Zounek, Jiří

Základy zálohování dat a bezpečnosti ve virtuálním světě (aneb jak předejít katastrofě)

In: Lojdová, Kateřina; Novotný, Petr; Trnková, Kateřina; Šeďová, Klára; Švaříček, Roman; Zounek, Jiří. *Psaní odborných textů : průvodce tvorbou ročníkové práce na Ústavu pedagogických věd FF MU.* Trnková, Kateřina (editor). 1. vyd. Masarykova univerzita, 2014, pp. 61-70

ISBN 978-80-210-6863-6; ISBN 978-80-210-6866-7 (online : Mobipocket)

Stable URL (handle): https://hdl.handle.net/11222.digilib/130764
Access Date: 26. 03. 2025
Version: 20220831

ZÁKLADY ZÁLOHOVÁNÍ DAT A BEZPEČNOSTI VE VIRTUÁLNÍM SVĚTĚ (ANEB JAK PŘEDEJÍT KATASTROFĚ)

Jiří Zounek

ÚVOD

Počítač, notebook, skener, diktafon, internet, elektronické databáze či sociální sítě jsou dnes nedílnou součástí „dílny" každého studenta i učitele. Všechny uvedené digitální technologie, nástroje či online služby jsou bezesporu velkými pomocníky a studium již bez nich není myslitelné (a prakticky celý život). Nesmíme ovšem zapomínat také na fakt, že každá mince má svůj rub. Stejně tak využívání digitálních technologií sebou nese i mnohá negativa či nebezpečí. V naprosté většině případů jde o negativa, za nimiž stojí člověk/uživatel, který „zneužívá" možností technologií, není to tedy vlastnost těchto technologií. Dále je nutné si uvědomit, že není možné se bezhlavě spoléhat na technologie. Jak se říká, je jisté, že se váš počítač či jeho pevný disk rozbije, je jenom otázkou kdy. A věřte, bude to v ten nejnevhodnější okamžik.

PROČ ČÍST TUTO KAPITOLU

Tato kapitola má poskytnout čtenáři základní přehled o problematice ukládání dat, jejich zálohování, ale také o otázkách bezpečnosti ve virtuálním prostoru. **Text si neklade za cíl nahradit návody, jak konkrétně ovládat ten či onen program či systém**. **Cílem textu je uvést čtenáře/uživatele digitálních technologií do uvedené problematiky tak, aby byl po přečtení kapitoly schopen mnohé kroky podniknout sám, případně aby si uvědomil možná rizika a obrátil se s konkrétním dotazem například na zdatnějšího kolegu či odborný servis**. To vše předpokládá aktivní přístup čtenáře/uživatele k těmto otázkám. Tím může být kontrola vlastního počítače, zabezpečení svého profilu na sociální síti nebo instalace zálohovacího programu. To už záleží na každém čtenáři, protože jde o mnohdy velmi individuální situace a postupy.

Mnozí si nyní říkají, že nešli studovat filozofickou fakultu, aby se učili zabezpečovat počítač. To jistě ne! Pokud si je čtenář jist, že má dobrý přehled o této tématice, může klidně celou kapitolu přeskočit. Nicméně těm, kdo si nejsou příliš jistí, doporučuji číst pozorně a poté konat. Zabrání tak možná katastrofě v podobě smazané nebo ztracené takřka hotové ročníkové či diplomové bakalářské práce. Navíc mnohá nastavení zvládne většina čtenářů vlastními silami. S některými může případně pomoci kolega nebo odborník.[7]

ZABEZPEČENÍ POČÍTAČE A AKTUALIZACE PROGRAMOVÉHO VYBAVENÍ (ANEB „MŮJ DŮM, MŮJ HRAD“)

Využívání počítače, notebooku, mobilu je tak samozřejmé a časté, že si mnohdy neuvědomujeme potřebu tyto přístroje také nějakým způsobem chránit. A nejde jenom o přístroje samotné, ale zejména o data, která v nich máme uložená. Je to podobné jako s naším domem nebo bytem. Běžnou věcí je, že naše domy či byty zamykáme. Podobně je to s digitálními přístroji. V počítači či mobilu máme místo klíče heslo, případně různé kódy nebo dokonce čtečky otisků prstů. Vždy záleží, jaký přístroj máme, protože výrobci používají odlišné zabezpečovací technologie.[8]

Obecně lze ale doporučit používat hesla všude, kde je to možné nebo účelné. Například po zapnutí počítače bychom se měli setkat s prvním heslem. Podobně u mobilu či notebooku. Doporučujeme chránit heslem i přístup k nastavení počítače, v případě nutnosti zabezpečit heslem i důležité soubory. Možná se tato doporučení jeví jako lehce paranoidní, ale náhoda ...

Vytvořit heslo není těžké, ale měli bychom dodržet několik zásad:

- nepoužívat svoje jméno, rok narození, řadu čísel (typicky 1234, AAAAA apod.), prostě cokoliv, co lze jednoduše odhadnout;
- důležitá je délka hesla, doporučovaná délka hesla je minimálně osm až deset znaků;

7 Některé názvy použité v této kapitole mohou být registrovanými ochrannými známkami nebo obchodními značkami, které jsou majetkem svých vlastníků.

8 Nebudeme se zde více zmiňovat o nutnosti fyzické ochrany zařízení před ukradením či jiným poškozením (pádem, vysokou teplotou v autě aj.). Zde odkazujme na návody k užívání jednotlivých zařízení, případně webové stránky.

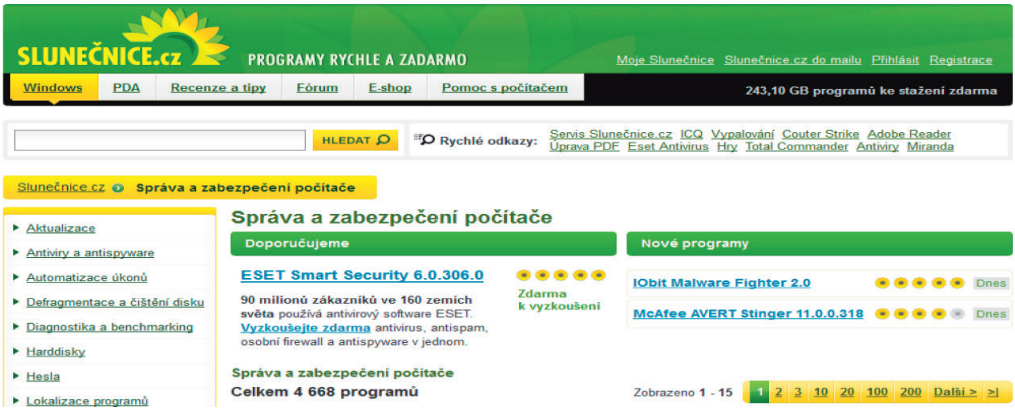
- heslo by mělo obsahovat malá i velká písmena, alespoň jednu číslici a dále nestandardní znak (plus, pomlčku, závorku aj.), tedy např. Ksh6nv+e-ds)q;
- heslo nikomu nesdělovat, a už vůbec ne poslat emailem, nelepit heslo na papírky u počítače či kamkoliv jinam, kde je možné odhadnout, k čemu ona změť písmen a čísel může být;
- heslo by se mělo pravidelně měnit, heslo pro vstup do počítače může zůstat delší dobu (záleží, také, zda daný přístroj používá jeden uživatel či více), ale u hesel používaných na internetu by se měla hesla měnit častěji (hesla je možné pomocí různých technologií „odposlouchávat", takže opatrnost je na místě).

Dům či byt (případně jejich zařízení) je nutné tu a tam opravit nebo něco vyměnit či inovovat. Podobně je tomu i s počítačem nebo notebookem, případně telefonem. Jednou z nejdůležitějších součástí počítačů je **operační systém**. Jde poměrně o složitý program, do něhož se občas vloudí chyba, kterou je nutné opravit (tyto chyby mohou být zneužity např. pro šíření virů apod.). Takovým opravám se říká záplaty bezpečnostních děr. Pokud jde o větší množství takových záplat v jednom souboru, pak se hovoří tzv. servis packu. Je proto velmi užitečné **nastavit v počítači automatické kontroly nových aktualizací**. Pokud je k dispozici nová aktualizace, je uživatel upozorněn a po schválení se aktualizace provede prakticky bez vědomí uživatele (někdy je nutné počítač restartovat).

Podobně je to i s ostatními programy, které jsou v zařízení nainstalované. Také v případě programů (např. internetový prohlížeč, textový editor aj.) se občas objeví chyba, kterou je nutné opravit. Případně vyjde nová verze daného programu obsahující lepší zabezpečení a nové funkce, takže je rovněž vhodné program aktualizovat. Je možné kontrolovat aktualizace programů ručně, nebo používat nástroje, které to dělají za uživatele (např. Secunia Personal Software Inspector[9] nebo OUTDATEfighter[10]). Vždy je dobré se ale podívat například na internet, jaké mají ostatní uživatelé zkušenosti s novými verzemi programů (i třeba se zmíněným programem Secunia nebo OUTDATEfighter). Ne vždy je nová verze lepší, může se stát, že i nová verze obsahuje chybu, kvůli níž je lepší zůstat u původní verze (počkat až na další opravenou verzi). Tyto informace a diskuze jsou na portálech, na nichž si lze nové programy či aktualizace stáhnout. Jde například o Slunečnice.cz (http://www.slunecnice.cz/), Sosej.cz (http://www.sosej.cz/), FileHippo (http://www.filehippo.com/) nebo třeba portál časopisu CHIP (http://download.chip.eu/cz/).

9 http://secunia.com/vulnerability_scanning/personal/.
10 http://www.spamfighter.com/OUTDATEfighter/.

Obrázek č. 1: Portál Slunečnice (sekce Správa a zabezpečení počítače)



Nezbytnou součástí programového vybavení počítače je **antivirový software**[11]. Naštěstí je k dispozici mnoho antivirových programů, které jsou dostupné zdarma. Je dobré vědět, že některé české produkty jsou již světově známé (např. Avast[12] nebo AVG[13]). Další antivirové programy jsou dostupné na uvedených portálech (např. Sosej.cz), kde je možné si antivirový program stáhnout zdarma (typicky pro domácí použití), nebo vyzkoušet tzv. zkušební verzi (funkčnost omezena např. na 15 dní, po uplynutí lhůty je nutné za program zaplatit). Je dobré zvážit, zda mi opravdu stačí verze programu zdarma. Ta nemusí obsahovat všechny funkce ve srovnání s placenou verzí. Rovněž je nutné zvážit, zda opravdu používám počítač pouze pro domácí účely. Pokud je zařízení používáno k výdělečné činnosti, měl by uživatel používat adekvátní verze programů (typicky placené).

Dále je vhodné zdůraznit, že stejně jako počítače a notebooky, **je nutné chránit pomocí antivirového programu i mobilní zařízení (mobil, tablet)**. Většina antivirových programů existuje i ve verzi pro mobilní zařízení, ať už využívá systém Windows Phone (dříve Windows Mobile), Android nebo iOS (Apple) či jiné.

Viry však nejsou zdaleka jedinými nebezpečnými programy. Může jít např. o tzv. trojské koně. To jsou programy, které mohou provádět zcela záslužnou činnost (informovat nás o stavu sněhu na horách), ale přitom ještě dělá jinou, méně potřebnou ba dokonce nebezpečnou, činnost z pohledu uživatele počítače. Jedním typem takových programů

11 V rámci této kapitoly se nebudeme podrobněji věnovat druhům virů, jejich šíření apod. Zájemci najdou informace v literatuře na konci kapitoly nebo na internetu, např. na Wikipedii (http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_virus).

12 Více viz http://www.avast.com/cs-cz/index.

13 http://www.avg.com/cz-cs/homepage.

je tzv. **spyware**, který shromažďuje různé informace a odesílá je bez vědomí uživatele někomu jinému. Jiným typem je tzv. **adware** – ten vedle své běžné činnosti zobrazuje reklamu. Některé programy mohou být spyware i adware dohromady, ovšem ne každý adware je současně spyware (Doseděl, 2005). Zákeřné je zde to, že si je „pustíme" do počítače sami a často ochotně společně s instalací nějakého programu. Trojský kůň je buď součástí stahovaného programu, nebo jde o jeho doplněk. Z tohoto důvodu **je vždy dobré sledovat informace při instalaci nových programů**, protože někdy můžeme takový doplněk odhalit velmi snadno – instalační program se ptá, zda chceme to či ono nainstalovat. Je dobré velmi zvažovat instalaci doplňku (ne všechny jsou samozřejmě nebezpečné), v některých případech je vhodné instalaci úplně ukončit a zeptat se na daný program například zkušenějšího kolegy či hledat na internetu. Čas věnovaný tomuto hledání se může vyplatit. Spyware totiž může „najít" a odeslat vaše hesla či přístupové údaje do bankovních účtů apod. Obecně je možné říci, že **nikdy není dobré už jenom otevírat podezřelé programy z internetu**.

V případě, že už k nákaze došlo (začaly se objevovat podivné reklamy apod.), je nutné spustit program určený k odstraňování těchto škodlivých programů. Je možné využívat například Spybot - Search & Destroy[14] nebo Ad-Aware[15] (takových programů je daleko více). Tyto programy se ovládají poměrně snadno, takže vyčištění počítače je jednoduché. Opět platí: **Pokud si nejsem jistý, co dělat, ptám se kolegů, volám servis. Neřešení této situace může mít velmi neblahé následky**.

Neexistuje ovšem návod, který by 100 % zaručil, že zařízení zůstane neustále bez potíží, protože například viry jsou stále sofistikovanější. **Pokud však dojde k vážnému poškození počítače, ať už virem nebo poruchou hardware (přestane fungovat pevný disk, porouchá se napájení počítače apod.), je nutné vyhledat odbornou pomoc**. Žádné poškození počítače by nemělo uživatele zaskočit, protože by měl mít veškerá svoje data (rozepsanou ročníkovou nebo dokonce bakalářskou/magisterskou práci) zálohována a neztratí to nejdůležitější – svoji práci. O ukládání a zálohování dat je následující kapitola.

14 http://www.safer-networking.org/.
15 http://www.lavasoft.com/.

UKLÁDÁNÍ A ZÁLOHOVÁNÍ DAT (ANEB JAK NEPŘIJÍT O VLASTNÍ SOUBORY)

V minulé kapitole jsme se zabývali zabezpečením počítače a do jisté míry i prevenci proti různým nebezpečím. Jedním z velkých nebezpečí při využívání digitálních technologií jsme ale my sami, tedy uživatelé! Celá řada nešťastných nehod, jako například náhodné smazání souboru s celodenní prací, jde z velké části na vrub nezkušenosti nebo nepozornosti uživatele. Nesmíme ovšem také zapomínat, že počítače, notebooky, mobily, tablety jsou jenom „stroje" s určitou životností a s chybami. Kdo si myslí, že má nový notebook a ten mu bude sloužit bez chyb po léta, je na velkém omylu. **I zcela nové zařízení může po několika dnech zkolabovat, protože dojde k neopravitelné poruše pevného disku**, který je pak nutné vyměnit, a data z něho nejdou obnovit[16]. Nicméně: Obnova dat z poškozeného disku je možná, ale stojí poměrně mnoho peněz a pozitivní výsledek není vždy zaručený. Proto se vyplatí zálohovat, což ve výsledku stojí méně peněz (a prakticky žádné nervy). Neobstojí ani názor, že se mi pět let nic nestalo, tak proč řešit zálohy. Až dojde ke ztrátě dat, tak si teprve uvědomíme, jak byla data cenná a co vše jsme měli uloženo ve svém počítači či notebooku. Nemusí to být pouze soubory s rozepsanou ročníkovou prací, ale také rodinné fotky, videa, filmy nebo hudba – taková ztráta pak opravdu bolí.

Ukládání souborů

Jedním ze základních východisek efektivního využívání počítačů při psaní ročníkových prací (ale platí to obecně) je **„pořádek" v souborech a složkách**. Není nic horšího, než chaotické ukládání souborů. V takovém případě je velká pravděpodobnost, že některé soubory nenajdeme, nebo ho omylem smažeme jako nepotřebný. Lze tedy doporučit vytvoření struktury adresářů a podadresářů, do nichž pak lze ukládat soubory. Struktura může být rozdělena na „pracovní" a „osobní" složku. Pracovní složka pak může být dále členěna podle studovaných předmětů či kurzů, podle ročníků studia apod. Zde záleží na uživateli, co mu vyhovuje.

Při samotném psaní je výhodné pojmenovat soubor podle data, kdy byl vytvořen nebo uložen. Takže například soubor vytvořený 27. 5. 2013 může mít název 2013_05_27_rocnikova_prace. Je samozřejmě možné dodat i čas uložení. Tento postup má obrovskou výhodu v tom, že se můžete vrátit k dříve uložené kopii, takže v případě havárie počítače

16 Autor textu má tuto zkušenost. Pevný disk v novém počítači měl životnost deset dnů! Po deseti dnech přestal pracovat a byla nutná jeho výměna, přičemž se nejednalo o levný disk.

(a uložení starší verze souboru na jiné médium) ztratíte „pouze" určitou část práce. Případně se můžete vrátit ke starší kopii, pokud zjistíte, že obsahuje něco, co můžete ještě potřebovat a v nové jste to již vymazali atp.

Zálohování dat na „tradiční" média

Již několikrát bylo zmíněno, že je důležité zálohování. Dobrým základem je **nastavení vytváření automatických záloh souborů** (např. u textového editoru). To ovšem nestačí, protože typicky se tyto zálohy ukládají na stejný pevný disk. V případě havárie či krádeže tak přicházíme o všechny soubory. Je proto nezbytné vytvářet zálohy na jiná média. Na tomto místě je nutné zdůraznit, že **„fleška" (Flash disk) je médiem pro zálohování naprosto nevhodným!** Životnost tohoto média je velmi problematická. Navíc ztráta této malé věcičky je poměrně běžný problém. V současnosti je ještě možné **zálohovat data jejich vypálením na DVD** (snad ještě i na CD), ale ta mají poměrně malou kapacitu. Pokud si však chcete vypálit pouze textové dokumenty, pak je možné DVD určitě použít. Ovšem i zde pozor na životnost! Některé DVD přestanou být čitelná již po několika letech (zejména při nevhodném uskladnění, např. na slunci).

V dnešní době se **pro zálohování dat** jeví jako velmi vhodný **externí pevný disk**, který připojíme k počítači nebo notebooku kabelem USB (nyní už i USB 3.0, které je poměrně rychlé) nebo i bezdrátově. Pokud máme 500 GB pevný disk v počítači a koupíme si externí disk o stejné velikosti, tak můžeme celý pevný disk v počítači zálohovat na externí disk. Lze tak učinit prostým ručním kopírováním souborů. Existuje však pohodlnější cesta, kterou je automatické zálohování. Na internetu je k dispozici celá řada programů určená k automatickému zálohování (např. Cobian Backup[17]), přímo v MS Windows je nástroj nazvaný Zálohování a obnovení, ale je možné využít i programy, které jsou připravené na externím disku hned při jeho nákupu. Nastavení automatických záloh bývá poměrně snadné, je ale nutné zvažovat, co všechno chce uživatel zálohovat (jednotlivé soubory, celé adresáře, celý pevný disk). Specializované programy navíc provádí tzv. přírůstkové zálohy, když zálohují pouze nové soubory a nevytvářejí vždy kompletní zálohu. Vše je ovšem otázkou nastavení zálohovacího programu. Je-li používán k ukládání záloh pevný disk, může být problém s tím, že tento disk zůstává blízko počítače nebo notebooku. Takže v případě vykradení bytu nebo požáru o data uživatel přijde (to i v případě krádeže tašky s notebookem, v jejíž jedné kapse byl externí disk). Jako jedno z nejlepších řešení tedy je, mít externí disk mimo byt, nechávat ho na bezpečném místě (u kamarádů, u rodičů – každý musí zvážit, které místo je bezpečné). Pak je ovšem poměrně nepraktické pro externí disk jezdit a vozit ho sem a tam.

17 http://www.cobiansoft.com/cobianbackup.htm.

Zálohování do „oblak" (cloudová úložiště)

Nevýhody zálohování na externí disk mohou být důvodem k tomu, proč se nyní stále více prosazuje zálohování do tzv. cloudu, tedy do online úložišť (datových úložišť na internetu). K nejznámějším cloudovým uložištím patří Dropbox[18] (zdarma uživatel získá poměrně dost prostoru, přinejmenším pro textové dokumenty). Navíc existují různé možnosti, jak si tuto kapacitu navýšit (více informací je přímo na webu této služby). Podobné služby nabízí Microsoft OneDrive[19] nebo třeba Google Drive[20]. Vytvořené soubory je možné opět ručně kopírovat do cloudového úložiště nebo si nastavit zálohování jako synchronizaci, tedy soubor je v okamžiku vytvoření **nahráván do cloudu. Zde může být dostupný i z jiných počítačů. K těmto souborům se mohou dostat spolužáci** (editovat ho, stáhnout), pokud jim to autor souboru povolí a nastaví sdílení daného souboru či složky. Výhodou je, že je záloha fyzicky oddělenou od místa, kde uživatel pracuje, takže zničení notebooku neznamená zničení souborů. Nevýhodou je, že nemáte pod kontrolou hardware ani software takového úložiště a hrozí zde i „krádež" dat. Proto by měl každý **dobře zvážit, jaká data bude do cloudu zálohovat**. Určitě tam nepatří citlivá osobní nebo firemní data. Pokud už chcete takto zálohovat citlivá data, je nutné taková data šifrovat. K tomuto účelu opět existuje celá řada programů, které je možné stáhnout na internetu. Příkladem takového programu je známý PGP[21], který ve verzi pro počítače umí zašifrovat emaily, pevné disky nebo třeba sdílené adresáře (podobným programem je Cryptext). Zašifrovat data jde i pomocí nástrojů, které obsahuje např. Windows XP či ve Windows 7.

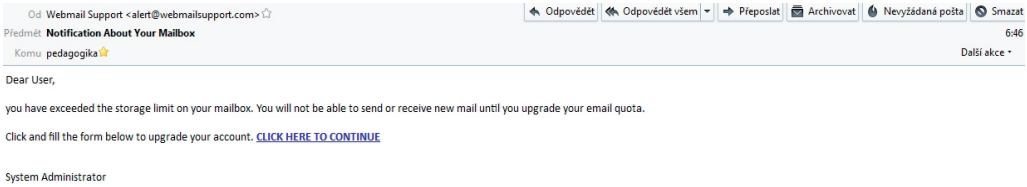
PRAVIDLA BEZPEČNOSTI V DIGITÁLNÍM SVĚTĚ

Svět digitálních technologií se velmi rychle mění, je proto velmi těžké definovat jakákoliv obecná bezpečnostní pravidla. Jde však o oblast natolik závažnou, že je v rámci této kapitoly nezbytné alespoň některá pravidla či doporučení nastínit[22].

18 https://www.dropbox.com/
19 https://onedrive.live.com/about/cs-cz/
20 https://drive.google.com/
21 http://www.pgp.cz/
22 Čerpám zde ze mimo jiné také ze seminární práce L. Lichtera, která vznikla v rámci předmětu Informační a komunikační technologie ve vzdělávání II v jarním semestru 2012 (vyučující J. Zounek).

- Rozmyslete si, **zda je nutné pro danou službu** (např. při registraci apod.) **vyplňovat všechna svá osobní data**.
- Své **heslo neposkytujte jiným lidem, a to ani poskytovateli služeb**. Pozor na podvodné emaily, které se snaží vaše z vás heslo či přístupové údaje vylákat (správce pošty či administrátor ve škole po vás heslo nikdy nebude chtít).

Obrázek č. 2 **Ukázka podvodného emailu**



- **Nereagujte na anonymní emailové zprávy, ani neklikejte na odkazy v nich uvedené, neotvírejte žádné „divné" přílohy**. Nevyžádanou poštu přímo smažte.
- **Pokud Vám přijde divný email od známé osoby** (navíc s přílohou), **neotvírejte přílohu a raději zavolejte kolegovi** nebo kamarádovi, zda vám opravdu takový email poslal.
- **Čtěte licenční ujednání služeb nebo alespoň důležité odstavce o osobních údajích a ukončení poskytování služeb** (u některých služeb se např. vámi zaslané soubory se stávají majetkem poskytovatele služeb).
- **Skryjte své osobní údaje na Facebooku před veřejností** a nepoužívejte aplikace třetích stran.
- **Zasílejte a sdílejte jen ty soubory, na které máte autorské právo**.
- **Dávejte pozor na to, co nahráváte na internet a zda tím neporušujete zákony**.
- **Rozmyslete, co chcete publikovat na internetu** (články, diskuze) a zda to nemůže ovlivnit vaši kariéru nebo bezpečnost (a to i v budoucnosti). Na internetu existují archivační služby, které uchovávají obrovské množství dat a jsou zde dohledatelné články i z hluboké internetové historie[23].
- **Na internetu nikdy nedůvěřujte nikomu, koho osobně neznáte!**

23 Viz například http://archive.org/web/web.php.

ZÁVĚR

V této kapitole jsme se snažili popsat a vysvětlit problematiku počítačové bezpečnosti, ukládání a zálohování dat včetně základních otázek bezpečnosti ve virtuálním světě. Možná by bylo vhodné napsat „vybrané otázky", protože nebylo možné zpracovat všechny „základní" otázky či problémy. Není to nedbalostí autora, ale je to zapříčiněno obrovskou šíří dané problematiky, která se navíc velmi rychle proměňuje a vyvíjí. Je tedy docela dobře možné, že někteří čtenáři si postesknou, že zde některé věcí chybí nebo jsou pouze naznačeny. Lze si také představit, že v blízké budoucnosti budou mnohá témata zde zmíněná již zastaralá. Nicméně se domníváme, že principy zůstanou. Pokud se budou čtenáři (uživatelé, studenti) držet našich doporučení a rad, přinejmenším výrazně sníží riziko velkých problémů, nehod či katastrof. Záleží především na uživateli (studentovi), jak s danými informacemi naloží a jak je aplikuje do svého studia nebo práce. A jak se říká, aktivitě se meze nekladou. Je možné jít daleko nad výše uvedené rady a svoji studentskou digitální dílnu si zabezpečit mnoha dalšími i jinými způsoby.

LITERATURA

Doseděl, T. (2005). *21 základních pravidel počítačové bezpečnosti.* Brno: CP Books.

Král, M. (2006). *Bezpečnost domácího počítače: prakticky a názorně.* Praha: Grada.

Lichter, L. (2012). *Internet ve vzdělávání a otázky bezpečnosti.* Brno: Masarykova univerzita. Seminární práce.