Miniminimum bezpečnosti práce v Internetu

Tento text vznikl jako reakce na poměrně živou diskusi po jedné poradě věnované tomuto tématu. Rozhodl jsem se ho rozdělit do tří úrovní (**co dělat**, **jak to dělat lépe**, **proč to dělat**) podle míry obsáhlosti a důležitosti.

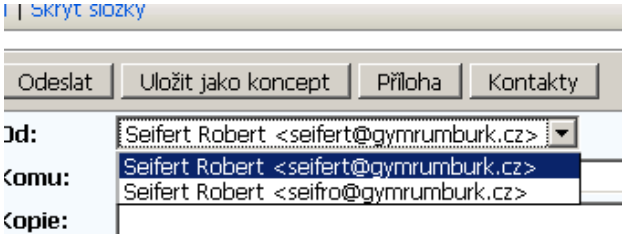
1 Co je potřeba dělat

1. Používejte svou „kryptickou“ e-mailovu adresu (přístupové jméno – například seifro@gymrumburk.cz) **pouze pro přihlašování** k poště. **Neuvádějte ji jako kontakt ani z ní nikomu nepište!**
2. Svůj veřejný e-mail zveřejňujte s rozvahou, uvádějte ho ve formě srozumitelné pouze lidem
3. Vytvořte si **silné heslo**, používejte různá hesla pro různé příležitosti. Hesla nikam nepište! Odhlašujte se!
4. **Používejte** při práci s internetem **zdravý rozum**, **chraňte své soukromí**, dvakrát zvažte zda je vše v pořádku, jedná-li se o zadávání citlivých údajů. Nerozumíte-li něčemu, neklikejte na to.

2 Jak to dělat (lépe)

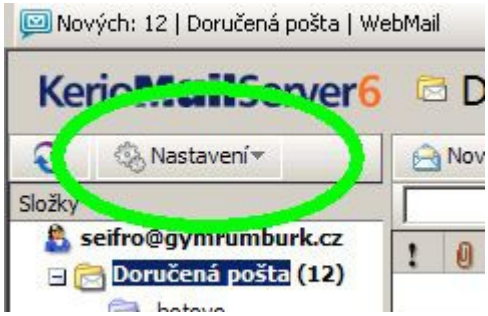
2.1 Ochrana přístupového jména do e-mailových schránek:

- „Kryptickou e-mailovou adresu“ (např. seifro@gymrumburk.cz) nikde nezveřejňujte! (ani na papírové prezenční listině)
- Pro odesílání používejte „veřejnou“ e-mailovou adresu (seifert@gymrumburk.cz). Je na to rozbalovátko – viz obr. vpravo.

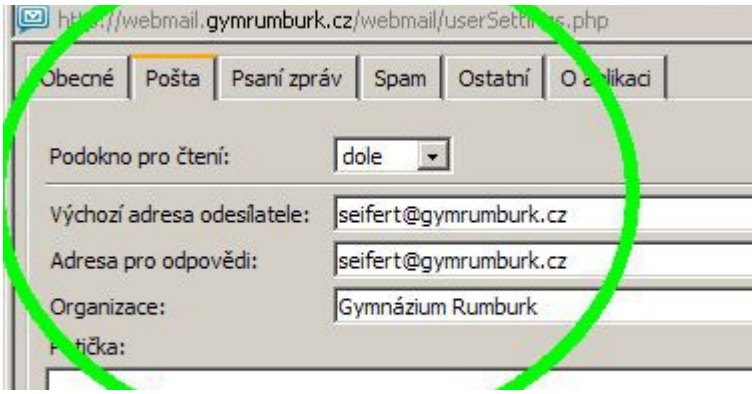


Druhý bod lze snadno zautomatizovat:

2.1.1 Nastavení výchozí e-mailové adresy:



- Přihlaste se ke školnímu e-mailu
- V menu klikněte na „Nastavení“, zvolte položku „Nastavení“. Objeví se dialogové okno
- V dialogovém okně na kartě „Pošta“ vyplňte e-mail, který adresáti uvidí a na který mohou odpovídat. Hledejte položky „Výchozí adresa odesílatele, Adresa pro odpovědi, Organizace



2.2 Ochrana e-mailové adresy

Pro komunikaci by měla být používána výhradně vaše druhá – veřejná – poštovní adresa (obvykle prijmeni@gymrumburk.cz). Tuto adresu je možno sdělit rodičům, uvádět do prezenčních listin atp. Je ale **vhodné**:

- **Uvádět svůj e-mail** (při registracích na konference atp.) pouze tam, kde vám sdělí podmínky, za jakých s ním budou nakládat (například kde se zaručí, že vaše e-mailové adresy nebudou veřejně „viset“ na Internetu. (Prohlášení o zásadách zpracování osobních údajů – e-mail je považován za jeden z osobních údajů podobně, jako telefonní číslo, rodné číslo...)
- **Zveřejňovat svůj e-mail** (zapsat ho na své www stránky, na www stránky školy, facebook, diskusní fórum, ...) pouze ve formě, která znemožní nebo znesnadní strojové čtení. Kupříkladu e-mailovou adresu *seifert@gymrumburk.cz* je vhodné na stránky uvést buď ve formě obrázku, nahradit znak „ampersand“ („zavináč“) slovem – např. *seifert<zavináč>gymrumburk.cz*, nebo *seifert<at>gymrumburk.cz*, nebo jinak „poškodit“ - např. *seifert@gymrumburk-tohle-vymaz-.cz*. Další možnost je e-mail „zašifrovat“ a uvést např. *e-mail je mé příjmení bez háčků a čárek zavináč gymrumburk.cz*.
- Pro skupinovou komunikaci se studenty je dle mého názoru vhodnější použít systém Bakaláři (po předchozí dohodě), protože:
  - systém doručuje automaticky celé třídě, studijní skupině nebo jednotlivcům
  - Systém obsahuje potvrzení o přečtení, které není možno zablokovat. Máte tak kontrolu, že si student přečetl váš vzkaz
  - Systém chrání vaši e-mailovou adresu i adresu druhých.

2.3 Silné heslo

Přístupové heslo je považováno za silné, jestliže:

1. Má minimální délku sedm znaků
2. Obsahuje jak číslice, tak velká i malá písmena
3. Nejedná se o slovníkový termín
4. Nejedná se o žádné „obecně známé heslo“
5. Nemá žádnou zjevnou spojitost s uživatelem
6. Není uloženo jinde než v paměti uživatele.

Uvedené požadavky tedy splňují například sekvence lsko158jha, zatímco sekvence „petr1976“ nebo „asdfghj“ už nikoliv[1]. Pro vygenerování silného a znovu použitelného hesla se doporučuje několik technik:

2.3.1 Mnemotechnické pomůcky

Heslo „*NapeAzma4no*“ splňuje výše uvedené požadavky na silné heslo, přičemž uživatel jej snadno vygeneruje pomocí věty „*Náš pes Azor má 4 nohy*“. Obdobné mnemotechnické pomůcky lze využít i jinde.

2.3.2 Záměna znaků

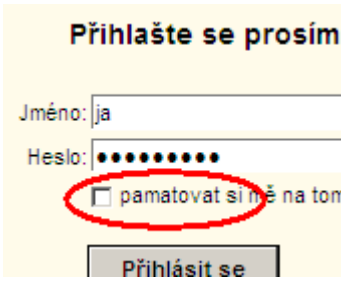
Heslo *„Eznvzej“* sice nesplňuje všechny požadavky na silné heslo, přeci jen je však bezpečnější než heslo *„Rumburk“*, ze kterého vzniklo nahrazením všech znaků písmeny, které jsou na klávesnici o jedno místo vlevo.

2.3.3 Náhrada znaků

Ze slova „Toníček“ získáme silné heslo „T0n!$ek“ díky vizuální podobnosti znaku O/0 a i/!/i a náhrady znaku č ekvivalentem na anglické klávesnici ($),

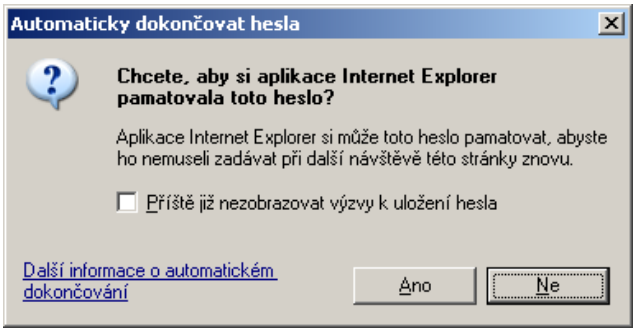
1 Proč?

2.3.4 Pár slov k ukládání hesel



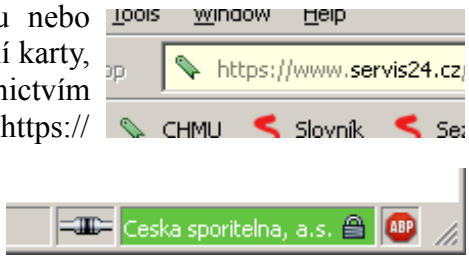
To, že by heslo nemělo být nikde zapsáno, je samozřejmé. Stejé pravidlo by mělo platit i pro funkci „automatické přihlašování“ a různé „zapamatovávače hesel“.

Představte si, že vám ukradnou notebook nebo stolní počítač, ztratíte atp. Jak vaše údaje ochrání super-složité heslo k poštovnímu účtu, je-li aktivováno automatické přihlašování? Jak víte, že hesla uložená „kdybych zapomněl“ na ztracené flashce nebudou použita?



2.4 Ochrana důležitých dat před neoprávněným použitím

Sebesložitější heslo je k ničemu, jestliže ho máte napsané nad psacím stolem. Sebelépe chráněný účet internetového bankovnictví bude bez náhrady vybrakován, dáte-li e-mailem k dispozici přístupové údaje.



Nikdo po vás nemá právo žádat citlivé údaje prostřednictvím e-mailu nebo telefonu. Nikde nesdělujte údaje, které by mohly být zneužity (číslo kreditní karty, číslo účtu, heslo k účtu, číslo mobilního telefonu.) Platíte-li online prostřednictvím kreditní karty, ujistěte se že je platba vedena zabezpečeným připojením (https:// v adresním řádku) a že jste skutečně na stránce organizace, kde se platí. (indikace zabezpečeného připojení je spolu s ověřením organizace součástí okna prohlížeče.

Dvakrát se rozmyslete než na Internet (například na sociální sítě) vypustíte jakoukoliv informaci. I zdánlivě nevinná informace může vést k vašemu poškození (více např. v tomto článku).

3 Proč to dělat

Splnění požadavků nastíněných v tomto textu by mělo snížit tato nejpalčivější rizika, se kterými se naše školní síť potýká[2]:

- Ukradení identity (zcizení přístupového jména, hesla, vydávání se za jinou osobu (rozesílání mailů pod vaším jménem a e-mailem, zápisu známek do Bakalářů pod vaším uživ. jménem atp.
- Napadení školní počítačové sítě/školního poštovního serveru prostřednictvím zcizeného/odhaleného přístupového jména a hesla
- příjmu spamů (nevyžádané pošty) do schránek uživatelů

3.1 Ochrana přístupového jména

Pro přihlášení do systému (školní počítačová síť, školní e-mail, soukromý e-mail) je zapotřebí znalost správné kombinace přihlašovacího jména a přístupového hesla. Při pokusu o napadení útočníci zkouší jednak obvyklá uživatelská jména, která v systému existují z nutnosti (administrator, root, host, guest, user, default atp.), a potom uživatelská jména, která se jim podaří někde najít (e-mailové kontakty na stránkách organizace, v adresářích...). Snadnost takového postupu (i když pro jiný účel) ilustruje např. následující dvouminutové video: http://www.youtube.com/watch?v=P0tXA24d-OY.

Jestliže útočník někde zjistí správné uživatelské jméno, stačí mu už jen rozlomit heslo. Z toho důvodu je nutno přístupová jména chránit a udržovat v tajnosti.

2 Obdobná pravidla platí samozřejmě i pro využívání soukromých e-mailových účtů.

3.2 Ochrana e-mailové adresy

Za většinu spamů můžou tzv. spamové roboty. Ty pro svou práci získávají e-mailové adresy z několika zdrojů:

- Využívají slabé ochrany dat v sociálních sítích a „dolují“ e-mailové adresy odtamtud. (proslulý je tím např. Facebook – vizte např. toto tříminutové video: http://www.youtube.com/watch?v=eqTFHjfOUlo.
- Využívají databáze e-mailových adres, které už na internetu visí (seznamy účastníků konferencí, seznamy spoužáků, seznamy pracovníků atp.
- Procházejí web a hledají e-mailové adresy náhodně roztroušené po internetových stránkách. Spolehlivým způsobem, jak nalézt e-mailovou adresu, je vyhledávat znak „@“ (Schválně – zkuste si to: zadejte do Google vyhledávače řetězec „*@gymrumburk.cz“)
- využívají virů, které se nabourávají do poštovních programů v napadených počítačích a získané e-mailové adresy pak odesílají svému pánu.

Z výše uvedeného plyne, že jakmile se někde na internetu uvede e-mailová adresa, bude použita. Pokud je nutno e-mail uvádět, je vhodné ho uvádět tak, aby nešel nějakým jednoduchým postupem získat.

3.3 Používání silného hesla

Podaří-li se útočníkovi získat správné přístupové jméno (viz odstavec 3.1), zbývá nalézt heslo. Používaných metod je několik:

- odhadnutí hesla na základě znalosti osoby, jejíž heslo chceme získat
- test na obecně známá hesla (existují seznamy nejčastěji používaných hesel – v anglicky mluvících zemích např „god“, „password“, „letmein“, „iamthegod“, „qwert“ a další (více viz např. zde).
- slovníkový útok – útočník postupně zkouší slova, která jsou v dispozici v existujících databázích slov (slovník pro kontrolu pravopisu, slovník cizích slov, slovník spisovné češtiny, překladový slovník atp.)
- útok hrubou silou – útočník postupně zkouší kombinace znaků – v případě třípísmenkového hesla by např postupně zkoušel kombinace aaa, aab, aac, aad, aae, ..., aaz, aba, abb, ..., zzx, zzy, zzz.

Až na první metodu je to opět práce pro stroj (password cracker). Pomineme-li test na známá hesla a slovníkový útok, je záležitost nalezení hesla soubojem mezi délkou hesla (počtem různých kombinací) a rychlostí počítače, který se snaží heslo rozlomit. Zatímco před deseti lety byla k nalezení pětiznakového hesla (celkem 26^5 – zhruba 12 000 000 – možností) na běžném stolním počítači potřeba doba v řádech desítek minut, dnes je to díky nárustu výpočetního výkonu otázka nejvýše několika sekund. (Tento vývoj ilustruje např. příběh počítače nazvaného DES cracker[3]).

Orientační dobu k rozluštění vámi zvoleného hesla hrubou silou pomocí moderních počítačů lze zjistit pomocí několika online nástrojů – např. zde: https://www.grc.com/haystack.htm nebo zde: http://www.howsecureismypassword.net/.[4]

Pravidla pro vytvoření silného hesla reflektují tyto skutečnosti. Body 1 – 4 zamezují slovníkovému útoku a znesnadňují útok hrubou silou, bod 5 je vytvořen k tomu aby snížil riziko odhadnutí hesla. Důvody existence bodu 6 již byly popsány v odstavci 2.3.4.

3 více viz tento článek na Wikipedii: http://en.wikipedia.org/wiki/EFF_DES_cracker

4 Pomiňme na chvíli skutečnost, že samo zadávání hesla jinam než tam, kde má být, je bezpečnostní riziko.

Dodatek: Používání zdravého rozumu

Pomineme-li sofistikované viry, jsou z hlediska vylákání podvodných údajů nejúčinnější techniky tzv. sociálního inženýrství. Pomocí klamů, přetvářky a sebejistého vystupování s využitím několika pravdivých údajů je oběť přesvědčena, že jedná s autorizovanou osobou a dobrovolně jí svěří citlivé údaje. Krásnou ilustrací těchto technik je např. film Policajt v Beverly Hills, známý (usvědčený) hacker Kevin Mittnick je popisuje ve své knize Umění klamu (ISBN 83-7361-210-6).

Nejběžněji se s takovým typem dá setkat v tzv. phishingových zprávách. Ty mohou vypadat třeba takto:

Vážený kliente, obrací se na Vás služba zpracování plateb ČSOB.

Vaše žádost o provedení platby byla přijata, ale bohužel nemá ČSOB v současné době možnost ji zpracovat. Důvod: nesprávné údaje v platebním příkazu. Prosím, zkontrolujte údaje v podané žádosti. (odkaz na žádost)

Do té doby, než budou údaje opraveny, se budou finanční prostředky nacházet ve „zmrazeném“ stavu. Po opravení údajů v platebním příkazu budou finanční prostředky odeslány do 10 minut.

S úctou Služba zpracování plateb ČSOB

Odkaz vede na stránku, kam uživatel dobrovolně zadá číslo účtu, heslo k účtu....

Žádná seriózní organizace po vás nikdy nebude tímto způsobem chtít heslo. Heslo je vaše věc a kdyby došlo k havárii (druhý oblíbený scénář – došlo k havárii poštovního serveru, na této stránce (odkaz) znovu zadejte uživatelské jméno a heslo aby byla vaše data obnovena), k obnově dat není potřeba.

Bankám je jedno, jestli je váš platební příkaz v pořádku.

Microsoft nikdy nedá peníze sirotkům, když kliknete na nějaký odkaz v e-mailu.

Před hloupostí software neochrání.