GYMNÁZIUM
MALACKY

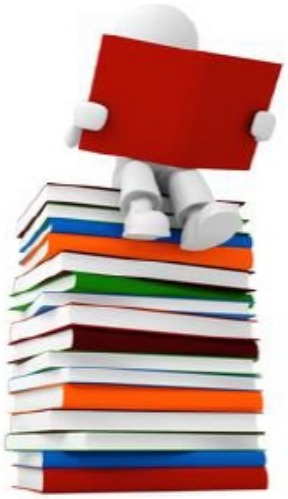
Nebezpečné výzvy v online prostredí

Nevyžiadaný obsah

PREVENCIA
KRIMINALITY

Obsah

- Čo je nežiadaný obsah
- Spam a ochrana pred ním
- Hoax + ochrana pred ním
- Škodlivý software – vírusy, spyware, reklama + ochrana pred nimi



Ako sa chrániť pred vírusmi a inými škodlivými programmy?

Na začiatok vám postačí antivírusový softvér. Ideálne však legálna verzia s pravidelnými updatemi. Môže sa totiž stať, že neaktualizovaný softvér vírus jednoducho deaktivuje. Ďalšími krokmi k bezpečnejšiemu používaniu internetu a ich funkcií sú: v e-mailovom prehliadači deaktivujte automatické sťahovanie a otváranie príloh, uistite sa, že máte zablokované automatické sťahovanie z prehliadačov, v prehliadači si môžete zablokovať vyskakovacie okná alebo pridať ad block, ktorý zablokuje reklamu, pravidelne čistite históriu prehliadača, cookies a cache, neklikajte na podozrivé linky alebo videá odosielané z konta vašich známych, používajte len aktualizovaný prehliadač, neklikajte na tlačidlá a reklamy, ktoré vyzerajú podozrivo, ignorujete vyskakovacie okná, ktoré vás informujú o zníženej bezpečnosti vášho PC, aplikácie sťahujte len z webov originálnych developerov alebo overených stránok, každý stiahnutý súbor a pripojené zariadenie nechajte preskenovať antivírusovým softvérom, pozor na torenty, no a napokon myslite na pravidelný back up vašich dát...

Ako zistím že mám vírus?

Počítačové vírusy sa prejavujú rôzne. V niektorých prípadoch však môže ísť o nekompatibilitu medzi hardvérom a softvérom. Je preto vhodné najskôr vylúčiť systémové príčiny. Najčastejšie sa prejaví napríklad:

Zariadenie je výrazne spomalené, počítač mrzne, nereaguje, vo Windowse sa častejšie zobrazuje modrá obrazovka, počítač sa sám reštartuje, pribudli vám nové ikonky na ploche, nemôžete sa dostať do control panelu, task managera a pod., ostávate časté error správy, na niektoré webové stránky sa nemôžete dostať alebo vás redirectuje na iné weby, váš internetový prehliadač zamŕza a nereaguje, vaša domovská stránka v prehliadači sa zmení sama od seba, pribúdajú nové toolbari, pribúdajú vyskakujúce okná s reklamami a zvláštnymi správami, v prípade malweru v emailoch môžete dostávať emaily bez odosielateľa, prípadne môžu byť z vašej adresy odosielané spamové emaily...

Čo je nevyžiadaný obsah?

Okrem dôležitých a užitočných informácií sa cez internet a email šíri aj veľa zbytočného materiálu. Prichádza množstvo reklamných správ a výhodných ponúk, preposlaných vtipných emailov a varovaní pred rôznymi nebezpečenstvami, ale aj vírusy a iný škodlivý softvér. Pri pozeraní webstránok vyskakujú blikajúce reklamné okná. To všetko je otravné, obťažuje nás pri práci, zbytočne pri čítaní strácame čas. Okrem toho hrozí, že naletíme na rôzne podvody alebo si nevedomky nainštalujeme vírus, ktorý poškodí počítač. Preto sa musíme pred nimi chrániť. Najlepšou všeobecnou ochranou pre všetky tieto správy je nevšímať si ich a od kliknúť ich preč. Táto metóda však nepomáha na vždy, lebo ak sa ukážu raz, môžu sa kedykoľvek vrátiť späť. Preto je treba sa proti nim brániť rôznymi spôsobmi. Na niekoľko z nich vám poradí táto brožúra, ktorá vám vysvetlí, čo je daný nevyžiadaný obsah a ako sa proti nemu máme brániť.

Spam

Pod označením spam sa skrýva hromadne rozosielaná nevyžiadaná pošta. Najčastejšie sa šíri prostredníctvom emailov, ale aj cez SMS a MMS správy v mobiloch, na četoch alebo v online diskusiách. Veľkú časť spamu tvoria reklamné správy, výhodné ponuky nákupov, ponuky na účasť v súťažiach a lotériách, ako aj ponuky erotických telefonických liniek a pornografických stránok, zázračných liekov a liečebných postupov, nelegálneho softvéru a pod. Spameri si vašu emailovú adresu vedia získať náhodným vygenerovaním, vyhľadaním na stránkach, kde ju máte zverejnenú, z hromadne preposielaných emailov alebo emailových diskusných skupín. Aj ľudia sami zadávajú na internete svoju emailovú adresu pri objednávaní služieb cez internet alebo pri prihlasovaní sa na rôzne stránky. Často tým zároveň dávajú súhlas na posielanie reklamných správ. Pre spoločnosti je posielanie reklamných správ lacný a efektívny spôsob komunikácie so zákazníkmi. Nie všetci hodnotia reklamný spam rovnako – niektorí radi privítajú upozornenia na najnovšie služby, produkty a akcie aj takouto formou. Pre iných sú však takéto správy obťažujúce – zbytočne im zapĺňajú emailovú schránku a oberajú ich o čas pri triedení správ. V súčasnosti sa ich množstvo zmenšuje, pretože poskytovatelia emailových stránok majú na ochranu svojich členov filter, ktorý triedy správy a tým likviduje ich možnosť preniknúť do počítača.

Ako sa chrániť pred škodlivým Softwarom

Zálohovanie

Pravidelne zálohujte vaše dáta, aby ste ich nestratili v prípade, ak bude váš počítač napadnutý vírusom.

Ochrana počítača

Používajte bránu firewall a pravidelne aktualizujte svoj antivírusový program. Nainštalujte si ochranu pred spyware a adware.

Výber stránok

Nenavštevujte nezabezpečené stránky, ako sú stránky s pornografiou alebo stránky na nelegálne sťahovanie.

Nebezpečné prílohy

Neotvárajte neznáme prílohy v emailoch. Všetky podozrivé správy, správy od neznámych odosielateľov alebo v cudzom jazyku hneď vymažte.

Informovanosť

Pred inštalovaním akéhokoľvek programu alebo jeho súčasti do počítača si preverte, na čo slúži (napr. zistite informácie cez internetový vyhľadávač). Podrobne si prečítajte, s čím súhlasíte, keď potvrdzujete licenčnú dohodu pri inštalácii. Aj na prvý pohľad užitočné programy môžu byť v skutočnosti adware alebo spyware.

Škodlivý software - vírusy, spyware, reklamy

Ďalšou kategóriou nevyžiadaného obsahu je škodlivý softvér, tzv. malware. Medzi malware („malicious software“) zaraďujeme počítačové vírusy, červy, trójske kone, spyware, adware a i. Malware sa do počítača dostáva zvyčajne cez internet, hlavne pri prezeraní stránok so slabo zabezpečeným systémom (najčastejšie stránok na nelegálne sťahovanie alebo stránok s erotickým obsahom), ako príloha v emailoch a pri inštalácii programov. Počítačové vírusy, červy, trójske kone sú softvér, ktorý po spustení napáda systémové súbory operačného systému počítača, maže súbory alebo adresáre, mení obsah súborov, prípadne poškodzuje hardvér. Dokáže sa sám rozosielať cez počítačovú sieť aj bez vedomia majiteľa počítača, a tak sa šíri k ďalším používateľom.

Spyware je program, ktorý sa sám nainštaluje do počítača a bez vedomia jeho majiteľa si vytvára prehľad o jeho činnosti, zaznamenáva jeho osobné a kontaktné údaje. Tieto informácie sa potom odosielajú tvorcovi spyware. Ten ich môže použiť na posielanie cielenej reklamy (targetingu), ale aj pri útoku na počítač (hacking). Príkladom adware môžu byť bežné bannery, ikony na stránkach, ale aj neustále vyskakujúce pop-up okná (najmä na stránkach s pornografiou, hudbou a zvoneniami na sťahovanie) alebo zmena domovskej stránky v internetovom prehliadači bez súhlasu užívateľa. Vo voľne dostupných programoch slúžia niekedy reklamy na pokrytie nákladov na ich tvorbu, inokedy si firmy „prenajmú“ časť monitora, na ktorom sa zobrazujú okná s reklamov.

Ako sa chrániť proti spamu

Ochrana osobných a kontaktných údajov

Chráňte svoju emailovú adresu a telefónne číslo na mobil, zvážte, kde ich uvediete. Vytvorte si dve emailové adresy – jednu pre rodinu a priateľov a druhú, ktorú budete zadávať pri prihlasovaní na rôzne internetové stránky. V tejto adrese neuvádzajte vlastné meno. Ak vám bude chodiť veľa spamových správ, jednoducho adresu prestaňte používať a vytvorte si novú.

Zamaskovanie emailovej adresy

Ak uvádzate svoj email na internete, uveďte namiesto znaku „@“ slovo zavináč (meno (zavináč) gmail.com). Takto nebudú môcť vašu emailovú adresu ľahko nájsť automatické vyhľadávacie programy.

Ochrana počítača

Používajte antivírusový softvér a pravidelne ho aktualizujte. Ten zachytí spamy, ktoré by mohli obsahovať škodlivý softvér.

Nahlasovanie spamu

Poskytovatelia emailových služieb a programy na prácu s emailami umožňujú označiť nevyžiadané správy ako spam. Adresa odosielateľa je tak zaradená medzi neželané a správy z nej sú blokované. Ak takúto správu dostanete, nezabudnite ju nahlásiť ako spam.

Ochrana pred zasielaním reklamných správ

Pri vypĺňaní online formulárov si pozorne prečítajte podmienky. Ich súčasťou býva súhlas s použitím osobných údajov a s posielaním informácií o nových produktoch. Aj neskôr môžete požiadať o zrušenie zasielania reklamných správ cez email alebo mobil.

Hoax

Pojmom hoax označujeme podvodné správy, ktoré upozorňujú na neexistujúce nebezpečenstvá alebo sľubujú rýchle zbohatnutie. Patria medzi ne aj falošné alebo neaktuálne prosby o pomoc, reťazové listy šťastia a rôzne petície. Takéto správy kolujú po internete roky – postupne sú preložené do rôznych jazykov a aj keď sú v nich úplné absurdnosti, stále sa nájde niekto, kto im uverí a pošle ich ďalej. Tým sa hoax líši od spamu – väčšinou ho preposielajú dôverčiví užívatelia, ktorí si myslia, že ide o dôležitú správu, chcú pomôcť alebo sa podeliť o možnosť výhodného zárobku (viac o ponukách ľahkých ziskov nájdete v kapitole Internetové podvody). Hoax zdôrazňuje naliehavosť nebezpečenstva a dramaticky opisuje riziká. Autor sa snaží vzbudiť zdanie dôveryhodnosti, opiera sa o vymyslené vyjadrenia známych osobností, odborníkov, spoločností alebo o fiktívny zážitok blízkych ľudí (napr. „Microsoft varuje“ alebo „kamarátka mi rozprávala svoju skúsenosť“). Ďalším znakom je prosba o okamžité rozoslanie hoaxu všetkým známym a priateľom. Ďalšími príkladmi hoaxu sú napríklad vymyslené prosby o pomoc, varovanie pred vymysleným nebezpečenstvami, obťažovanie príjemcu, nebezpečné rady...

Ako sa chranit pred hoaxom

Zastavenie šírenia

Neposielajte ďalej reťazové správy. Pre väčšinu ľudí sú takéto správy obťažujúce, zdržujú ich a zbytočne im zapĺňajú emailovú schránku. Rovnako poproste svojich blízkych, aby vám takéto správy neposielali.

Kritické myslenie

Riaďte sa zdravým rozumom. V praxi sa dá použiť pravidlo – ak správa obsahuje výzvu k hromadnému rozosielaniu na ďalšie adresy, je to s najväčšou pravdepodobnosťou hoax. Každú správu tiež kriticky prehodnoťte – to, čo vyznieva príliš dokonale, je väčšinou podvod.

Osveta

Ak vám príde hoax, napíšte odosielateľovi a vysvetlite mu, čo vám vlastne poslal a prečo je to zlé. Svoje tvrdenia môžete podložiť odkazom na databázu hoaxov.

Overovanie pravdivosti informácií

Zistite si, či sú informácie pravdivé alebo ide o hoax. Ak vám prišla podozrivá správa, tak skôr než ju pošlete ďalej, overte si, či sa podobná správa nespomína v niektorej databáze hoaxov (napr. www.hoax.cz).