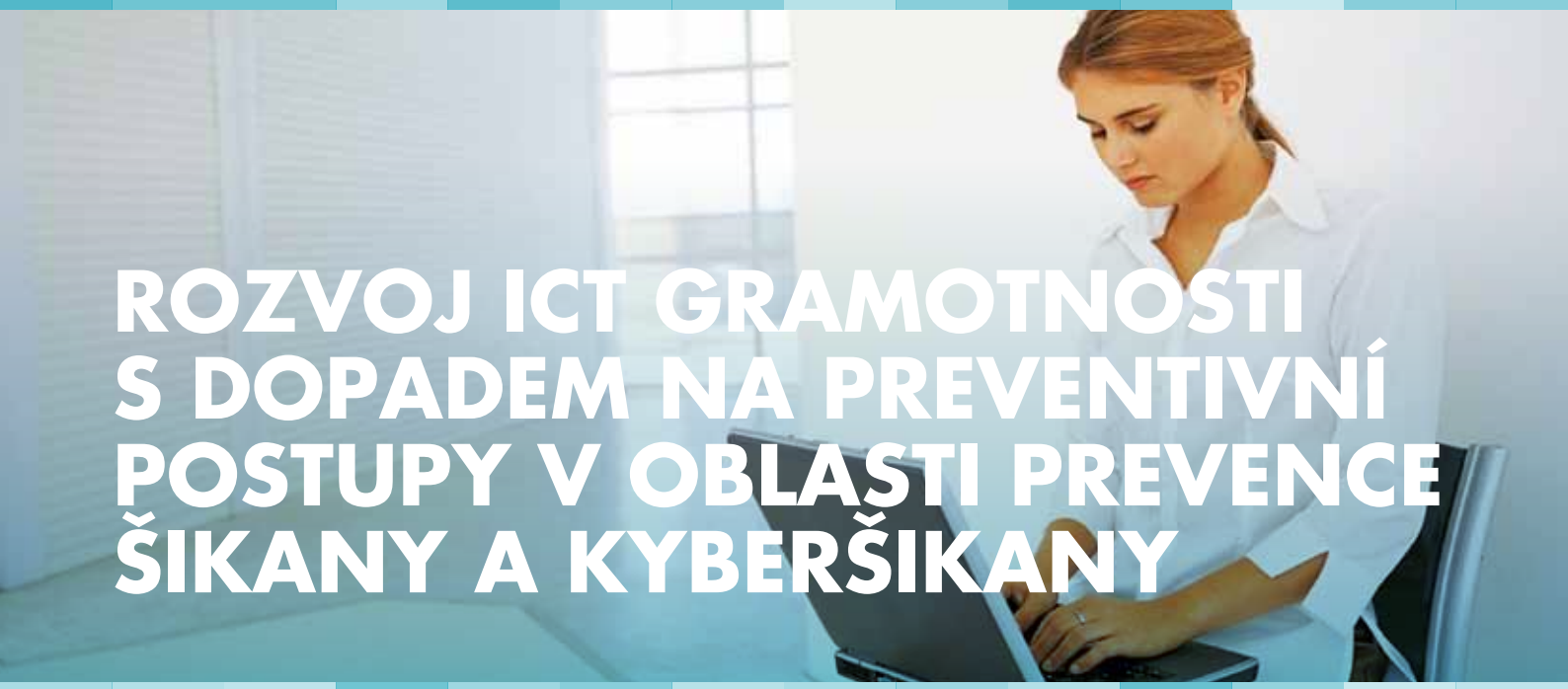
projekt: Vzdělávání napříč KHK



ROZVOJ ICT GRAMOTNOSTI S DOPADEM NA PREVENTIVNÍ POSTUPY V OBLASTI PREVENCE ŠIKANY A KYBERŠIKANY

autor

Mgr. Michal Hodovský

žadatel

Českomoravská vzdělávací, s.r.o.

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Projekt: Vzdělávání napříč KHK

AUTOR: Mgr. Michal Hodovský

Žadatel: Českomoravská vzdělávací,s.r.o.

Obsah

Anotace: *cílem tohoto školení je ukázat rozšířenost kyberšikany mezi dětmi. V první části je vysvětlena problematika kyberšikany a uvedeny její nejčastější projevy. Dále jsou nastíněny možná nebezpečí virtuální komunikace a na sociálních sítích a popsány jednotlivé formy kyberšikany. Vše je pro lepší názornost zaneseno do grafů. V druhé části se pokusíme nastínit možnou cestu snížení nebo částečného omezení kyberšikany, zařadíme kyberšikanu z pohledu zákona a nastíníme možná potrestání nezletilých i mladistvých. Závěrem přiblížíme postup PČR při řešení samotného problému a upozorníme na důležité kontakty.*

Úvod

V dnešní době je již téměř samozřejmostí, že každá domácnost je vybavena počítačem. Neustále se snižuje věková hranice, kdy děti začínají s počítačem pracovat. Všichni uživatelé, nejen děti, jsou pak vystaveny negativnímu vlivu masy informací, aniž by měli schopnosti informace kriticky vyhodnotit a zpracovat. Dochází tak k rozšiřování počítačové kriminality v nejrůznějších podobách (cyber-grooming - sexuální obtěžování mladistvých spojené s využitím internetu, cyber-stalking - cílený útok na uživatele realizovaný různými komunikačními kanály, cyber-bullying - elektronická forma psychické šikany, happy slapping – fackování pro zábavu, sexting – elektronické rozesílání SMS, videí a fotografií se sexuálním obsahem, hoaxing a spamming apod).

V souvislosti s problematikou kyberšikany proběhlo i několik výzkumů zaměřených na ukazatele týkajících se daného problému. Velmi zajímavé bylo výzkumné šetření Centra prevence rizikové virtuální komunikace PdF UP a projektu E-Bezpečí Nebezpečí internetové kriminality III. Základní vzorek byl vytvořen uživateli internetu a mobilních telefonů z řad žáků základních a středních škol v celé České republice. Do výzkumu se zapojilo celkem 10 830 žáků ve věku 11 - 17 let.

Z tohoto šetření vyplynulo, že nejčastější formou kyberšikany z pohledu útočníka je útok na účet a dále ponižování, ztrapňování prostřednictvím elektronických prostředků. Obdobné je to i z pohledu oběti, nejčastější formy jsou útoky na účet, ponižování, ztrapňování. Do popředí se však dostává i publikování ponižujících fotografií a videí. Zveřejňování nejrůznějších fotografií je velmi časté také z toho důvodu, že uživatelé (možné oběti) dávají k dispozici velmi citlivý materiál. To znamená, že na internet umisťují své fotografie, poloobnažené fotografie a další velmi osobní materiál. Pro útočníka je pak velmi jednoduché takový materiál různým způsobem zneužít.

Kromě fotografie děti sdělují mnoho svých osobních údajů. Nejčastěji se jedná o jméno a příjmení, díle e-mail a na třetím místě je potom fotografie. Poté následuje i adresa bydliště. Pokud však dítě uvede všechny zmiňované údaje, jak se tomu v mnoha případech děje, je riziko kyberútoku daleko větší.

Virtuální komunikace

Vzhledem k tomu, že děti v dnešní době mají velmi snadný přístup na internet, tráví na něm většinu volného času. Činnost dětí na internetu spočívá především ve virtuální komunikaci pomocí sociálních sítí. Díky této komunikaci se pak snadno stávají obětí nebo původcem kyberšikany. V mnoha případech si však tuto skutečnost vůbec neuvědomují.

To, že si děti neuvědomují možná rizika svého počínání, dokazují i čísla, opět z výzkumného šetření v rámci projektu E-Bezpečí.

Virtuální komunikaci vyhledává 57, 60% dotazovaných dětí.

31,15% je ochotno si přidat na vyžádání neznámou osobu mezi své kontakty,

25,25% bylo požádáno, aby komunikaci udrželo v tajnosti,

66,02% bylo požádáno o fotografii obličeje a 37,75% ji skutečně odeslalo,

43,48% bylo požádáno o osobní setkání a 22,89% tomuto požadavku vyhovělo.

S neznámými lidmi komunikuje na internetu více než polovina respondentů (53,84%). Je potřeba také říci, že ne všechna komunikace musí končit protiprávním jednáním, ale je nutné si uvědomit možná rizika.

Velmi zajímavé jsou výsledky výzkumu právě v otázce osobní schůzky domluvené přes internet.

V rámci průzkumu byly děti dotazovány, zda by šly na osobní schůzku, pokud by je internetový „kamarád“ požádal. Většina respondentů (64,14%) odpověděla, že ne. Přes 35% dotazovaných pak odpovědělo, že ano. Další otázka byla, zda už je někdy někdo pozval na osobní schůzku. Zde byly výsledky poměrně vyrovnané. Přes 41% respondentů odpovědělo, že pozvání dostalo, přes 58% odpovědělo, že ne.

Nejzarážející byly odpovědi v třetí související otázce. Zda již respondent šel na osobní schůzku s „kamarádem“ z internetu. Téměř 53% dětí odpovědělo, že ano. Což se vylučuje s první částí otázek, kde většina odpovídala, že by na schůzku nešla.

Je jasné, že u dětí převládá zvědavost a chtíč poznat někoho nového, seznámit se, najít „lásku“. Riziko svého jednání si neuvědomují, nebo spíše nepřipouštějí. Chtějí to zkusit.

Sociální sítě

Nejčastěji dochází ke kyberšikaně prostřednictvím sociálních sítí, dále potom přes sms.

Přes 91% dětí zná nějakou sociální síť a více než 81% dětí má svůj účet na Facebooku. Zarážející je ovšem to, že přes 56% tvoří děti ve věku 11 – 14 let, přičemž věková hranice pro založení profilu na Facebooku je stanovena na 13 let.

Nejčastější formy kyberšikany

- Cyber grooming – chování, které v dítěti vyvolává falešnou důvěru, pozvání na schůzku a následné zneužití
- Cyberstalking (pronásledování) – opakované intenzivní obtěžování a ponižování spojené s vyhrožováním nebo zastrašováním
- Happy slapping (fackování pro zábavu) – nečekané fyzické napadení osoby spojené s nahráváním na mobilní telefon nebo kameru. Získané video je poté publikováno na internetu
- Vydírání – útočník využívá kyberšikanu k vydírání oběti, čímž se snaží dosáhnout svých záměrů
- Sexting – elektronické rozesílání SMS, fotografií, videa se sexuálním obsahem

Preventivní rady

- Nebýt přehnaně důvěřivý
- Nesdělovat citlivé informace, které by mohly být zneužity (osobní údaje, fotografie, hesla k elektronickým účtům…)
- Seznámit se s pravidly služeb internetu a GSM sítí
- Respektovat ostatní uživatele
- **Ukončit** komunikaci

- **Blokovat** – zamezit útočníkovi přístup k oběti i k dané službě (kontaktovat poskytovatele služby, zablokovat si přijímání útočníkových zpráv nebo hovorů, změnit svou virtuální identitu)
- **Odhalit** pachatele- pokud je to možné, např. podle profilu
- **Oznámit** – oznámit útok dospělým, schovat si důkazy pro vyšetřování (zprávy, odkazy na weby…)
- Nebýt nevšímavý – upozornit na kyberšikanu v okolí
- Podpořit oběti
- Online přátelství jsou nejlepší, když zůstanou online a je naprosto v pořádku odmítnout osobní setkání
- Dvakrát si promysli slib úžasného vztahu a zvaž, zda nehledáš lásku na špatném místě

Rady pro školy

- Zhodnoťte rozsah problému ve vaší škole – dotazníky, rozhovory se studenty..
- Vymezte jasná pravidla používání internetu a mobilních telefonů na vaší škole
- Zahrňte pojem kyberšikana do školního řádu a stanovte potrestání při jejím odhalení
- Potřebná opatření do hodin výpočetní techniky (kontrolní software, blokování některých webových stránek, nefunkčnost flash apod.)
- Vyslechněte oběť kyberšikany
- Poskytněte oběti veškerou podporu a pomoc
- Navrhněte oběti další možný postup
- Snažte se případ dořešit
- Hovořte se žáky o problému kyberšikana
- Důsledně potrestejte viníky

- V případě nutnosti se obraťte na policii

Rady pro rodiče

- Buďte ke svým dětem vnímavý
- Mluvte se svými dětmi
- Sledujte, k čemu vaše dítě užívá komunikační technologie a učte je používat tyto technologie bezpečně
- Nepodceňujte riziko, které kyberšikana představuje, uvědomte si, kam až může vést
- Uchovávejte textové zprávy nebo záznamy online komunikace jako důkazy
- To, že se vaše dítě stalo obětí kyberšikany oznamte škole, správcům internetové služby popř. policii

Kyberšikana a zákon:

Kyberšikana může naplňovat skutkovou podstatu trestných činů (omezování osobní svobody, nebezpečné vyhrožování, nebezpečné pronásledování, ublížení na zdraví, vydírání, znásilnění, pohlavní zneužívání, rasově motivované skutky).

Osoba **mladší 15 let** není trestně odpovědná. Pokud se dopustí jednání, které jinak nese znaky trestného činu, koná se řízení podle **občanského soudního řádu** a soud pro mládež ji může uložit podle zákona č. 218/2003 Sb., (o soudnictví ve věcech mládeže) některá z následujících **opatření**:

- dohled probačního úředníka,
- zařazení do terapeutického, psychologického nebo jiného vhodného výchovného programu ve střediscích výchovné péče,
- ochrannou výchovu
- napomenutí s výstrahou
- výchovné povinnosti

- výchovné omezení

Trestní odpovědnost mladistvých **(15 – 18)** je posuzována soudy pro mládež podle zákona č. 218/2003 Sb. s ohledem na jejich rozumovou a mravní vyspělost osoby, proti níž se vede trestní řízení. Ve věcech mladistvých se neukládá trest, ale **opatření**:

- **Výchovné opatření** – dohled probačního úředníka, probační program, výchovné povinnosti, výchovná omezení, napomenutí s výstrahou
- **Ochranná opatření** – ochranné léčení, zabezpečovací detence, zabrání věci nebo jiné majetkové hodnoty a ochranná výchova
- **Trestní opatření** – obecně prospěšné práce, peněžité opatření, propadnutí věci nebo jiné majetkové hodnoty, zákaz činnosti, vyhoštění, domácí vězení, zákaz vstupu na kulturní, sportovní a jiné společenské akce, odnětí svobody podmíněně odložené na zkušební dobu, odnětí svobody nepodmíněně

Trestně právní odpovědnost

- každý je povinen oznámit trestný čin, neoznámením, nebo nepřekažením se může občan vystavit nebezpečí trestního postihu,
- nikdy nemůžeme předem vědět k jak závažnému jednání (trestnému činu) může, byť i zpočátku zdánlivě bagatelní záležitost, vést, a proto se nikdo nemusí bát své podezření policii oznámit,
- každý policista je povinen přijmout oznámení,
- PČR po oznámení protiprávního jednání, vede prověřování, které směřuje k odhalení pachatele,
- v případě odhalení pachatele a nashromáždění důkazů, je zahájeno trestní stíhání obviněného, nebo v případě přestupku, zahájeno přestupkové řízení,
- orgány činné v trestním řízení (policie, státní zastupitelství, soudy) dle zákonných ustanovení vedou svoji činnost tak, aby byly náležitě zjištěny trestné činy a jejich pachatelé podle zákona spravedlivě potrestání,

- policie, za účelem odhalení trestné činnosti a pachatelů, je dle zákonných ustanovení oprávněna používat mnoho prostředků, kdy v případech kyberšikany se jedná zejména o zjištění telekomunikačního provozu, provádění domovních prohlídek spojených se zajištěním výpočetní techniky a dat a jejich následné znalecké zkoumání,
- soudy v odsuzujících rozsudcích ukládají tresty dle trestního zákoníku,
- za páchané trestné činy může soud uložit tresty: odnětí svobody (nepodmíněné/podmíněné), domácí vězení, obecně prospěšné práce, propadnutí majetku, peněžitý trest, propadnutí věci nebo jiné majetkové hodnoty, zákaz činnosti, zákaz pobytu aj.
- každý člověk, který přistupuje do sítě internet, je zodpovědný za své jednání v síti a musí si uvědomit, že se může stát jak obětí, tak pachatelem.

Kyberšikana a související zákony

40/1964 Sb. OBČANSKÝ ZÁKONÍK

Ochrana osobnosti

§ 11 Fyzická osoba má právo na ochranu své osobnosti, ...

§ 12 (1) Písemnosti osobní povahy, podobizny, obrazové snímky a obrazové a zvukové záznamy týkající se fyzické osoby nebo jejích projevů osobní povahy smějí být pořízeny nebo použity jen s jejím svolením.

(2) Svolení není třeba, ... k účelům úředním na základě zákona.

(3) Podobizny, obrazové snímky a obrazové a zvukové záznamy se mohou bez svolení fyzické osoby pořídit nebo použít přiměřeným způsobem též pro vědecké a umělecké účely a pro tiskové, filmové, rozhlasové a televizní zpravodajství. ...

§ 13 (1) Fyzická osoba má právo se zejména domáhat, aby bylo upuštěno od neoprávněných zásahů ...

(3) Výši náhrady podle odstavce 2 určí soud s přihlédnutím k závažnosti vzniklé újmy a k okolnostem, za nichž k porušení práva došlo.

ZÁKON 101/2000 Sb. o ochraně osobních údajů

§3 Působnost zákona

(1) Tento zákon se vztahuje na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby.

(2) Tento zákon se vztahuje na veškeré zpracování osobních údajů, ať k němu dochází automatizovaně nebo jinými prostředky.

(3) Tento zákon se nevztahuje na zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní potřebu.

(4) Tento zákon se nevztahuje na nahodilé shromažďování osobních údajů, pokud tyto údaje nejsou dále zpracovávány.

§ 4 Vymezení pojmů

a) osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat ...

b) **zpracováním osobních údajů je jakákoliv operace nebo soustava operací, které správce nebo zpracovatel** systematicky provádějí s osobními údaji, ... **zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace,**

SPRÁVNÍ DELIKTY

§ 44 (2) Fyzická osoba se jako správce nebo zpracovatel dopustí přestupku tím, že při zpracování osobních údajů

e) zpracovává osobní údaje bez souhlasu subjektu údajů mimo případy uvedené v zákoně

(2) Za přestupek podle odst. 1 lze uložit pokutu do výše 1 000 000 Kč.

(3) Za přestupek podle odstavce 1 spáchaný tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem lze uložit pokutu do 5 000 000 Kč.

ZÁKON 359/1999 Sb. o sociálně-právní ochraně dětí

§ 10 odst. 4) Státní orgány, pověřené osoby**, <u>školy, školská zařízení</u>** a zdravotnická zařízení, popřípadě další zařízení určená pro děti **<u>jsou povinny oznámit obecnímu úřadu</u>** obce s rozšířenou působností skutečnosti, které nasvědčují tomu, že jde o **<u>děti</u>** uvedené v § 6 odst. 1, a to bez zbytečného odkladu po tom, kdy se o takové skutečnosti dozví.

§ 6 odst. 1) Sociálně-právní ochrana se zaměřuje zejména na děti,

c) které vedou zahálčivý nebo nemravný život spočívající zejména v tom, že zanedbávají školní docházku, nepracují, i když nemají dostatečný zdroj obživy, požívají alkohol nebo návykové látky, živí se prostitucí, spáchaly trestný čin nebo, **jde-li o děti mladší než patnáct let, spáchaly čin, který by jinak byl trestným činem,4) opakovaně nebo soustavně páchají přestupky nebo jinak ohrožují občanské soužití;**

Projekt BEZPEČNĚ V KYBERPROSTORU

Hlavním cílem je omezení rozšiřování nebezpečných počítačových jevů. Vedlejší cíle projektu jsou zvyšování informovanosti občanů JMK a jejich motivace k aktivnímu přístupu pro zajišťování vlastní bezpečnosti a ochrany majetku a dále provázání jednotlivých složek škola, obec, policie při řešení nebezpečných komunikačních jevů.

Cílovou skupinou jsou všichni uživatelé počítačů.

Realizátor projektu je Jihomoravský kraj ve spolupráci s Krajským ředitelstvím policie Jihomoravského kraje a Městskou policií Brno.

Spolupracujícími subjekty jsou Pedagogicko-psychologická poradna Brno, Střední škola dopravy, obchodu a služeb Moravský Krumlov, Orgán sociálně právní ochrany dětí, Městské státní zastupitelství Brno.

Projekt je realizován formou seminářů pro ředitele škol, učitele IT, školní metodiky prevence, veřejnost, žáky ZŠ a SŠ v JMK.

Všichni jsou seznámeni s nebezpečnými komunikačními jevy a postupy obrany proti nim.

Součástí projektu je výukové dvd, informační letáky

Skimming

Jako „skimming“ je označováno podvodné jednání, při kterém pachatelé (padělatelé platebních karet) zkopírují údaje z magnetického proužku karty bez vědomí právoplatného držitele karty. Tyto údaje následně nahrají na novou padělanou platební kartu

Rizika elektronické komunikace

Spam

SPAM je NEVYŽÁDANÉ (většinou obchodní) sdělení šířené zpravidla internetem.

Tvoří podle různých výzkumů 50 – 90 % veškeré komunikace.

Obchodním sdělením (se rozumí) všechny formy sdělení určeného k přímé či nepřímé podpoře zboží či služeb nebo image podniku fyzické či právnické osoby, která vykonává regulovanou činnost nebo je podnikatelem vykonávajícím činnost, která není regulovanou činností; za obchodní sdělení se považuje také reklama podle zvláštního právního předpisu. Za obchodní sdělení se 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.

Rozvrstvení témat nevyžádané pošty (společnost Clearswift)

- 40 % - péče o zdraví
- 37,8 % - finanční informace
- 12,8 % - přímé produkty
- 4,8 % - pornografie

Ne každá reklama, kterou považujete za nevyžádanou, musí být SPAM. Stačí, když jednou nakoupíte třeba v internetovém obchodě a při nákupu souhlasíte s obchodními podmínkami (ty stejně nikdo nečte)

Obrana proti spamu

- Prostředky technické

Nepřeposílejte řetězové e-maily!

Neuvádějte svůj e-mail na nedůvěryhodných stránkých

Přidejte spamery na BlackList

Používejte antispamové filtry

Vytvoření nového e-mailového účtu

Prostředky technické

Denně chodí na Váš email desítky nebo stovky SPAMů. Většina těchto e-mailů je odfiltrována anti-SPAMovými filtry přímo na internetových serverech.

Ty, které dorazí do Vaší schránky, jsou pak často automaticky ukládány a složky SPAM.

Prostředky právní

- Prostředky právní

V České republice reguluje nevyžádaná obchodní sdělení zákon č. 480/2004 Sb., o některých službách informační společnosti. Za zasílání spamu zákon umožňuje udělit sankci ve výši až 10 000 000 Kč. Orgánem pověřeným výkonem dozoru nad dodržováním ustanovení zákona, která se týkají nevyžádaných obchodních sdělení, je Úřad pro ochranu osobních údajů

Hoax

(anglické slovo hoax označuje podvod, mystifikaci či žert) je 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.

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.)

Oficiálně z banky: Jakmile se ocitnete v kritické situaci a musíte pod nátlakem vybrat peníze z bankovního automatu na požádání/přinuceni násilníkem, zadejte svůj PIN opačně: to je od konce - např. máte-li 1234, tak zadáte 4321, automat vám peníze přesto vydá, ale též současně přivolá policií, která vám přijde na pomoc. Tato zpráva byla před nedávnem vysílaná v TV, protože málo lidí využívalo tuto skutečnost, protože o tom nevěděli. Přepošlete toto co nejvíce lidem.

Nepřidávejte si do kontakt listu na ICQ uživatele xxx-xxx-xxx. Je to vir a po udělení autorizace vám smaže všechna data na disku, včetně kontaktů na ICQ a automaticky se rozešle všem vašim přátelům.

Od xx.xx.xx bude ICQ placené!! Ale ještě máte šanci s tím něco udělat, podepište petici na www.xxx.com!! Potom odešlete tuto zprávu x lidem a stiskněte F1. Vaše ikonka zmodrá a placení se vám vyhne.

Obtěžování příjemců – Opakovaný příjem nesmyslných zpráv je pro mnohé uživatele nepříjemný, zejména v době epidemie, kdy se v emailových 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.

Zbytečné zatěžování linek a serverů – V době, kdy je nějaký „módní“ hoax na vrcholu popularity, může zbytečně generovat vysokou zátěž počítačových sítí a serverů.

Ztráta důvěryhodnosti – Odesílatel nepravdivých zpráv ohrožuje svou důvěryhodnost, zvláště pokud takové zprávy odesílá z pracovního emmailu. 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.

Obrana proti Hoaxu

je komplikovanější o fakt, že je nutné Hoax rozlišit od dalších zpráv. Hoaxy Vám totiž přicházejí od Vašich přátel a známých.

Platí dvě jednoduchá pravidla:

Důvěřujte pouze takovým zprávám, které přicházejí od lidí, o kterých jste přesvědčeni, že jsou v daném oboru odborníky.

Pokud zpráva vybízí k dalšímu rozesílání, jedná se téměř vždy o hoax.

Phishing

je podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) v elektronické komunikaci. K nalákání důvěřivé veřejnosti komunikace předstírá, že pochází z populárních sociálních sítí, aukčních webů, on-line platebních portálů nebo od IT administrátorů.

Na odkazy v e-mailu neklikejte! Přesměrují vás na podvodné stránky, které se vás mohou snažit oklamat a pokusit se vylákat důvěryhodné informace, ale také mohou obsahovat škodlivé kódy, které se vám pokusí instalovat do počítače.

Jestliže potřebujete vstoupit na stránky internetového bankovnictví nebo na stránky příslušné organizace, raději napište internetovou adresu do prohlížeče sami!

Pokud se vaše elektronické bankovnictví chová nestandardně nebo jsou po vás požadovány jiné údaje než obvykle, nezadávejte je! Ukončete svoji činnost a kontaktujte zákaznické centrum banky! Existuje další trik podvodníků, tzv. pharming. Ten umožňuje přesměrovat uživatele na podvodné stránky, aniž by si toho všimnul a to i za předpokladu, že dodrží oba předchozí body.

Používejte aktualizovaný operační systém.

Používejte antivirový program. Aktualizujte ho!

Nespouštějte neznámé programy, které vám příjdou e-mailem, ani na které e-mail odkazuje! Dodržujte nejvyšší opatrnost, přestože zpráva může vypadat, že je od vašich nejbližších přátel.

K elektronickému bankovnictví nebo ke svým účtům (nejen bankovním) se nepřihlašujte z veřejně přístupných nebo nedůvěryhodných počítačů, které nemáte pod kontrolou.

Jestliže nemůžete mít pro svoji práci svůj počítáč, který nesdílíte s ostatními členy rodiny, mějte každý svůj účet. Uživatelům nepřidělujte práva administrátora! Získáte tím částečnou ochranu před nežádoucími úpravami systému.

Používejte svůj rozum a zdravý úsudek! Pamatujte, útočníci jsou vždy o krok napřed a stále zkoušejí nové triky, jak vás nachytat! I přes veškeré technologické zabezpečení se může objevit jednoduchý trik, kterým se vás mohou snažit obelstít. Jestliže nebudete dodržovat základní bezpečnostní pravidla a nepřemýšlet nad svojí činností, můžete se stát další obětí.

Zabezpečení a zefektivnění práce s ICT

Naše cíle:

- Maximální zefektivnění práce s informačními technologiemi
- Zkvalitnění práce
- Maximální časová úspora
- Minimalizace nákladů spojených s ICT
- Maximální zabezpečení vlastích dat

Ochrana dat:

- Ochrana dat před ztrátou
- Ochrana dat před zneužitím

Zálohování:

- Disková pole – NAS
- Zálohování – ochrana dat před ztrátou
- Záloha na CD (DVD)
- Záloha na USB flashdisk
- Záloha na pevný disk v počítači
- Záloha na externí pevný disk
- Cloudová řešení

Cloudová řešení

Klady:

- Data jsou velmi dobře chráněna proti poškození
- K datum je možno přistupovat odkudkoli

- Data je možno sdílet
- Není nutný neustálý přístup k internetu

Zápory:

- Data jsou uložena u cizí osoby
- Nemůžeme ovlivnit případný výpadek na straně poskytovatele služby
- Omezená velikost prostoru (zdarma)

Microsoft (www.live.com)

- Dokumenty
- Word
- Excel
- Powerpoint
- Fotogalerie
- Kalendář
- Zabezpečení rodiny
- Silverlight
- Photosynth (Image copmosite editor)
- Live Fotogalerie
- Live Movie Maker

Google Google - účet

- Gmail
- Google – přehled shromažďovaných informací
- Google – Chrome
- Google – trends
- Google – public data

- Google drive
- Google – Dokumenty (sdílení, formuláře) Offile, formuláře
- Google+
- Google SketchUP

Seznámení s operačním systémem Linux. Co je to linux. Srovnání s MS Windows.

Digitální fotografie

Základní principy fungování digitálních fotoaparátů. Vliv délky času a clony na výsledný snímek.

Nejčastější vady fotografií – podexponovaná, přeexponovaná, rozmazání, zrnitost.

Uložení fotografie a zápis metadat. Význam metadat pro budoucí zpracování fotografie.

Pokročilé funkce kancelářských aplikací

- Tvorba automatického obsahu
- Odkazy na použitou literaturu, poznámky pod čarou
- Základy tvorby maker
- Hromadná korespondence

ROZVOJ ICT GRAMOTNOSTI S DOPADEM NA PREVENTIVNÍ POSTUPY V OBLASTI PREVENCE ŠIKANY A KYBERŠIKANY

autor: Mgr. Michal Hodovský
žadatel: Českomoravská vzdělávací, s.r.o.