhlas k zasílání obchodního sdělení lze ale například získat pomocí formuláře na webových stránkách prodejce.

Cílem tohoto odstavce bylo přenesení nákladů za rozesílání spamu na odesílatele. Spam podle zákona není například e-mail ve tvaru „Podívejte se na www.obchodni-nabidka.cz“ a dále politická či náboženská sdělení. Někteří čeští publicisté proto tvrdí, že nový zákon legalizoval spam a vyčítají ministerstvu přílišnou benevolenci.

Dozorem nad dodržováním zákona byl pověřen Úřad pro ochranu osobních údajů. Důvodem pověření jsou vyšší pravomoce úřadu.

Spam a Evropská unie

Členství České republiky v EU přineslo v boji proti spamu výhodu. Nově je možné postihnout odesílatele obchodního sdělení v případě, že firma či subjekt sídlí v některé ze zemí EU. Většina spamu však přichází z jiných částí světa a vymáhání práva je proto složitější a prakticky nemožné.

Dřívější zákony proti spamu

Česká republika neměla dlouho žádný zvláštní zákon, který by výrazně omezoval zasílání nevyžádaných reklamních e-mailových zpráv. Opravdu palčivé případy proto řešili úředníci živnostenských úřadů podle Zákona o regulaci reklamy (sb. 138/2002, částka 57/2002, datum 15. 4. 2002). Podle § 2, bod e) se zakazovalo šíření nevyžádané reklamy, *pokud vede k výdajům adresáta nebo pokud adresáta obtěžuje.* Úřad mohl potrestat porušení zákona udělením pokuty až do výše dvou milionů korun.

Dalším problémem byly omezené pravomoci pověřených úřadů. Pokud byl odesílatel anebo příjemce spamu připojen prostřednictvím mobilního operátora, nemohl úřad zahájit správní řízení. Ve svém dopise úřad trpělivě vysvětloval důvody, proč nemůže vyšetřit porušení zákona: *„Vzhledem k tomu, že živnostenské úřady nejsou osobou oprávněnou k získání předmětu, který tvoří telekomunikační tajemství, nelze nám požadované údaje sdělit. Na podkladě uvedených skutečností Vám však nyní musíme sdělit, že danou věc není možno řešit ve správním řízení, jelikož se v současné situaci nedal zjistit přesně a úplně skutečný stav věci.“*

Úřad také postupoval nejednotně. Například v kauze Dimar, s. r. o., doložil postupně stěžovatel veškeré další podklady. Úřad si pouze vyžádal stanovisko jednatele společnosti a uzavřel celou záležitost, aniž by zahájil správní řízení. Když se poškozený znovu domáhal zahájení správního řízení a poukazoval na porušení zákona, úředníci mu ve své odpovědi vysvětlili, že je výhradně na jejich posouzení, jestli bude případ udělena pokuta a firma potrestána za porušení zákona. Později byl stěžovatel informován, že se čeká na vyjádření soudního znalce, které úřad dosud neobdržel

Problém byl později částečně vyřešen přijetím zákona o některých službách informační společnosti (č. 480/2004).

Obrana před spamem

Ochrana emailových adres na straně uživatele

E-mailové adresy do spamových databází jsou získávány mj. pomocí robotů, kteří procházejí webové stránky a sbírají e-mailové adresy na nich uvedené. Roboty se zpravidla nezatěžují hlubší analýzou zdrojového kódu a sbírají vše, co vypadá jako e-mailová adresa – tedy posloupnost písmen, číslic, pomlček a teček, která obsahuje zavináč. Proto se doporučuje vyhnout psaní e-mailové adresy přímo na webovou stránku a raději ji opsat nějakým, pro člověka srozumitelným, způsobem – např. **jmeno (zavinac) domena.cz**.

Doporučuje se vždy dobře zvážit, zda je vhodné či nutné určitému subjektu svůj e-mail svěřit (týká se především webových stránek, různých registrací, upozorňování). I v případě seriozních subjektů nelze nikdy vyloučit únik informací a zneužití třetí stranou. Pro různé registrace, zasílání informací atd. se doporučuje mít specializovaný e-mail (s případným přeposíláním).

E-mailové adresy pro databáze pro rozesílání spamu můžou být získávány také pomocí virů, je proto důležité znát základní pravidla pro chování na internetu a mít počítač proti virům dobře zabezpečený.

Na adresy, z nichž je spam poslán, by se nemělo žádným způsobem reagovat a neklikat na žádný z odkazů v e-mailu obsažených, neboť tím je spamerovi pouze potvrzeno, že elektronická adresa je funkční a schránku někdo vybírá.

Adresa, z níž je spam poslán, často není pravá a často se mění; může jít i o zfalšovanou adresu jiného člověka, jenž s rozesláním e-mailu nemá nic společného.

Spamovací robot však mailové adresy může získat rovněž sledováním odpovědí vzdálených SMTP serverů. Provádějí na vzdálený poštovní server tzv. slovníkový útok, kdy se pokouší doručit e-mail na adresy složené z obvyklých jmen a příjmení, oblíbených názvů a přezdívek (svoboda, novak, standik atd.). Tyto adresy jsou proto ve větším ohrožení, jako protiopatření se doporučuje např. rozšíření adresy o další znaky (xsvoboda).

U tzv. hoaxu (řetězového dopisu obsahujícího často žádost o pomoc a další rozeslání) je vhodné odesílatele upozornit na omyl a e-mail dále nerozesílat (pokud je v e-mailu obsažena žádost o hromadné rozeslání současně s žádostí o pomoc nebo o podporu někoho, nebo něčeho, jde většinou o podvod, nebo hloupý vtip).

Opatření omezující rozesílání spamu

Většina spamu je rozesílána distribuovaně z počítačů napadených počítačovým virem nebo červem. Vir nebo červ často na počítači otevírá tzv. zadní vrátka (backdoor), která umožňují útočníkovi počítač dálkově ovládat a zneužít jej mj. pro rozesílání spamu. Rozesílací robot i databáze adres může být na napadený počítač zaslána ad hoc, rozesílání nemusí probíhat neustále.

Obranou proti distribuovanému rozesílání je klasická antivirová ochrana. Pro správce sítě je důležité, aby uměl napadený počítač lokalizovat a izolovat.

Další možnost jak ztížit rozesílání spamu je neprovozovat SMTP server jako tzv. open relay. SMTP server, který funguje jako open relay, převezme k dopravě jakýkoli dopis bez ohledu na odesílatele i adresáta. Open relay usnadňuje rozesílání spamu tím, že umožňuje přijmout dopis (spam) odkudkoli a dopravit jej kamkoli, často je jeden dopis adresován na stovky cílových adres. Tím jednak snižuje zátěž na straně spammerova rozesílacího robota, jednak se průchodem přes open relay zamaskuje IP adresa, odkud dopis přišel, což silně ztěžuje filtraci spamu na straně cílového SMTP serveru.

SMTP server by měl být konfigurován tak, aby nepřebíral k dopravě dopisy, které přicházejí z vnějšku domény (domén) a nemají adresáta uvnitř domény, kterou server pokládá za „vlastní“. Příklad: SMTP server pro doménu firma.cz propustí pouze dopisy, které v doméně firma.cz začínají nebo končí.

Spamové pasti

Firmy zabývající se počítačovou bezpečností vytvářejí falešné emailové adresy, které zobrazují na místech, kde je může najít jen robot při prohledávání stránek, ale ne lidská obsluha. Spammeři pak na takové adresy posílají spam, čímž se odhalí. Ve spamovou past se promění i opuštěné mailové schránky u některých poskytovatelů mailových služeb.

Filtrace podle způsobu dopravy

Blacklisting

Blacklisting rozhoduje, zda dopis je nebo není spam, podle adresy odesílatele (která může být zfalšována), nebo lépe podle IP adresy, ze které dopis přišel na cílový SMTP server. Blacklisty obsahující IP adresy, ze kterých

bylo zaznamenáno rozesílání spamu, bývají zveřejňovány nejčastěji pomocí systému DNS. Výskyt adresy v blacklistu může mít za následek buď přímé odmítnutí (nepřevzetí) dopisu ještě během SMTP relace, nebo může být informace z blacklistu použita jako dodatečná informace při následné filtraci podle obsahu.

Greylisting

Podrobnější informace naleznete v článku Greylisting.

Greylisting rozhoduje také podle IP adresy a emailové adresy odesílatele a adresáta, ale dělá to dynamicky. SMTP server, který provozuje greylisting, udržuje databázi, kde pro trojici (IP adresa, odesílatel, příjemce) je uvedeno, zda dopis s těmito atributy má být převzat k dopravě, nebo zda jeho převzetí má být *dočasně* odmítnuto. První dopis je odmítnut a je zaznamenán čas, kdy k tomu došlo. Po určitou dobu (typicky několik desítek minut) pak jsou dopisy s týmiž atributy odmítány. Po uplynutí této doby, pokud se původní SMTP server stále pokouší o odeslání dopisu, je záznam v databázi potvrzen a dopisy jsou naopak přijímány a dopravovány bez zdržení. Po další době (typicky několik málo týdnů) je záznam z databáze odstraněn, takže příští dopis bude opět pozdržen. K odstranění záznamu z databáze dojde také v případě, že v příslušném intervalu, kdy byly dopisy odmítány, se nepokusí původní SMTP server o znovudoručení.

Tato metoda využívá faktu, že protokol SMTP rozlišuje chyby trvalé, jejichž číselný kód začíná číslicí 5, a chyby dočasné s kódem začínajícím číslicí 4. V případě dočasné chyby má odesílající SMTP server dopis uložit do fronty a pokusy o odeslání opakovat (typicky po několika málo desítkách minut). Robot rozesílající spam však často chyby neošetřuje a snaží se všechny dopisy rozeslat co nejrychleji, neboť je možné, že před případným dalším (nebo novým) pokusem o rozeslání, již bude spamerova IP adresa zveřejněna v některém blacklistu. Proto k druhému pokusu již nedojde.

Greylisting se zpravidla používá jako předstupeň před filtrováním podle obsahu a výrazně zvyšuje jeho účinnost. Nevýhodou greylistingu je občasné zdržení dopisu a možnost, že dopisy mohou dojít v jiném pořadí než byly odeslány. Další nevýhodou je, že některé odesílající SMTP servery jsou chybné a neimplementují frontu dopisů k odeslání.

Filtrace podle obsahu dopisu

Automatické rozpoznávání nemůže z principu fungovat dokonale, protože názor, zda konkrétní dopis je spam je individuální. Přesto filtrování podle obsahu dává použitelné výsledky a hojně se používá. Existují dvě základní metody, některé antispamové programy (např. SpamAssassin) je kombinují.

Filtry založené na pravidlech

Filtry založené na pravidlech vyhledávají v dopisech rysy, které jsou pro spam typické. Jde jednak o některá slova (např. viagra) a slovní spojení, jednak jsou vyhledávány chyby pro spam typické. Příkladem je třeba datum odeslání v budoucnosti, nedovolené znaky v hlavičce, chybně označený MIME-typ zprávy apod. Za každý rozpoznaný rys je dopisu přiděleno bodové ohodnocení, body se zpravidla sečítají a pokud součet přesáhne hranici, je dopis pokládán za spam. Rozpoznávané rysy jsou definovány pomocí pravidel,

která je třeba pravidelně aktualizovat a přizpůsobovat praktikám spammerů. K vytváření a údržbě souboru pravidel je třeba mít znalosti, není to práce pro běžného uživatele, laika.

Filtry založené na učení (bayesovské)

Filtry založené na učení (často nazývané bayesovské) využívají znalosti z oblasti umělé inteligence. V režimu učení se filtru předkládají dopisy explicitně označené jako spam a ham (ne spam), filtr z předložených dopisů extrahuje informace, které si ukládá do databáze. Nejčastěji je dopis rozkládán na slova (popř. jiné úseky textu) a pro jednotlivá slova se statisticky zjišťuje pravděpodobnost, že dopis, který toto slovo obsahuje, je spam. V režimu rozpoznávání pak filtr využívá nashromážděné informace a testovanému dopisu přiřadí pravděpodobnost, že je to spam. Nejčastěji se pro výpočet pravděpodobnosti používá vzorec, který navrhl matematik Bayes. Velkou výhodou je, že filtr může učit i uživatel – laik. Učící se filtry jsou nejúčinnější, učí-li je přímo sami koncoví uživatelé podle svého individuálního názoru, co je spam a co ne. Přesto se bayesovské filtry používají i na serverech, kde učení probíhá pro všechny uživatele serveru společně.

Bayesovský filtr je součástí např. poštovního klienta Mozilla Thunderbird. Příkladem čistě bayesovského filtru pro server je bogofilter.

Ochrana na straně příjemce

Příjemce se může pokusit ověřit, zda přijímaný e-mail byl odeslán z důvěryhodného zdroje pomocí metod SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) a dalších, z nichž však žádná neposkytuje úplné a konečné řešení problémů s příjmem spamu.

Spam v různých médiích

Spam v emailech

Emailový spam spočívá v odesílání velkého množství nevyžádaných emailových zpráv, které často obsahují komerční obsah. Problém emailového spamu se začal objevovat v devadesátých letech, kdy se Internet stal dostupným pro širokou veřejnost. Během dalších let objem spamu v emailech exponenciálně narostl, dnes tvoří přibližně 80–85 % všech odesílaných emailů na světě. Tlak, aby se emailový spam stal nezákonným, byl úspěšný jen v některých zemích, takže spammeři často provozují svou činnost v zemích, kde jim nehrozí problémy se zákonem.

Dnes jsou k rozesílání spamů stále častěji využívány tzv. botnety, což jsou sítě tvořené z viry nebo červy infikovaných osobních počítačů (tzv. zombie) po celém světě. Mnoho moderních červů instaluje do počítače zadní vrátka, která spammerovi umožní přístup k napadenému počítači a použít jej k nekalým účelům, např. k rozesílání spamu. To komplikuje jakékoliv pokusy o kontrolu šíření spamu, jelikož v mnoha případech spam nepochází přímo od spammera, ale z nakaženého počítače.

Instant messaging

Většina Instant messaging (IM) systémů nabízí adresář uživatelů, včetně informací jako je např. věk nebo pohlaví. Inzerenti mohou tyto informace

shromažďovat a uživatelům tak zasílat nežádoucí zprávy obsahující zejména reklamy.

Diskusní fóra

Diskusní spam spočívá ve vytváření zpráv s vloženou reklamou, či jiným nevhodným příspěvkem, na volně dostupných diskusních fórech. Slouží k tomu automatické spamovací roboty (tzv. Spamboty).

Online hry

Mnoho online her umožňuje hráčům vzájemný kontakt přes soukromé zprávy nebo speciální místnosti pro to určené. Jako spam pak můžeme označit opakovaného rozesílání stejné zprávy, rozesílání bezvýznamných, či reklamních zpráv nebo zprávy porušující podmínky poskytování služeb (Terms of service) dané hry. Takový spam je běžný v MMORPG hrách, kde se spammeři snaží vydělat reálné peníze např. za prodej herních předmětů nebo uživatelských účtů.

Spam cílený na vyhledávací systémy

Tento spam spočívá v modifikaci kódu HTML stránek za účelem lepšího umístění ve vyhledávacích seznamech. Moderní vyhledávací roboty jsou však schopny identifikovat např. opakovaná klíčová slova jako účelový spam a dané stránky pak penalizovat.

Více informací na anglické wikipedii: Spamdexing.

Spam mířený na stránky sdílející videa

Videa sdílející stránky, jako je YouTube, jsou často vyhledávány spamery. Nejběžnější metodou útoku je šíření odkazů na pornografické nebo seznamovací stránky v prostorech pro komentáře k náhodnému videu nebo profilu. Další častou metodou je užívání robotů k šíření zpráv náhodným uživatelským profilům. Tento spam pak obsahuje odkazy spolu s lákavým textem a obrázky, které mají většinou sexuální charakter. Tyto stránky mohou obsahovat svoje vlastní nebo uživatelská videa. Hlavním cílem těchto profilů je nalákat lidi na odkaz na domovské stránce v jejich profilech. YouTube zakázal umísťování těchto odkazů. Kromě toho implementoval CAPTCHA systém, který značně ztěžuje rychlé umísťování těchto opakovaných příspěvků více než kdy předtím. Tento systém byl zaveden kvůli masovým spamerům, kteří zahltili uživatelské profily tisícovkami opakovaných zpráv.

Nyní je však aktuální jiný druh video spamu. Nově uploadované video dostane název a popis podle známé osobnosti nebo události, které je třeba věnovat pozornost. Obsah videa však nemá nic společného s vlastním názvem. Rickroll, občas urážlivý odkaz na propagovanou stránku. Ostatní mohou uploadovat videa v rámci reklamy na jejich produkt, s herci a zaplacenými referencemi, ačkoliv propagovaný produkt nebo služba má pochybnou kvalitu a pravděpodobně by neprošla podrobným přezkoumáním oddělení norem a postupů určité televizní stanice nebo kabelové sítě.

Ve světě zločinu

Spam může být využit k šíření počítačových virů, trojských koní a jiných zákeřných softwarů. Cílem může být krádež identity, nebo hůře (finanční podvody). Některý spam se pokouší zneužít lidské chamtivosti a jiný se snaží obelstít lidi, kteří nemají dostatek zkušeností s počítačovou technologií. 31.

května 2007 byl zatčen jeden ze světově nejproduktivnějších spamerů Robert Alan Soloway. Popisován jako jeden z 10 největších spamerů na světě byl obviněn ze 35 trestných činů. Mezi nimi byly poštovní podvody, telefonní podvody, e-mailové podvody, krádeže totožnosti a praní peněz. žalobce prohlásil, že Soloway během roku 2003 použil miliony „zombie“ počítačů k rozšíření spamu. „Toto je první případ, ve kterém američtí žalobci použili zákony o krádeži identity k odsouzení spamera za převzetí jména domény patřící jinému majiteli.“

V pokusu o zhodnocení potenciálně legálních a technických strategií k zastavení nelegálního spamu vznikla studie univerzit the University of California, San Diego, and the University of California, Berkeley s názvem “Click Trajectories: End-to-End Analysis of the Spam Value Chain”. Studie katalogizovala po tři měsíce data ze spamu a zkoumala jména webových stránek a hostingových infrastruktur.

studie prokázala, že:

- Polovina spamovacích programů má svoje domény a servery rozmístěné jen na 8 nebo méně procentech hostingových společností nebo autonomních systémů. Celkově 80 procent spamovacích programů využívá služby 20 procent hostingových společností nebo autonomních systémů.
- Ze 76 nákupů, o kterých získali výzkumníci transakční informace, bylo pouze 13 různých bank vystupujících jako nabyvatelé platební karty a pouze 3 banky poskytovaly platební servis pro 95 % spamově nabízeného zboží ve studii.
- „Finanční blacklist“ (finanční černá listina) bankovních subjektů, které obchodují se spamery chtěl dramaticky snížit vydělávání na nevyžádané elektronické poště. Navíc by měl být tento „blacklist“ aktualizován častěji než spameři získají bankovní prostředky. Asymetrie nakloněná snaze zabránit anti-spamu.

Hoax

Hoax ([*houks*], anglické slovo ze 17. století) obecně označuje podvod, mystifikaci či žertovnou klamnou zprávu. V elektronické komunikaci je hoax speciálně nevyžádaná e-mailová nebo IM zpráva, která uživatele varuje před nějakým virem, prosí o pomoc, informuje o nebezpečí, snaží se ho pobavit apod. Hoax většinou obsahuje i výzvu žádající další rozeslání hoaxu mezi přátele, příp. na co největší množství dalších adres, proto se někdy označuje také jako **řetězový e-mail**.

Škodlivost hoaxů

Běžní uživatelé hoaxům často věří a (v dobré víře) jednají podle nich (a rozesílají je dále ve snaze pomoci i ostatním), či je považují za pouhý neškodný vtip, odborníci a správci sítí často hoaxy chápou jako nebezpečný jev, kterému je nutno se bránit. Mezi důvody škodlivosti patří např.:

Obtěžování příjemců

Opakovaný příjem nesmyslných zpráv je pro mnohé uživatele nepříjemný, zejména v době epidemie, kdy se v e-mailových schránkách objevuje stejná zpráva několikrát denně.

Nebezpečné rady

Některé hoaxy poskytují nebezpečné rady, např. jak se zbavit domnělého viru smazáním nějakého souboru. Uživatel, který takové rady slepě následuje, může svému počítači naopak ublížit.

Ztráta důvěryhodnosti

Odesílatel nepravdivých zpráv ohrožuje svou důvěryhodnost, zvláště pokud takové zprávy odesílá z pracovního e-mailu. V takovém případě může utrpět i pověst příslušné firmy či úřadu.

Prozrazení důvěrných informací

Pokud uživatel hoax přeposílá na mnoho dalších adres, běžně ponechá adresy všech příjemců ve zprávě, kde si je mohou všichni přečíst. Tím se šíří obrovský seznam e-mailových adres mezi předem neurčité množství cizích lidí a zvyšuje se tím potenciál pro šíření spamu a počítačových virů. V některých případech dokonce hoax žádá o vyplnění dalších údajů jako adresy či rodného čísla a odeslání takové zprávy na jakousi adresu.

První hoax

Senzace s balónem nebo také Sensace s balónem (v angličtině „The Balloon-Hoax“) je titulek novinového článku napsaného americkým spisovatelem a literárním teoretikem Edgarem Allanem Poem v roce 1844. Článek o přeletu řiditelného balonu Victoria přes Atlantik vyšel v newyorských novinách The Sun 13. dubna 1844 [1] a byl považován za pravdivou zprávu. Dva dny poté byla odhalena jeho nevěrohodnost a článek byl označen za mystifikaci.
Zpráva obsahuje 2 kapitoly: popis balonu s podrobnými technickými detaily a palubní deník, do nějž členové výpravy zapisují své dojmy a z něhož údajný redaktor čerpá.

Poškození konkrétní instituce

Hoaxy mohou velmi snadno poškodit konkrétní instituci. Mezi známé hoaxy paří zfalšovaná účtenka z Lídlu (kde součet položek neodpovídá), Coca-Cola a Mentos,

hybriochalutor v nápoji Coca-Cola, různé značky jedovatých šamponů apod. Firma CocaCola Company si pro tyto účely zřídila speciální www stránku http://www.thecoca-colacompany.com/contactus/myths_rumors/, na které prezentuje řadu hoaxů, které se o tomto oblíbeném nápojí šířilo či šíří.

Nekritický příjem informace a její další šíření

Negativní dopad mají hoaxy také všude, kde je nekriticky zpracovaná informace zapojena do každodenního dění v rodině. Například známé případy představují *jedovatá éčka , vajíčka uvařená mobilem ,* apod…

Typické hoaxy

- Falešný poplach – původní význam slova hoax. Zpráva manipuluje s informacemi a snaží se uživatele přimět hlavně k dalšímu šíření (Pozor ICQ vir, pošlete to všem.) nebo dokonce k nějakému destruktivnímu zásahu (Smažte jbdmgr.exe z instalace Windows, je to virus.).
- Zábavné – dříve se řetězové dopisy šířily jen klasickou poštou, dnes se přesunuly na internet. Tyto využívají uživatelovy touhy být vtipný nebo jeho pověrčivosti a vyhrožují (Nepřepošleš-li, budeš mít smůlu.). Naopak poslušnému uživateli slibují všechno možné.
- Prosby – hoax většinou působí na city a prosí příjemce o darování krve, hledání ztracené osoby, případně přímo vylákává peníze. Některé z těchto zpráv původně opravdu rozeslali lidé ve svízelné životní situaci, ale hoaxy často přežívají mnohem déle, než měl autor v úmyslu. (Např. známý hoax s žádostí o krev pro Alexandra Gála šířený v prosinci 2004 více než čtyři roky po jeho smrti.)

Ochrana proti hoaxu

Odborníci se shodují, že pokud dostaneme takovýto e-mail (případně zprávu přes ICQ nebo jiným způsobem), je dobré kontaktovat odesílatele, a pokusit se ho poučit o zbytečnosti a nezřídka kdy také o škodlivosti jeho počínání (i když to mohl dělat v dobrém úmyslu). Do budoucna by se takto dalo ušetřit mnoho času i energie.

Občas se však může stát, že jde o reálné varování před hrozbou, které je vhodné

Mimozemská invaze

Na začátek se vrátíme do třicátých let 20. století. Na konci října roku 1938 totiž zaútočili mimozemšťané v New Jersey a vyvolali paniku po celém New Yorku. Nevěříte? A přece sugestivní rozhlasové vysílání o marťanské invazi přesvědčilo o reálné hrozbě obyvatele napříč Amerikou, řada z nich uprchla ze svých domovů a řada dalších se začala připravovat na ozbrojený odpor proti invazi. V některých zdrojích se mluví až o milionu posluchačů, kteří podlehli strachu a hysterii. Přestože bylo vysílání uvedeno jako rozhlasová adaptace knihy Válka světů a v jejím průběhu bylo několikrát zmíněno, že se jedná o fikci, řadu lidí skutečně zmátla. Byla totiž koncipována jako běžné vysílání a tak bylo snadné upozornění přeslechnout. A tak mezi běžnými předpověďmi počasí a hudebními bloky začaly probleskovat zprávy o pádu meteoritů v New Jersey, následovaly dramatické scény objevení mimozemského vetřelce a „živá“ spojení s armádními jednotkami, čelícími invazi v marném boji. Došlo i na evakuační výzvy a zprávy o tisících uprchlíků, ucpávajících cesty.
Samotný autor hry Orson Welles se druhý den za šíření poplašných zpráv omluvil na tiskové konferenci. Řekl mimo jiné, že ani jeho, ani nikoho z rádia nenapadlo, že by je mohli posluchači vzít skutečně vážně. A přestože hra řadu lidí vyděsila, dramatický popis milionů hysterických posluchačů je spíše než cokoli jiného mýtem, vzniklým na titulních stránkách senzacechtivých novin.
Zdroj:
https://www.idnes.cz/zpravy/mediahub/proslule-hoaxy-ktere-poblaznily-svet.A160831_902432_mediahub_imp

rozeslat dále. To se ovšem doporučuje pouze v tom případě, kdy si je uživatel jistý, že se o hoax opravdu nejedná. Například, když znáte odesílatele a víte, že rozumí tomu co píše, že hoax neposílá a důvěřujete mu.

Známý server, HOAX.cz, zabývající se touto tematikou, uvádí jednoduché pravidlo, jak jednoduše rozeznat hoax od důležité informace: „V praxi můžeme použít následující pravidlo: Jestliže zpráva obsahuje výzvu k hromadnému rozeslání na další adresy, je to s největší pravděpodobností HOAX.“ Samozřejmě, že neplatí na 100 %, ale alespoň částečně se rozeznat dá.

Existuje mnoho důvodů, které mohly vést původního autora hoaxu k odeslání zprávy. Většinou se snaží se zabavit, někoho nebo něco poškodit, popřípadě udělat z lidí hlupáky (viz níže v příkladech hoaxu). V mnohých případech se jedná o naprosté absurdnosti, to však nebrání mnoha uživatelům v dalším rozesílání této zprávy.

Obsah