ZÁKLADNÍ ŠKOLA ÚSTÍ NAD LABEM, HLAVNÍ 193, 403 31
Tel.:472731819, 472731253 Tel.řed./fax:472731480, e-mail:skola@zsmojzir.cz

6.A, 6.B
1. 2. 2021 + 15. 2. 2021

(8. 2. jarní prázdniny)

Z následujícího textu si udělejte výpisky. Sešit s výpiskami doneste do školy ke kontrole nebo je můžete vyfotit a poslat nám je na email:

a.hola@zsmojzir.cz, e.sibalova@zsmojzir.cz.

Desatero internetové a počítačové bezpečnosti

www – prohlížení internetových stránek

1. **Prohlížejte pouze důvěryhodné stránky s bezpečným obsahem**.
   Nedůvěryhodné stránky, stránky s podezřelým, závadným či nebezpečným obsahem okamžitě opusťte.

2. **Používejte bezpečné internetové prohlížeče** (např. Firefox, Opera atd.).
   Internetové prohlížeče musí být pravidelně aktualizovány, zejména jedná-li se o méně bezpečné programy (např. Internet Explorer).

3. **Věnujte pozornost hlášením, výzvám a dotazům jednotlivých počítačových programů a odkazům na internetových stránkách – vždy pečlivě zvažte, na co klinout, a zda na to vůbec kliknout.**
   Vyvarujte se bezhlavému potvrzování hlášení, která si nepřečtete, neklikejte na odkazy, které vedou neznámo kam či působí nedůvěryhodně.

4. **Nestahujte z internetu podezřelé a nedůvěryhodné programy. Neinstalujte tyto programy, nevíte-li o nich nic bližšího.**
   Před stažením a instalací programu se vždy pokuste získat si o něm co nejvíce informací a referencí. Řada volně stáhnutelných programů obsahuje viry, trójany a další škodlivé kódy. Každý program (formáty souborů exe, com a bat) bezprostředně po stažení proscanujte antivirovým softwarem.

e-mail a další formy elektronické komunikace

5. **Využívejte poštovních kont na důvěryhodných webserverech s kvalitním zabezpečením**.
   (např. Centrum, Seznam, Volný, Atlas, Gmail atd.)

6. **Věnujte pozornost svému přihlášení a odhlášení. Chraňte své heslo před ostatními uživateli.**
   Při používání e-mailu, instant messengeru (např. ICQ), IP telefonního programu (např. Skype) atd. dodržujte základní zásady bezpečného přihlášení – přihlašujte se sami, tak aby nikdo neviděl vaše heslo; heslo si nepište vedle počítače a neukládejte jej do počítače nastálo; volte těžko odhadnutelné heslo a průběžně jej měňte. Při odchodu od počítače se vždy odhlašte. Tam kde to jde, smažte historii práce v prohlížeči (Firefox). Všude v internetu chraňte svoji identitu – vždy pečlivě zvažte co a kam píšete a kdo a jak se zadanými údaji bude či může dále manipulovat. Ověřujte pravost stránek.

7. **Používáte-li poštovního klienta nebo speciální program pro on-line komunikaci, vždy pracujte jen s bezpečnými a důvěryhodnými nástroji v aktualizované verzi.**
   Vyvarujte se používání nebezpečných a zastaralých produktů (např. Pegasus Mail, MS Outlook Express atd.). Jestliže se bez nich neobejdete, alespoň je aktualizujte a upravte jejich nastavení tak, aby poštu neotevíraly automaticky, ale jen s Vaším svolením. Používejte raději pouze osvědčené bezpečné e-mailové klienty (např. Thunderbird atd.) a komunikátory.

8. **Filtrujte ve své poště SPAM a HOAX, neotevírejte nevyžádanou poštu, nestahujte podezřelé přílohy e-mailů, neklikejte na neznámé odkazy v poště.**
   Součástí nevyžádané pošty (SPAM) a pošty obsahující dezinformace a fámy (HOAX), jakož i všech připojených příloh, může být virus či jiný škodlivý kód. Tuto poštu a její přílohy, jde-li to, vůbec neotevírejte a na nic (na žádné odkazy v ní) neklikejte. Velmi nebezpečné jsou přílohy s příponami exe, com a bat – tyto soubory, pokud možno, neotevírejte. Jisté riziko mohou představovat také soubory pro programy Word, Excel a Powerpoint doc, xls a ppt. Musíte-li tyto soubory otevřít, prověřte je antivirem

obecné zásady bezpečnosti

9. **Mějte v počítači nainstalovaný kvalitní antivirový program s automatickou rezidentní ochranou. Udržujte jej stále aktualizovaný. Mějte zapnutý firewall.**

10. **Průběžně aktualizujte operační systém a všechny nainstalované programy, které aktualizaci umožňují. Pravidelně stahujte bezpečnostní záplaty.**