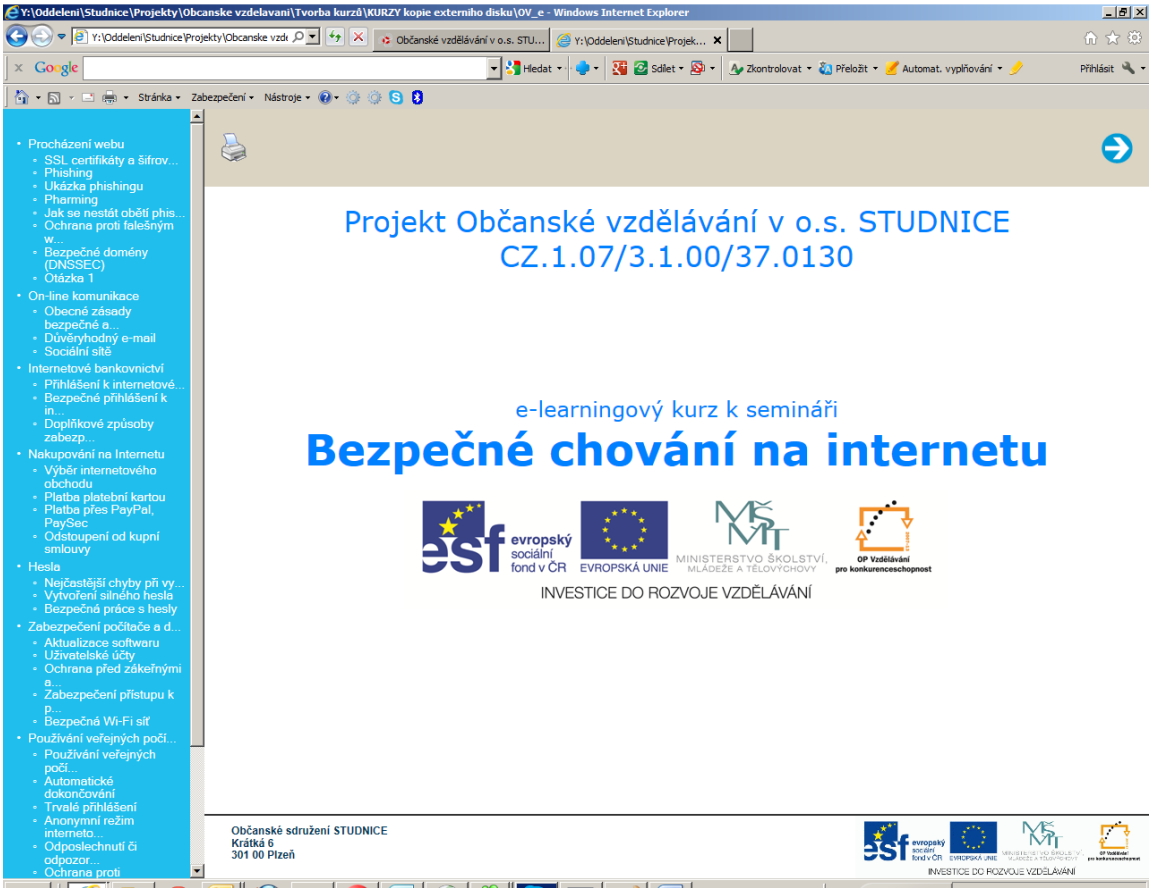
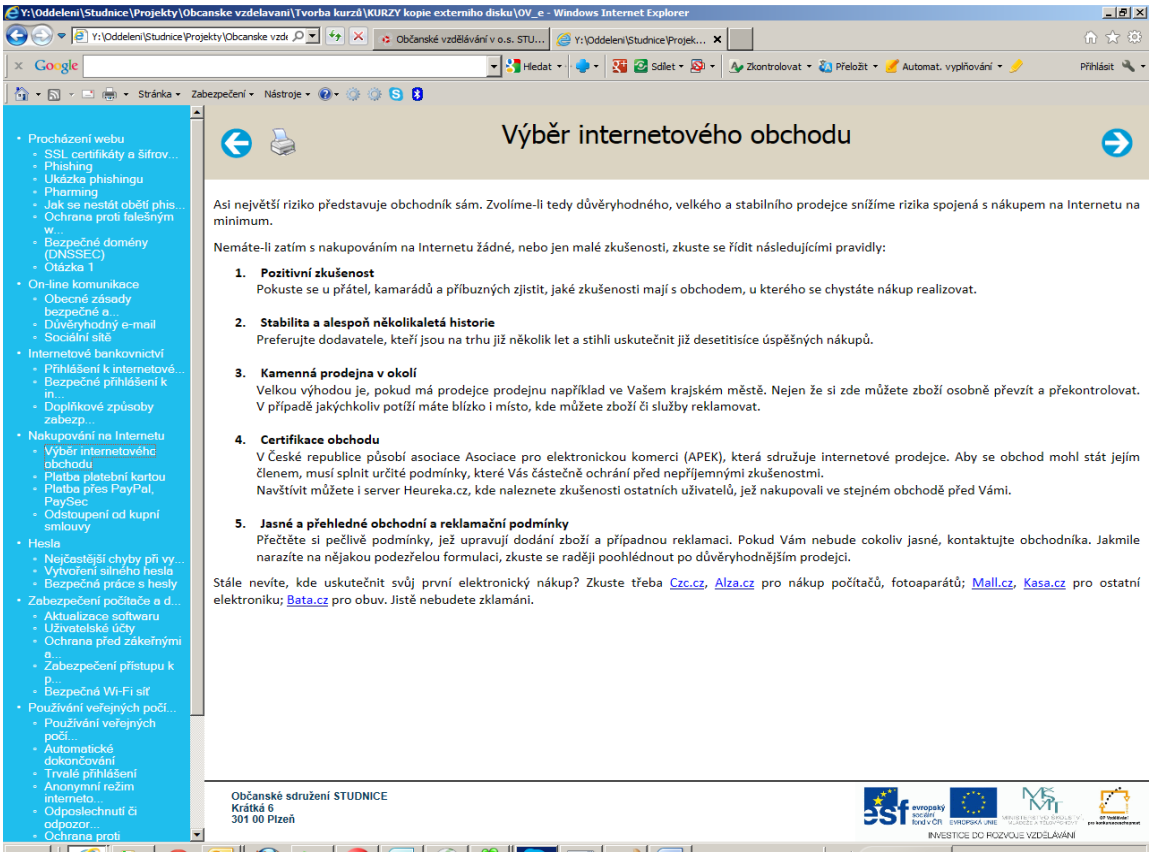
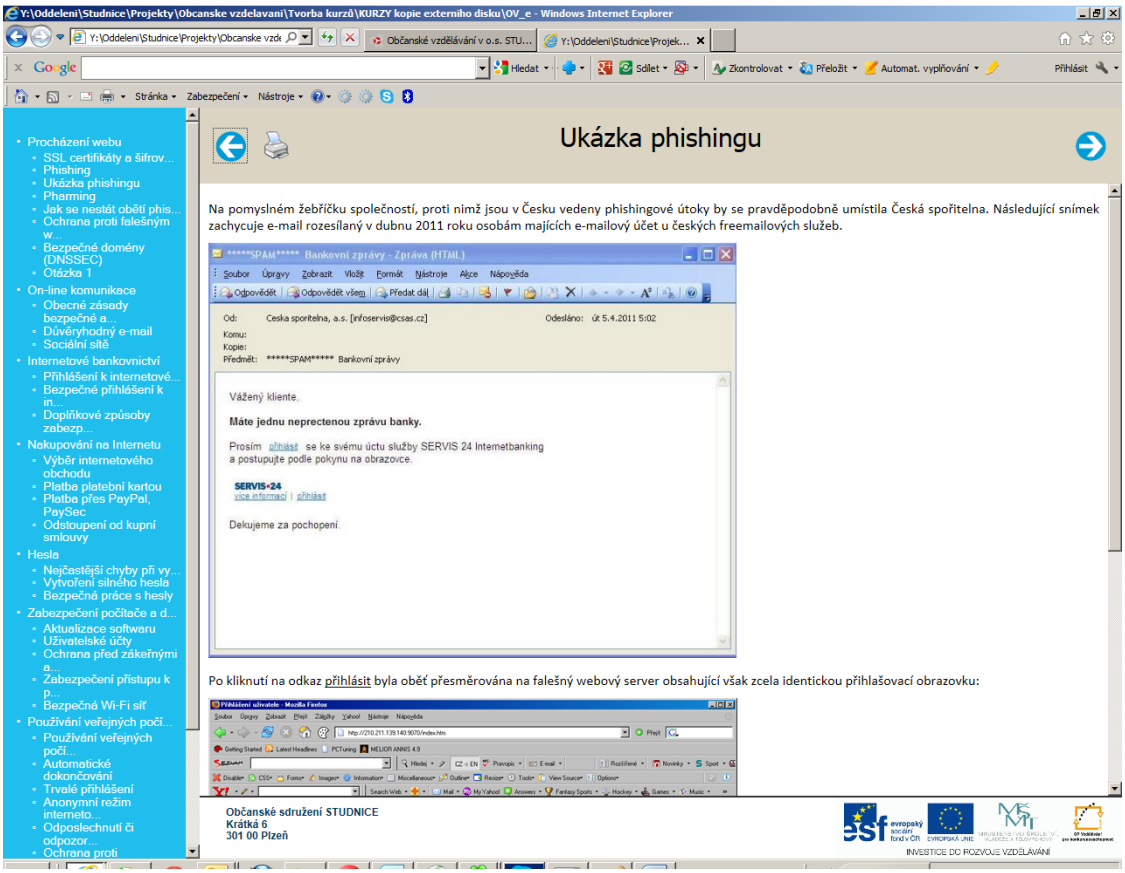
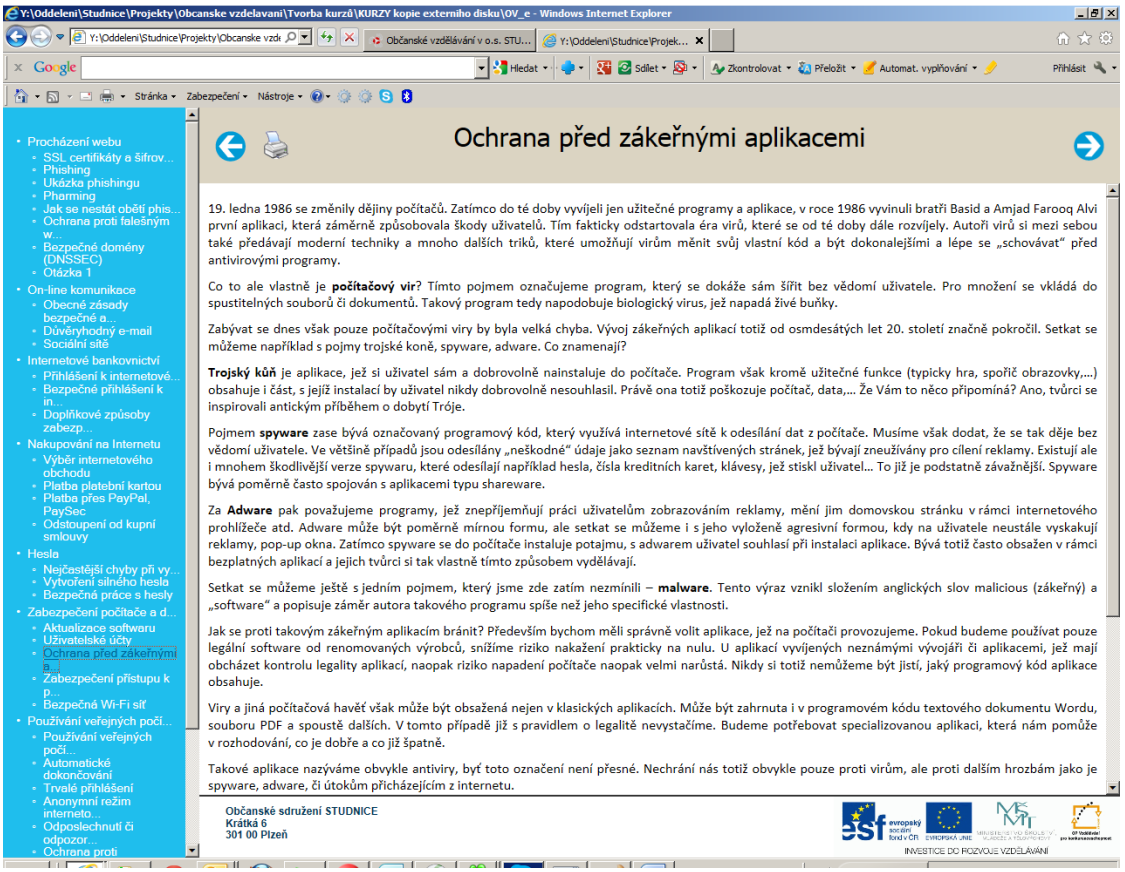

Y:\Oddeleni\Studnice\Projekty\Obcanske vzdelavani\Tvorba kurzů\KURZY kopie externiho disku\OV_e - Windows Internet Explorer
Občanské vzdělávání v o.s. STU...
Y:\Oddeleni\Studnice\Projek...
Google
Hledat
Sdílet
Zkontrolovat
Přeložit
Automat. vyplňování
Přihlásit
Stránka
Zabezpečení
Nástroje
Procházení webu
SSL certifikáty a šifrov...
Phishing
Ukázka phishingu
Pharming
Jak se nestát obětí phis...
Ochrana proti falešným w...
Bezpečné domény (DNSSEC)
Otázka 1
On-line komunikace
Obecné zásady bezpečné a...
Důvěryhodný e-mail
Sociální sítě
Internetové bankovnictví
Přihlášení k internetové...
Bezpečné přihlášení k in...
Doplňkové způsoby zabezp...
Nakupování na Internetu
Výběr internetového obchodu
Platba platební kartou
Platba přes PayPal, PaySec
Odstoupení od kupní smlouvy
Hesla
Nejčastější chyby při vy...
Vytvoření silného hesla
Bezpečná práce s hesly
Zabezpečení počítače a d...
Aktualizace softwaru
Uživatelské účty
Ochrana před zákeřnými a...
Zabezpečení přístupu k p...
Bezpečná Wi-Fi síť
Používání veřejných počí...
Používání veřejných počí...
Automatické dokončování
Trvalé přihlášení
Anonymní režim interneto...
Odposlechnutí či odpozor...
Ochrana proti
Projekt Občanské vzdělávání v o.s. STUDNICE
CZ.1.07/3.1.00/37.0130
e-learningový kurz k semináři
Bezpečné chování na internetu
evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ
Občanské sdružení STUDNICE
Krátká 6
301 00 Plzeň


Y:\Oddeleni\Studnice\Projekty\Obcanske vzdelavani\Tvorba kurzů\KURZY kopie externiho disku\OV_e - Windows Internet Explorer
Výběr internetového obchodu
Asi největší riziko představuje obchodník sám. Zvolíme-li tedy důvěryhodného, velkého a stabilního prodejce snížíme rizika spojená s nákupem na Internetu na minimum.
Nemáte-li zatím s nakupováním na Internetu žádné, nebo jen malé zkušenosti, zkuste se řídit následujícími pravidly:
1. Pozitivní zkušenost
Pokuste se u přátel, kamarádů a příbuzných zjistit, jaké zkušenosti mají s obchodem, u kterého se chystáte nákup realizovat.
2. Stabilita a alespoň několikaletá historie
Preferujte dodavatele, kteří jsou na trhu již několik let a stihli uskutečnit již desetitisíce úspěšných nákupů.
3. Kamenná prodejna v okolí
Velkou výhodou je, pokud má prodejce prodejnu například ve Vašem krajském městě. Nejen že si zde můžete zboží osobně převzít a překontrolovat. V případě jakýchkoliv potíží máte blízko i místo, kde můžete zboží či služby reklamovat.
4. Certifikace obchodu
V České republice působí asociace Asociace pro elektronickou komerci (APEK), která sdružuje internetové prodejce. Aby se obchod mohl stát jejím členem, musí splnit určité podmínky, které Vás částečně ochrání před nepříjemnými zkušenostmi. Navštivit můžete i server Heureka.cz, kde naleznete zkušenosti ostatních uživatelů, jež nakupovali ve stejném obchodě před Vámi.
5. Jasné a přehledné obchodní a reklamační podmínky
Přečtěte si pečlivě podmínky, jež upravují dodání zboží a případnou reklamaci. Pokud Vám nebude cokoliv jasné, kontaktujte obchodníka. Jakmile narazíte na nějakou podezřelou formulaci, zkuste se raději poohlédnout po důvěryhodnějším prodejci.
Stále nevíte, kde uskutečnit svůj první elektronický nákup? Zkuste třeba Czc.cz, Alza.cz pro nákup počítačů, fotoaparátů; Mall.cz, Kasa.cz pro ostatní elektroniku; Bata.cz pro obuv. Jistě nebudete zklamáni.
Občanské sdružení STUDNICE
Krátká 6
301 00 Plzeň


Y:\Oddeleni\Studnice\Projekty\Obcanske vzdelavani\Tvorba kurzů\KURZY kopie externiho disku\OV_e - Windows Internet Explorer
Ukázka phishingu
Na pomyslném žebříčku společností, proti nimž jsou v Česku vedeny phishingové útoky by se pravděpodobně umístila Česká spořitelna. Následující snímek zachycuje e-mail rozesílaný v dubnu 2011 roku osobám majících e-mailový účet u českých freemailových služeb.
Po kliknutí na odkaz přihlásit byla oběť přesměrována na falešný webový server obsahující však zcela identickou přihlašovací obrazovku:
Občanské sdružení STUDNICE
Krátká 6
301 00 Plzeň
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ


Y:\Oddeleni\Studnice\Projekty\Obcanske vzdelavani\Tvorba kurzů\KURZY kopie externiho disku\OV_e - Windows Internet Explorer
Ochrana před zákeřnými aplikacemi
19. ledna 1986 se změnily dějiny počítačů. Zatímco do té doby vyvíjeli jen užitečné programy a aplikace, v roce 1986 vyvinuli bratři Basid a Amjad Farooq Alvi první aplikaci, která záměrně způsobovala škody uživatelů. Tím fakticky odstartovala éra virů, které se od té doby dále rozvíjely. Autoři virů si mezi sebou také předávají moderní techniky a mnoho dalších triků, které umožňují virům měnit svůj vlastní kód a být dokonalejšími a lépe se „schovávat" před antivirovými programy.
Co to ale vlastně je **počítačový vir**? Tímto pojmem označujeme program, který se dokáže sám šířit bez vědomí uživatele. Pro množení se vkládá do spustitelných souborů či dokumentů. Takový program tedy napodobuje biologický virus, jež napadá živé buňky.
Zabývat se dnes však pouze počítačovými viry by byla velká chyba. Vývoj zákeřných aplikací totiž od osmdesátých let 20. století značně pokročil. Setkat se můžeme například s pojmy trojské koně, spyware, adware. Co znamenají?
Trojský kůň je aplikace, jež si uživatel sám a dobrovolně nainstaluje do počítače. Program však kromě užitečné funkce (typicky hra, spořič obrazovky,...) obsahuje i část, s jejíž instalací by uživatel nikdy dobrovolně nesouhlasil. Právě ona totiž poškozuje počítač, data,... Že Vám to něco připomíná? Ano, tvůrci se inspirovali antickým příběhem o dobytí Tróje.
Pojmem **spyware** zase bývá označovaný programový kód, který využívá internetové sítě k odesílání dat z počítače. Musíme však dodat, že se tak děje bez vědomí uživatele. Ve většině případů jsou odesílány „neškodné" údaje jako seznam navštívených stránek, jež bývají zneužívány pro cílení reklamy. Existují ale i mnohem škodlivější verze spywaru, které odesílají například hesla, čísla kreditních karet, klávesy, jež stiskl uživatel... To již je podstatně závažnější. Spyware bývá poměrně často spojován s aplikacemi typu shareware.
Za **Adware** pak považujeme programy, jež znepříjemňují práci uživatelům zobrazováním reklamy, mění jim domovskou stránku v rámci internetového prohlížeče atd. Adware může být poměrně mírnou formu, ale setkat se můžeme i s jeho vyloženě agresivní formou, kdy na uživatele neustále vyskakují reklamy, pop-up okna. Zatímco spyware se do počítače instaluje potajmu, s adwarem uživatel souhlasí při instalaci aplikace. Bývá totiž často obsažen v rámci bezplatných aplikací a jejich tvůrci si tak vlastně tímto způsobem vydělávají.
Setkat se můžeme ještě s jedním pojmem, který jsme zde zatím nezmínili – **malware**. Tento výraz vznikl složením anglických slov malicious (zákeřný) a „software" a popisuje záměr autora takového programu spíše než jeho specifické vlastnosti.
Jak se proti takovým zákeřným aplikacím bránit? Především bychom měli správně volit aplikace, jež na počítači provozujeme. Pokud budeme používat pouze legální software od renomovaných výrobců, snížíme riziko nakažení prakticky na nulu. U aplikací vyvíjených neznámými vývojáři či aplikacemi, jež mají obcházet kontrolu legality aplikací, naopak riziko napadení počítače naopak velmi narůstá. Nikdy si totiž nemůžeme být jistí, jaký programový kód aplikace obsahuje.
Viry a jiná počítačová havěť však může být obsažená nejen v klasických aplikacích. Může být zahrnuta i v programovém kódu textového dokumentu Wordu, souboru PDF a spoustě dalších. V tomto případě již s pravidlem o legalitě nevystačíme. Budeme potřebovat specializovanou aplikaci, která nám pomůže v rozhodování, co je dobře a co již špatně.
Takové aplikace nazýváme obvykle antiviry, byť toto označení není přesné. Nechrání nás totiž obvykle pouze proti virům, ale proti dalším hrozbám jako je spyware, adware, či útokům přicházejícím z internetu.
Občanské sdružení STUDNICE
Krátká 6
301 00 Plzeň
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ