Web 2.0 – Uživatelsky generovaný obsah

Významná část obsahu internetu je dnes tvořena uživateli. Uživatelsky generovaný, nebo chcete-li uživatelsky tvořený obsah se začal rozmáhat s nástupem publikačních možností a sociálních médií na přelomu tisíciletí. Synonymem pro dnešní internet je Web 2.0. Význam je stejný jako uživatelský generovaný, nebo uživatelsky tvořený obsah.
Jednoduše řečeno: dnešní uživatel internetu už dávno není pasivním konzumentem obsahu. Aktivně se podílí na neustále rostoucím objemu online dat každou sekundu...

Uživatelé používají při tvorbě internetového obsahu různé aplikace. Nejčastěji využívanými jsou sociální média, jako nástroje pro tvorbu nejširšího spektra dat (textu, obrázků, videí, komentářů apod.). Každý uživatel internetu může být reportérem, bloggerem, Youtuberem, recenzentem a hodnotitelem, každý uživatel internetu může do jeho prostředí umístit jakýkoliv druh informace.

Díky vyhledávacím nástrojům máme uživatelsky příjemnou možnost prohledávat obsah internetu a okamžitě si prohlížet výsledky. Stinnou stránkou publikačních možností každého je fakt, že v dnešním internetu nikdy nevíte, zda nalezená informace je korektní, zda se nejedná o falešnou (fake) či poplašnou (hoax) zprávu. Zda nejde o manipulaci. V dnešním internetu jsou kladeny na uživatele mnohem vyšší nároky z hlediska ověřování hodnoty a seriózności informace. Dnešní internetovou realitou jsou sociální bubliny a manipulace.

Čím více informací je dostupných online, tím větší nároky jsou kladeny na uživatele při jejich vyhodnocování.

Internet jako veřený prostor

Kyberprostor umožňuje svým uživatelům najít nové možnosti a cesty ekonomické, politické a sociální interakce. Jeho univerzální konektivita je jeho potenciálem pro každého ať se nachází kdekoliv.
Považujme internet za veřejný prostor a s tímto vědomím k němu i přistupujme. Považujme každou informaci publikovanou online za veřejnou a mějme na vědomí, že informaci mohou vidět všichni online uživatelé, včetně našich přátel, nepřátel, rodičů, kolegů, nadřízených, podřízených, pedagogů a dalších.

Každý uživatel internetu si nalezenou informaci může uložit, pořídit si její kopii, zálohovat, dále šířit, komentovat, a to kdykoliv se mu zachce. To samé platí i pro obrázky, videa a další typy informací.

I když konkrétní služba zdůrazňuje ochranu Vašich informací a dat, zůstaňte obezřetní.

Přečtěte si o úniku dat ve službě Ashley Madison: https://en.wikipedia.org/wiki/Ashley_Madison_data_breach

V internetovém prostředí zapomeňte na tlačítko **<Delete>**. V online prostředí jednoduše **neexistuje**.

Každá informace je **dohledatelná**, pokud je publikována v online prostředí, autor nad ní ztrácí kontrolu. Dbejte na svou **online reputaci**.

Online monitoring

Je jedno zda tweetujete, nakupujete na online shopu či jen bezcílně brouzdáte internetem. Firmy vás neustále monitorují. A nejen firmy.

Internetoví giganti se stále zlepšují ve shromažďování dat o uživatelích a vytvářejí detailnější uživatelské profily. Stále také hledají možnosti, jak taková data využít.

Někteří výrobci a prodejci tak mohou uživatelské profily zneužít ke znevýhodnění uživatele vůči ostatním. Pokud budete vyhodnoceni jako bonitní zákazníci, může vám být nabízeno dražší zboží, nebo bude konkrétní typ zboží pro váš za vyšší cenu než pro ostatní.

V budoucnu mohou také být vaše online aktivity (tzv. digitální stopa) brány v potaz při žádosti o půjčku nebo zaměstnání.

https://www.theguardian.com/technology/2017/may/13/how-to-get-privacy-digital-life-data-monitoring-gathering-amazon-facebook-google

Tip!

- Minimalizujte své aktivity na free WiFi
- Nepoužívejte e-banking na free WiFi nebo veřejných PC v hotelu, internetových kavárnách apod.
- Při používání mobilů v dopravních prostředcích si dávejte pozor na sledování „přes rameno“
- Nesdílejte své zařízení s ostatními uživateli a pokud tak činíte, používejte uživatelský profil a chraňte si ho dostatečně silným heslem
- Pro lepší ochranu používejte připojení přes VPN
- Při použití sdíleného PC, vždy vymažte historii procházení, cache and cookies po ukončení vaší práce s internetem.

Hoax

Trik jak získat vaší důvěru, zmanipulovat váš názor a přesvědčit o pravosti falešné či absurdní informace. Poplašná zpráva.

Rozmach internetu s sebou také přinesl nové metody jak oklamat uživatele a zmanipulovat jejich mínění.

Hoaxy (poplašné, manipulativní zprávy) mají za cíl přimět uživatele k prozrazení anebo zaslání:

- peněz,
- Informací o kreditních kartách,
- osobních dat,
- hesel,
- Přístupových kódů,
- a dalších informací převážně osobního charakteru...

Uživatelé musí být obezřetní zvlášť v případech, kdy obdrží např. prostřednictvím e-mailu žádost o sdělení informací osobního charakteru, hesel a poslání peněz.

Tip! Jak se ochráníte před Hoaxy

1. Věřte vašemu instinktu. Pokud cítíte, že něco není v pořádku, pravděpodobně není.
2. Ověřte si firemní telefon a adresu. Pokud nejsou uvedeny, zpozorněte.
3. Vždy vyhledávejte a prověřujte zákaznické reference.
4. Zkuste vyhledat informace o vrácení peněz či zboží, chystáte-li se nakupovat.
5. Nenechte se vmanipulovat do nákupu zboží, služby či podpisu smlouvy pokud nemáte dostatek času si vše řádně rozmyslet.
6. Použijte k platbě kreditní kartu, ale buďte obezřetní před vyzrazením jejího čísla. Pokud nastane problém, banka je schopna vám peníze vrátit zpět.
7. Neodpovídejte na hromadné e-maily, které nejsou adresovány vám.
8. Uložte si vytištěnou kopii e-mailové nabídky pro případ, kdy byste informaci potřebovali později.
9. Buďte obezřetní před nabídkami, které používají anonymní e-mailovou adresu.
10. Držte se dále od pyramidálních schémat. Ty od vás požadují poslat peníze ostatním, kteří opět posílají peníze ostatním atd.
11. Buďte obezřetní před e-maily, které vás informují o výhře finanční částky. Pokud jste požádáni o zaplacení částky, aby vám mohla být vyplacena výhra, vždy odmítněte.

Jak odhalit falešné zprávy (fake news)

Buďte dobří digitální občané a nepropagujte falešné zprávy.

Uživatelé slepě sdílejí falešné zprávy nebo články zvlášť při využívání sociálních sítí. Existuje několik základních kroků, jak odhalit falešné zprávy a nepodílet se na jejich dalším šíření. Falešné zprávy bývají „chytlavé“, zaujmou uživatele na první pohled a dá se jim snadno uvěřit od prvních momentů čtení.

1. Sami si vyhledejte zdroje anebo další informace o tématu

Pokud čtete sporný článek, věnujte pár chvil rychlému vyhledávání na internetu témat z jeho obsahu. Ujistěte se, že zdroje, ze kterých jste čerpali, jsou seriozní.

2. Prověřte citace

Aktuální zprávy běžně používají citace. Pokud najdete v článku uvozovky, zkuste si na internetu vyhledat i další vyjádření osoby, která je citována.

3. Prověřte zdroje

Pokud čtete nějaký článek, první věc kterou byste měli udělat je zkontrolovat zdroj. Podívejte se, z jaké domény článek pochází. Jde o renomované webové stránky. Pokud URL končí na .co, je často falešná.

Běžný trik pro manipulaci se zdroji je použít legitimně vyhlížející jméno a přidat **.co** na jeho konec.

Příklad:
Abcnews.com je legitimní reálná stránka aktualit
Abcnews.com.co je jistě falešná doména

4. Jaké jsou vaše pocity?

Mnoho falešných zpráv je psáno způsobem, aby se vám „dostaly pod kůži“ a zjitřily vaše emoce. Pokud máte podobné pocity při čtení zprávy, měli byste zpozornět. Jde o běžnou metodu jak ve vás vyvolat pocit, že se o článek musíte okamžitě podělit s ostatními, sdílet jej. Ale zadržte. Před tím si ještě důkladně prověřte zdroje. Vždy si připomeňte známé heslo: „raději dvakrát prověřit než jednou kliknout“

5. Působí realisticky?

Ve snaze získat váš zájem se autoři často uchylují k extrémům a napíší obsah, který se nezdá reálný. Buďte při zemi a vše si důkladně prověřte.

Internetové viály – Ice Bucket Challenge

Virální zprávy či události (tzv. viály) jsou lavinovitě šířené informace, obrázky, videa či výzvy, které mají tendenci se rychle šířit napříč internetem během krátké doby. K nejčastějším projevům virálů patří virální videa. Objeví se videoklip, animace či film, které se velmi rychle šíří prostřednictvím sdílení. Virální videa mohou získat miliony zobrazení, jsou sdíleny prostřednictvím sociálních sítí, umisťovány na blogy, posílány e-maily apod.

Virálem se může stát i článek nebo obrázek.

Jedním z dobrých příkladů virálu byl tzv. Ice Bucket Challenge. Jde o masové vylévání nádoby plné ledové vody na hlavu pro podporu povědomí o onemocnění amyotrofické laterální sklerózy. Virál se objevil v prostředí sociálních sítí v červenci až srpnu 2014.

Šlo o úspěšnou kampaň. Namísto zlepšení povědomí o onemocnění poukázala na sílu sociálních médií a sdílení. Využitím sociálních médií jako nosné platformy se dostala k mnoha uživatelům po celém světě.

Síla sociálních médií může být také zneužita. Pro oslovení velkého množství lidí jsou sociální média ideální platformou a zdrojem dat. Uživatelé jsou často lhostejní k ochraně svých osobních dat. Pokud chtějí být populární, dostávat více lajků a získávat více přátel, uživatelé jsou ochotni sdílet detaily ze svých životů, jejichž zneužití se může v budoucnu velmi obrátit proti nim. Každodenní praxí internetu je profilování uživatelů, personalizace, dolování dat, sdílení dat uživatelů s dalšími subjekty, jejich prodej a využívání pro marketingové a obchodní účely.

Jaké mají informace na internetu dopad na děti

Děti a mládež žijí online. To už není nic, co by nás šokovalo. Fenoménem dnešní mládeže je jejich online život na sociálních sítích. Nezáleží na tom, zda jsou ve škole, doma, na prázdninách nebo jen na večeři s rodiči, jsou jednoduše stále „on“. Prostřednictvím sociálních médií neustále komunikují se svými „veřejnostmi“, sdílejí co je sdílitelné, komentují apod. Internet změnil způsob komunikace mladých. Ať se nám to líbí nebo ne.

Děti nejsou výjimkou. Začínají s digitálními technologiemi v raném věku, většinou hrají (online) hry. Přirozený nedostatek zkušeností a socializace je ale činí zranitelnými. Není žádný problém děti ovlivnit některým z druhů podvodů, nebo použít manipulace pro nastavení masivních trendů. Děti věří tomu, co čtou, co vidí, co sdílejí ostatní uživatelé. Necítí potřebu si informace ověřovat, prověřovat zdroje nebo si udělat vlastní průzkum zda jsou informace falešné či nikoliv.

Ano, jde o velmi snadné a bezstarostné používání online technologií ve smyslu konzumace, někdy to ovšem může vést k manipulacím a nepochopení reality.

Dva dobré příklady skutečnosti, jak jsou děti manipulovatelné, jsou fenomény Modrá velryba a Talking Angela. Zeptejte se na ně dětí. Budete překvapeni.

Modrá velryba – fenomén sebepoškozování

Jaro roku 2017 bylo časem Modré velryby. Společností otřásly informace o hře, ve které se plní celkem 50 sebepoškozujících úkolů a tím posledním je sebevražda. Modrá velryba se dostala do povědomí díky článku v ruských novinách Novaja Gazeta v roce 2016 a velmi brzy tento fenomén zahltil celý internet. Zatímco mnoho odborníků považuje Modrou velrybu za zdařilý hoax, věří, že časem mohl inspirovat ke vzniku sebepoškozujících a sebevražedných skupin, které měly vliv i na děti a nabádaly je k podobným aktivitám.

Talking Angela a její „schopnosti stalkingu“

Dalším příkladem toho, jak by mohla internetová manipulace ovlivnit názory dětí, je fenomén Talking Angela.

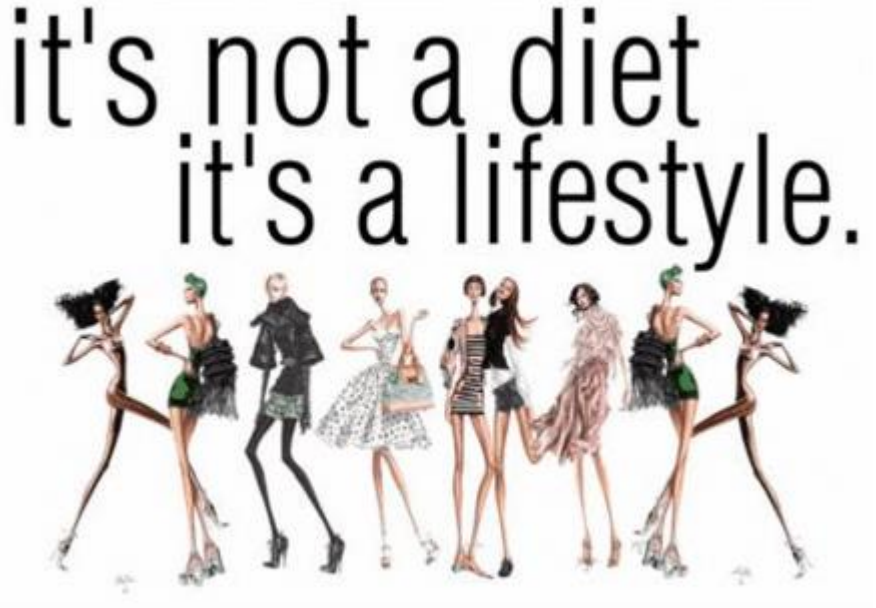
Hra Talking Angela byla vydána v roce 2012 jako appka pro iPhone a iPad. Později se rozšířila i na platformu Android. Vychází z předchozí verze aplikace Talking Tom and Friends. Virtuální zvíře v ní opakuje vše co říkáte do mikrofonu svého zařízení. Děti si s ním mohou hrát i dotykem a posouváním po obrazovce.

Talking Angela byla od počátku provázena manipulací, a to varováním před stalkovacími schopnostmi hry. Rodiče měli díky těmto manipulativním zprávám oprávněné obavy z této hry. Jedna z dobře známých společností v oblasti počítačové bezpečnosti, Sophos, však vše uvedla na pravou míru, vysvětlila komunikační schopnosti hry a poukázala na dezinformaci ohledně dětské zranitelnosti při hraní hry. Dětí věří, že Angela (zvíře zobrazené ve hře) má v očích kamery a díky nim hackeři vidí vše, co se odehrává před jejíma očima.

Důkazem „skutečnosti“ stalkovacích schopností Angely je mnoho internetových obrázků, ve kterých je vidět zrcadlená scéna v zorničkách Angely. Zkuste se dětí zeptat, co si o tom myslí? Jak je možné, že má Angela kamery v očích? Jak to může fungovat? Přestože v tomto případě jde o manipulaci, na internetu existuje množství programů a aplikací, které mají skutečné sledovací schopnosti. Proto je dobré děti poučit, že hry a další obsah mají stahovat pouze z ověřených zdrojů, ignorovat vyskakovací okna a manipulativní oznámení typu „*Jste miliontým návštěvníkem této webové stránky a proto vyhráváte nejnovější model mobilu iPhone.*“ Stahování filmů, hudby, her a dalšího obsahu z podezřelých stránek může být velmi riskantní.

Viz také zde: https://www.theguardian.com/technology/2014/feb/18/talking-angela-app-children-safety

ProAna/ProMia stránky, manipulativní obsah



Pro-anorexia (‘pro-ana’) a **pro-bulimia** (‘pro-mia’) stránky nabádají k poruchám stravování. Nabízí anorexii a bulimii jako životní styl a typicky obsahují rozličné návody, jak přizpůsobit stravování právě těmto metodám. Radí, jak skrýt anorexii a bulimii před rodiči nebo lékaři, radí, jak se chovat, jak se zbavit zkonzumovaného jídla, jak potlačit hlad apod. Nejčastější motivací je štíhlost, ztráta anebo udržení váhy. Stránky se snaží budovat komunity, sdružovat ostatní uživatele se stejným zaměřením a získat jejich podporu. Stránky existují od doby, kdy se začal masově rozšiřovat internet. Nyní jsou k dispozici i na sociálních sítích, např. Facebooku. Tyto stránky navštěvuje významné množství dospívajících dívek, pro které manipulace jejich prostřednictvím může znamenat velké riziko.
Je k dispozici rostoucí množství důkazů o skutečnosti, že webové stránky nabádající k poruchám potravy přitahují ohroženou skupinu mladých lidí, kteří mají k těmto extrémům sklony. Tyto stránky představují riziko škodlivého dopadu na uživatele, protože zvyšují obavy o udržení váhy a tělesné konstituce a mají negativní dopad na jejich biorytmy a další tělesný vývoj. Rodiče mají obvykle minimální povědomí o těchto stránkách a jejich obsahu.

Tipy a triky na těchto stránkách obsahují: návody na diety a omezování příjmu kalorií, hladovění a zbavování se zkonzumované stravy. Přitahuje nejisté a zranitelné uživatele a uživatelky, kteří mají komplex méněcennosti, jsou si nejistí, hledají sami sebe, prožili životní trauma, mají chorobnou představu o své nadváze, nejsou spokojeni se svým vzhledem, touží po dokonalosti, upínají se ke vzorům celebrit a známých osob, kteří propagují štíhlost a dokonalost vzhledu, mají špatné rodinné zázemí.

Příklady:

- https://www.anorexicdiettips.com/
- http://www.myproana.com/
- http://www.proanatipsandtricks.com/

ProAna – pozor na bezpečnost dětí

Většina internetových pokynů pro rodiče o bezpečnosti na internetu je napsána z hlediska ochrany dítěte před pornografií nebo kyberzločinci, kteří se soustředí na děti. Některé obecné pokyny mají podobný význam i pro ochranu dětí před poruchami stravování.

Tyto podněty obsahují:

1. Nakupte vhodný monitorovací software, který vám umožní zablokovat určité webové stránky a sledovat historii webových stránek podle jejich navštěvování.

2. Umístěte počítač, který používá vaše dítě do společné místnosti, abyste měli dítě pod dozorem a mohli také dohlížet na to, jaké webové stránky navštěvuje.

3. Stanovte délku používání počítače vašim dítětem tak, aby odpovídala věku dítěte a dítě s ním netrávilo neúměrně mnoho času. Prodiskutujte pravidla s dítětem a umístěte je vytištěná vedle počítače.

Nadměrná doba používání počítače, zejména pozdě v noci, může být signálem skrytého problému.

4. Dávejte pozor na to, s kým vaše dítě komunikuje v online prostředí.

Characteristika webů of Pro-Ana, Pro-Mia a Pro-ED*

- Vyzdvihují a oceňují vzhled extrémně štíhlých jedinců
- Považují jídlo a váhu za nepřítele
- Podporují a učí k nebezpečnému chování vedoucímu k poruchám stravování
- Propagují hubnutí za každou cenu bez ohledu na zdravotní dopady
- Podsouvají, že odmítání potravy je volbou nikoliv vážnou nemocí
- Pokus o maskování zhoubného dopadu exkluzivitou

**vedoucích anebo nabádajících k poruchám stravování*

Stránky nabádající k sebepoškozování

Online obsah s charakterem sebepoškozování

V rozsáhlém internetovém prostoru se objevují i specializované komunity, které se zabývají sebepoškozováním a nabádají k těmto aktivitám i ostatní.

Online komunity, které sdílejí zkušenosti se sebepoškozováním a v některých případech podporují sebepoškozování nebo sebevraždu u ostatních, nabádají k záměrnému způsobovaní vlastního poranění nebo ubližování (např. pořezání). Ačkoli sebevražedné chování může u jednotlivců naznačovat depresi nebo vážné duševní zdravotní stavy, které souvisejí se sebevražednými úmysly, lidé se ne vždy sebepoškozují, protože chtějí spáchat sebevraždu. Je důležité pochopit, že toto chování není stejné jako pokus o sebevraždu.

Převážná většina dospívajících nechodí na webové stránky s touto tématikou. Navíc jimi oblíbené stránky sociálních médií mají pravidla proti aktivitám podporujícím škodlivé chování. Vynucování těchto pravidel však může být nekonzistentní, což umožňuje některým komunitám, aby se on-line uživatelé stali obětí jejich zájmů chování v oblasti sebepoškozování.

Pokud znáte někoho, kdo navštěvuje webové stránky o sebepoškozování nebo sebevraždách, promluvte si s ním o tom. Snažte se pochopit, co se děje a proč ho tyto stránky přitahují. Přemýšlejte společně o dalších stránkách, které můžete prozkoumat, kde může najít podporu a porozumění, a nabídněte mu pomoc při vyhledání dalších míst, pokud to považujete za užitečné. Být schopen oslovit ostatní uživatele a mluvit s nimi o problému, může být velmi dobrým krokem pro oslovení mladých, kteří potřebují pomoc.

Tak jako obrovské množství jiných informací jsou i otřesné obrázky trpících a sebepoškozujících se dětí na „dosah jednoho klepnutí“.

Co je sebepoškozování?

Někteří lidé mají pocit, že se jim život vymyká z jejich kontroly. Přistupují tedy k metodám sebepoškozování a způsobování si vlastní bolesti, aby se vyrovnali s bolestí nebo aby se trestali za vlastní selhání. Není to totéž, jako pokusy o sebevraždu, kdy se někteří jedinci často v depresích snaží ukončit své životy.

Sociální inženýrství

Sociální inženýrství v kontextu informační bezpečnosti se týká psychologické manipulace lidí za účelem provedení požadovaných akcí nebo předávání důvěrných informací. Typ důvěryhodného triku pro účely shromažďování informací, podvodů nebo přístupu k systémům je často jedním z mnoha kroků v komplexnějším systému podvodů.

Termín „sociální inženýrství“ je používán pro metodu psychologické manipulace s uživatelem a často má vědecký základ. Je ale používán profesionály v oblastech počítačové a informační bezpečnosti.

Všechny techniky sociálního inženýrství jsou založeny na specifických atributech lidského rozhodování, známých jako kognitivní předsudky (zkreslení). Tyto předsudky, někdy nazývané "chyby v lidském hardwaru", jsou využívány v různých kombinacích k vytvoření techniky útoku. Útoky používané v sociálním inženýrství mohou být použity k získání důvěrných informací zaměstnanců. Nejběžnější typ sociálního inženýrství probíhá po telefonu. Dalšími příklady útoků sociálního inženýrství mohou být zločinci, kteří se prezentují např. jako exekutoři, požární a revizní technici, aby pronikli do firemního perimetru a získali tak přístup k citlivým anebo střeženým informacím.

https://cs.wikipedia.org/wiki/Sociální_inženýrství_(bezpečnost)

Techniky sociálního inženýrství

- předstírání
- odcizení krádeží
- phishing (rybaření), telefonický phishing
- spear phishing (neosobní hromadný e-mail s cílem získat chráněné informace)
- water holing (napadení skupiny uživatelů infikováním jimi navštěvovaného webu virem)
- baiting (infiltrace viru podvodem např.přes vyhraný USB flash disk)
- quid pro quo (něco za něco, nabídka opravy techniky za poskytnutí přístupu)
- Tailgating (neautorizovaný přístup do perimetru podvodem)

Cíle a motivy sociálního inženýrství:

- Odcizení čísel a hesel kreditních karet.
- Prolomení e-mailových účtů a komunikačních chatů a manipulace s nimi editací za účelem získání peněz z účtů nebo vzbuzení nedůvěry mezi uživateli.
- Nabourání webových stránek firem a organizací s cílem poškození jejich reputace.
- Poplašné zprávy o počítačových virech
- Přesvědčení uživatele, aby spustil ve svém prohlížeči škodlivý kód prostřednictvím XSS útoku a umožnil tak přístup k webovému anebo jinému účtu.

Spam a nebezpečné přílohy

Spam = nevyžádaný nebo nelegální e-mail zpravidla od neznámého odesilatele.

Mnoho e-mailových spamových zpráv je komerční povahy, ale může také obsahovat maskované odkazy, které se zdají být pro známé webové stránky, ale ve skutečnosti vedou k phishingovým webům nebo webům, které jsou hostitelem malwaru.

Spamový e-mail může obsahovat také škodlivý kód, jako např. skripty nebo jiné přílohy spustitelného souboru (trojské koně).

Spameři shromažďují e-mailové adresy z chatovacích míst, webů, seznamů zákazníků, diskusních skupin a stránek, které shromažďují adresáře uživatelů. Tyto databáze jsou někdy také prodávány dalším spammerům.

Spameři často používají falešná jména, adresy, telefonní čísla a další kontaktní informace k nastavení "jednorázových" účtů u různých poskytovatelů internetových služeb. Také často používají padělaná nebo ukradená čísla kreditních karet, která platí pro tyto účty. To jim umožňuje rychlý přesun z jednoho účtu na druhý.

https://cs.wikipedia.org/wiki/Spam

Mnoho rozšířených e-mailových systémů používá antispamové filtry. Chrání koncového uživatele před spamem, nicméně proces filtrování není 100%. Pouhou náhodou někdy filtruje antispamový filtr běžný e-mail (například naskenovaný dokument zaslaný vaší tiskárnou ve formátu PDF), na druhou stranu se stává, že ve schránce doručené pošty najdete e-maily s typickým komerčním obsahem. Rozhodovací proces je na zodpovědnosti uživatele.

- Pokud si nejste jisti, zda se jedná o spam či nikoliv, podívejte se pozorně na odesilatele e-mailu a text v jeho těle.
- Pokud odesilatele neznáte, raději e-mail neotevírejte.
- Přečtěte si pozorně text e-mailu. Našli jste gramatické chyby? Pokud ano, jedná se o spam. Vymažte ho (nebo označte jako spam).
- Má e-mail emotivní obsah? (např. žádost o pomoc nebo finanční podporu) Nevěřte tomu, jde 99,90% případů o spam.
- Má e-mail od neznámého odesilatele přílohu? V žádném případě ji neotevírejte! Může se jednat o spustitelný soubor obsahující škodlivý kód (trojan, virus atd.)
- Vypadá e-mail jako od vaší banky? Nevěřte tomu. Banky nekomunikují se svými klienty přes e-mail.
- Pokud e-mail obsahuje odkaz, neklikejte na něj. Může vést na stránky se škodlivým obsahem nebo kódem, který napadne váš PC.
- Instalujte na své zařízení antivirový SW a pravidelně jej updatujte. Může zabránit spuštění anebo stažení škodlivého kódu na vaše zařízení.

FOMO syndrom

FOMO = Fear of Missing Out

Znáte to velice dobře. Neustálé prohlížení a kontrola statutů vašich přátel na sociálních sítích vás vede k přesvědčení, že všichni si žijí mnohem lépe, než vy. A co víc, pokud jste zaneprázdněni jinou činností a nemáte šanci se připojit, trpíte pocitem, že vám něco důležitého uniká.

Toužíte být neustále informováni o tom, co dělají ostatní. Nedokážete si představit okamžik, kdy byste nebyli připojeni. Znáte takové pocity? Zažíváte je také? Pokud ano, pravděpodobně máte **syndrom FOMO** (strach z promeškání, strach že stojíte stranou).

FOMO může jednoduše existovat jako permanentní mentální stav, ale může být také provázen různými fyzickými reakcemi (např. pocením). Na základě průzkumu realizovaného v USA a Velké Británii většina dospělých, kteří se narodili na přelomu tisíciletí anebo krátce před (současný věk 18 až 34 let), odpověděla že by byla schopna souhlasit s čímkoliv ze strachu z FOMO a více než polovina odpověděla, že stěží investují dostatečný čas a energii na to, aby se zabývali novými tématy anebo zájmy.

FOMO je často také motiv, který odvádí lidi od učení anebo ruší při řízení motorových vozidel.

Spoluvytváří také nezdravé sociální návyky, jako neustálé ověřování e-mailů, kontrola sociálních médií, místo toho, aby se uživatelé zapojili do současných sociálních interakcí.

https://en.wikipedia.org/wiki/Fear_of_missing_out

Sociální média, jako např. Facebook, Foursquare a Twitter, jsou nástroje pro hledání sociálního propojování a většího zapojení do společnosti. Nicméně nezdravé sociální návyky se mohou odrazit v nedostatečném zapojení do současných sociálních interakcí. Pokud uživatelé používají technologii k vlastní identifikaci a definici sdílením svých myšlenek a pocitů aniž by je skutečně měli a prožívali, nepřímo tím vysílají zprávu "sdílím proto, že jsem", což může ostatní uživatele vést k nepochopení podstaty sociálního sdílení a interakce. Pokud stále více uživatelů vyhledává novinky jen proto, aby upoutali pozornost ostatních, mohou se časem cítit izolovanější a prázdnější.
Sociální média se staly velkým umocňujícím faktorem syndromu **FOMO**. U uživatelů se rozvíjejí negativní pocity a emoce **díky závisti** z aktualit a obrázků životů ostatních. Odborníci na dvou německých univerzitách zkoumali obsah Facebooku a došli k závěru, že uživatelé mají při používání sociálních sítí negativní pocity z důvodu sledování „dokonalého“ života svých přátel.

FOMO:
Úzkost, roztěkanost a pocit promarněné příležitosti z přesvědčení, že v současném okamžiku se na jiném místě odehrává mnohem zajímavější událost, která uživateli uniká. Pocity často vyvolané díky příspěvkům na sociálních médiích.