Dobré rady pro Vaši bezpečnost na internetu.

Internet nabízí spoustu zábavy a poučení, ale i nebezpečí. Chraňte sebe i své blízké!

Projekt "Bezpečný internet.cz" vznikl s cílem **poukázat na mnohá rizika spojená s používáním internetu a na způsoby jak se jim bránit.**

V současné době lze na internetu najít mnoho informací, které se internetové bezpečnosti věnují. Ve většině případů se však jedná pouze o popis konkrétních rizik bez celkového rámce, jsou zaměřeny pouze na určitou skupinu uživatelů nebo jsou vázány na produkty konkrétní společnosti.

Snahou projektu "Bezpečný internet.cz" je oslovit co nejširší okruh uživatelů internetu a na názorných příkladech pomáhat **vytvářet správné návyky internetové bezpečnosti a vzdělávat české uživatele internetu**.

Projekt "Bezpečný internet.cz" není vázán na produkty žádných společností a zcela zdarma poskytuje rady, návody i zkušenosti provozovatelů nejnavštěvovanějších internetových služeb. Jde o nekomerční službu, která je otevřena pro další partnery, kteří chtějí vzdělávat uživatele v oblasti bezpečného internetu.

Zakládajícími partnery projektu "Bezpečný internet.cz" jsou společnosti Česká spořitelna, a.s., Microsoft, s.r.o. a Seznam.cz, a.s.; dalšími spolupracujícími partnery jsou vedle Policie České republiky společnosti Pierstone, s.r.o. a Quantasoft, s.r.o.

Desatero bezpečného internetu [1]

Drž se zásad o bezpečnosti na internetu a zbytečně neriskuj.

Pro bezpečí na internetu ti stačí dodržet jen pár důležitých, ale přitom jednoduchých zásad.

- Nedávej nikomu adresu ani telefon. Nevíš, kdo se skrývá za monitorem na druhé straně.
- Neposílej nikomu, koho neznáš, svou fotografii a už vůbec ne intimní. Svou intimní fotku neposílej ani kamarádovi nebo kamarádce - nikdy nevíš, co s ní může někdy udělat.
- Udržuj hesla (k e-mailu i jiné) v tajnosti, nesděluj je ani blízkému kamarádovi.
- Nikdy neodpovídej na neslušné, hrubé nebo vulgární maily a vzkazy. Ignoruj je.
- Nedomlouvej si schůzku přes internet, aniž bys o tom řekl někomu jinému.
- Pokud narazíš na obrázek, video nebo e-mail, který tě šokuje, opusť webovou stránku.
- Svěř se dospělému, pokud tě stránky nebo něčí vzkazy uvedou do rozpaků, nebo tě dokonce vyděsí.
- Nedej šanci virům. Neotevírej přílohu zprávy, která přišla z neznámé adresy.
- Nevěř každé informaci, kterou na internetu získáš.
- Když se s někým nechceš bavit, nebav se.

[1] http://www.bezpecnyinternet.cz/

Informace o mně

Pokud budeš na internetu vystupovat pod přezdívkou, nic se ti nemůže stát. Pokud ale o sobě vyplníš osobní údaje, vystavuješ se riziku. Změnit přezdívku lze jednoduše, telefon a adresu nikoli.

Na internetu můžeš najít mnoho informací. Internet je výborným nástrojem a pomocníkem. Můžeš tu komunikovat, posílat si fotografie nebo se dívat na videa. Ne všemu a všem se dá ale věřit. Je proto dobré být opatrný a na internetu o sobě sdělovat jen základní informace.

- Máš profil na nějaké seznamce? Buď opatrný a nezveřejňuj na něm svoje osobní informace. **Třeba kde bydlíš, své telefonní číslo nebo adresu.**
- Zamysli se, zda opravdu musíš všude **uvádět svoje celé jméno** nebo informace o své rodině a kamarádech.
- Kamarádům veřejně na internetu a už vůbec ne úplně cizím lidem v žádném případě nesděluj informace, kam chodíš do kroužků, do školy nebo za zábavou. Nikdy nikam nepiš, že jedeš na dovolenou. Po návratu domů by na tebe a na tvé rodiče mohlo čekat moc nemilé překvapení v podobě prázdného bytu.
- Když zveřejňuješ na internetu svoji fotografii, uvědom si, že ji může kdokoli použít. Nikdy na internetu **neposílej svoje intimní fotografie, a to ani svým známým.** Pokud se dostanou do nesprávných rukou, může tě někdo vydírat nebo je použít tak, že ti to bude nepříjemné. Pokud se tvé intimní fotografie objeví někde na internetu, jejich dalšímu šíření už nezabráníš a nejde to vzít zpět.
- Chce po tobě nějaká seznamka **citlivé údaje**? Třeba jaké nosíš spodní prádlo? Takové informace nesděluj.
- Znáš ve svém okolí někoho, kdo o sobě na internetu zveřejňuje osobní nebo citlivé údaje? Zkus mu poradit a sdělit, jakému se vystavuje riziku. Ukaž mu třeba film www.seznamsebezpecne.cz.
- Pokud máš webovou kameru, neukazuj víc, než je nezbytně nutné. Zařízení bytu nebo sebe v nějaké citlivé situaci nemusíš nikde ukazovat. Nezapomeň, že si tě může někdo nahrávat.

Rada

Pamatuj: Nedávej nikomu adresu ani telefonní číslo. Nevíš, kdo se skrývá za vzdáleným monitorem. Když nebudeš dávat pozor, hrozí ti opravdu vážné nebezpečí. I když si myslíš, že zrovna tebe to potkat nemůže. Sdílej jen nejnutnější informace o sobě a minimum fotografií. Informace o školácích denně vyhledává několik set slídilů - nenech se chytit do té nesprávné sítě a nedovol nikomu zneužít informace o tobě.

Kde hledat pomoc

Neboj se svěřit. Třeba zrovna v tuto chvíli ten, co ti ublížil, ubližuje někomu jinému a pokračuje v tom, co sis nechal pro sebe.

Nikdy nezapomínej na to, že v tom nejsi sám. Neboj se svěřit kamarádům, rodičům nebo učitelům. Pokud k nim nemáš takovou důvěru nebo bys to raději řešil s někým cizím, obrať se na lidi, kteří se takovou pomocí běžně zabývají. Ti už budou vědět, jak ti pomoci. Budou tě umět vyslechnout. Pokud máš nějaký problém, hlavně nikdy neváhej s jeho řešením.

Nahlásím, ale chci zůstat anonymní

Setkal ses někdy na internetu se závadným obsahem nebo potřebuješ radu odborníka? Hledáš radu, ale chceš přitom zůstat anonymní? Podívej se sem: seznamsebezpecne.cz/nahlaste-zavadny-obsah.

Zavolám a poradí mi - Linka bezpečí

Celostátní linka pro děti a mládež v krizových životních situacích. Linka bezpečí pomáhá řešit problémy dětem na útěku, dětem týraným či zneužívaným, ale i těm, co pociťují znepokojení a ohrožení během prohlížení webových stránek, při chatování a hraní her. Pomáhá i těm, co jsou obtěžováni prostřednictvím mobilu nebo jiných komunikačních médií. Služba funguje zdarma 24 hodin denně, včetně nedělí a svátků, a to z pevného i mobilního telefonu na telefonní lince **116 111**.

Kromě telefonního kontaktu můžeš využít také chatovou službu nebo e-mailovou poradnu: chat.linkabezpeci.cz, pomoc@linkabezpeci.cz.

Závadný obsah na internetu - Internet Hotline

Každý, kdo se při používání internetu setká s nebezpečným či podezřelým obsahem, může prostřednictvím webových stránek www.internethotline.cz nebo e-mailové adresy oznamte@internethotline.cz kontaktovat odborníky Internet Hotline. Vyškolení specialisté tato oznámení vyhodnotí a potenciálně nelegální případy předají Policii ČR. Nevhodný obsah umístěný na serverech v zahraničí postupují i spolupracujícím horkým linkám, které působí po celém světě.

Policie - zavolej 158

Neboj se kontaktovat policii. Čím dříve ohlásíš, že se ti něco děje, tím dříve může být věc řešena a případný pachatel může být dopaden. Takový člověk nemusí obtěžovat jenom tebe. Svou odvahou můžeš pomoci i někomu jinému.

Diskuse Lidé.cz

Zde se můžeš podělit o svůj příběh, problém a mluvit s jinými lidmi. Budeš překvapen, kolik lidí mělo podobnou zkušenost jako ty.

Procházení webu

Hackeři se zlými úmysly a tvůrci virů mohou infikovat počítač využitím nastavené nízké úrovně zabezpečení v e-mailové aplikaci a webovém prohlížeči. Mohou to provést zasláním škodlivého e-mailu nebo zlákáním k návštěvě škodlivého webu.

Phishing

Dávejte si dobrý pozor, jakou přílohu otevíráte a na jaké odkazy klikáte - může se jednat o podvod!

Phishing je podvodné jednání s cílem vylákat vaše osobní data jako např. čísla kreditních karet, hesla a další důležité údaje. Dá se také popsat jako krádež identity nebo jako typ sociálního inženýrství. Někdy se pro něj v češtině razí název „rhybaření".

S podvody tohoto typu se můžete setkat:

- v e-mailech, které se tváří, jako by byly od vašeho kolegy nebo od kohokoli jiného, koho znáte,
- na webových stránkách vaší sociální sítě,
- na různých falešných webových stránkách, které třeba vybírají dary pro charitu,
- na webových stránkách, které vám připadají důvěrně známé, nicméně mají trochu jinou webovou adresu, takže je těžké si toho všimnout,
- při chatování,
- na vašem mobilním zařízení.

Podvodné informace často spoléhají na linky v e-mailech, webových stránkách nebo při chatu, které se zdají přicházet od služby, které důvěřujete, jako je např. vaše banka, poskytovatel platebních karet nebo vaše sociální síť. Cílem sociálního inženýrství je obvykle v tichosti nainstalovat spyware nebo vás zmást, abyste prozradili vaše hesla nebo jiné finanční či osobní informace.

Nikdy neodpovídejte na nevyžádané výzvy k aktualizaci informací o účtu. Takové e-mailové zprávy mohou být pokusy o podvody, jejichž cílem je krádež vaší identity. Většina seriózních společností nikdy nezasílá nevyžádané zprávy se žádostmi o vaše heslo nebo jiné osobní informace. A pamatujte si, že pokud něco zní příliš dobře, než aby to byla pravda, pravděpodobně to pravda není.

Jak se můžete chránit před podvodnými informacemi? Následné tipy mohou pomoci se vyvarovat podvodu na internetu:

- ❖ Mějte zapnutý firewall.
- ❖ Vždy udržujte váš software a operační systém aktuální.
- ❖ Mějte vždy aktuální antivirový program.
- ❖ Mějte vždy aktuální antispywarový program.

Věnujte dostatečnou pozornost odkazům na webu! Protože mnoho podvodů na internetu spoléhá na kliknutí uživatele na link, je velice dobrým způsobem, jak se chránit, prostě dávat pozor, na co klikáte v e-mailech, při chatu nebo na webových stránkách. Pokud dostanete e-mail, který jste neočekávali a obsahuje nějaký odkaz, jenž chcete zkusit, napište odkaz raději přímo do webového prohlížeče. Pokud webový odkaz pochází ze stránky, kterou často navštěvujete, použijte raději vaše internetové záložky pro přístup na tuto stránku.

Mažte nevyžádanou poštu! Neotevírejte ji a neodpovídejte na ni, ani když si přejete být odstraněni z distribučního listu. Když odpovíte, tak potvrdíte odesílateli, že váš účet je aktivní.

Buďte obezřetní při poskytování svých osobních nebo finančních údajů na internetu. Nevyplňujte formuláře v e-mailech, které vás žádají o osobní nebo finanční informace.

Používejte silná hesla a vyvarujte se používání stejných hesel pro různá internetová bankovnictví a další důležité účty.

Kontrolujte si pravidelně bankovní výpisy a okamžitě nahlaste platby, ke kterým jste nedali souhlas.

Za žádných okolností neplaťte účty či neprovádějte jiné finanční úkony na veřejném počítači, pokud jste na otevřené veřejné bezdrátové síti. Jestliže se přesto musíte přihlásit k veřejnému počítači, dejte přednost takovému, který požaduje heslo, což zvyšuje bezpečnost.

Co dělat, pokud se stanu obětí phishingu?

K zadávání citlivých údajů používejte pouze oficiální komunikační kanály vaší banky, které jsou vždy jištěny samostatnými hesly.

Obdržel jsem následující e-mail (hlavička i údaje zdánlivě odpovídající bance, kde mám veden účet):

Vážený zákazníku,

dne 13. 4. 2010 v 17:34 CET byla v zahraničí provedena platba z Vaší kreditní karty ve výši 12 452 jenů. Jelikož se jedná o platbu na nestandardním místě a v nestandardní měně, máme důvodné podezření, že jste se stal obětí krádeže. V případě, že je výše uvedená informace pravdivá, neberte prosím na tuto zprávu zřetel.

V opačném případě doporučujeme urychleně provést blokaci Vaší kreditní karty na této adrese: www.banka-blokace.cz/blokace/kartaX584fgH56sddv.php.

S pozdravem, Martin Hořejš, oddělení bezpečnosti transakcí

V domnění, že se jedná o moji banku, jsem vyplnil na zmiňovaném odkazu všechny požadované údaje včetně hesel a nahrál přístupový certifikát. Po několika dnech jsem kontaktoval banku, abych si domluvil vyzvednutí nové kreditní karty, a s hrůzou zjistil, že k žádné blokaci ani korespondenci z jejich strany nedošlo. Z mého účtu bylo navíc odesláno 200 tisíc Kč na jakýsi neznámý účet někam do Latinské Ameriky. Dozvěděl jsem se jedinou užitečnou informaci, a to, že se všechny věci ohledně hesel a citlivých údajů řeší zabezpečeným způsobem přímo přes banku. E-mail slouží pouze k informativním účelům. Co teď?

Rada

Velmi pravděpodobně jste se stali obětí podvodného e-mailu a sdělili jste přístupové údaje třetí osobě.

Pokud si včas uvědomíte, že jste své údaje sdělili nedůvěryhodnému zdroji, pokuste se je ještě co nejrychleji změnit, a to oficiální cestou.

V každém případě kontaktujte svoji banku - opět oficiální cestou (např. hotline).

Většina prohlížečů umožňuje nahlásit phishing, pokud si právě prohlížíte stránku snažící se vylákat citlivé údaje. Využijte tuto možnost.

Ve výše uvedeném případě se jedná o trestný čin, můžete tedy kontaktovat Policii ČR a případně podat trestní oznámení na neznámého pachatele.

Co ale dělat s odeslanými penězi do Latinské Ameriky? Pachatele pravděpodobně nedopadnou. Jedná se o odpovědnost klienta nebo banky? Klient je odpovědný za to, že se údaje jako certifikát, přístupová hesla apod. nedostanou do cizích rukou. Pokud se převod uskuteční na základě zadání platných přihlašovacích údajů, banka není odpovědná za vzniklou škodu. Pro některé případy phishingu existuje také pojištění, zkontrolujte si, zda tomu tak není i u vás. Nejlepší prevencí je nikdy nevyplňovat hesla nebo citlivé údaje na základě pouhého podnětu z e-mailu. Vaše banka by vás o ně nikdy takovýmto způsobem nepožádala! Těžko se na první pohled rozlišuje věrohodný zdroj, stránka, na kterou

podvodný e-mail odkazuje, může vypadat stejně jako stránka skutečného internetového bankovnictví, odkazy se liší pouze nepatrně, např. tím zda začínají „“, nebo „“.

Falešné webové stránky neboli Spoofing

Věnujte velkou pozornost webovým stránkám, které navštěvujete.

Určitý typ kyberkriminality spočívá v používání podvodných informací a snaží se přesvědčit člověka, že je na pravé webové stránce, a přimět ho prozradit své osobní údaje, jako je např. číslo kreditní karty.

Naštěstí existuje pár kroků, které vám pomohou se chránit před tímto druhem útoků.

Co je falešná webová stránka?

Falešná webová stránka je velice často používána v kontextu s phishingem. Jedná se o podvrženou webovou stránku, která se tváří jako pravá. Nespoléhejte na text v adresovém řádku jako na ukazatel, že jste na té správné adrese. Existuje totiž několik způsobů, jak je možné uvést v adresovém řádku jiný text než té stránky, na které oprvdu jste.

Vyhýbejte se podvodům typu phishing a škodlivému softwaru pomocí používání Internet Exploreru 8

Aplikace Internet Explorer 8 ve svém výchozím nastavení používá filtr SmartScreen, který pomáhá blokovat škodlivý software nebo hrozby útoků typu phishing, a varuje vás před nimi. Filtr SmartScreen zobrazí výzvu, pokud byl web, který se pokoušíte otevřít, oznámen jako nebezpečný, a umožňuje vám také oznámit jakékoli zjištěné nebezpečné weby.

Identifikujte falešné webové adresy

Aplikace Internet Explorer 8 pomáhá vyhýbat se podvodným webům, které se vás snaží nalákat na zavádějící adresy. Název domény na panelu Adresa je zvýrazněn černě, aby bylo snazší určit skutečnou identitu webu.

Úmyslná chyba v názvu webové adresy

Kyberkriminalita také používá názvy webových adres, které připomínají známé, důvěryhodné společnosti. Tyto webové adresy jsou nicméně změněny přidáním, odebráním nebo záměnou písmene, a to tak, že v rychlosti si toho člověk nemusí všimnout. Například adresa www.microsoft.com se může místo toho zobrazit jako www.micosoft.com nebo www.mircosoft.com.

Podvodníci registrují tyto domény, aby je později mohli použít k různým podvodům jako např. Výdělkům z reklamy.

Když zadáte špatnou URL adresu, můžete být přesměrováni na stránku, kde uvidíte reklamu nebo inzerát, který vás osloví. Pokud na banner kliknete, tak podvodník vydělá peníze. Podvodníci také využívají různé záludné postupy, jak stáhnout škodlivý software na nechráněný počítač, který se připojí k jejich webovým stránkám.

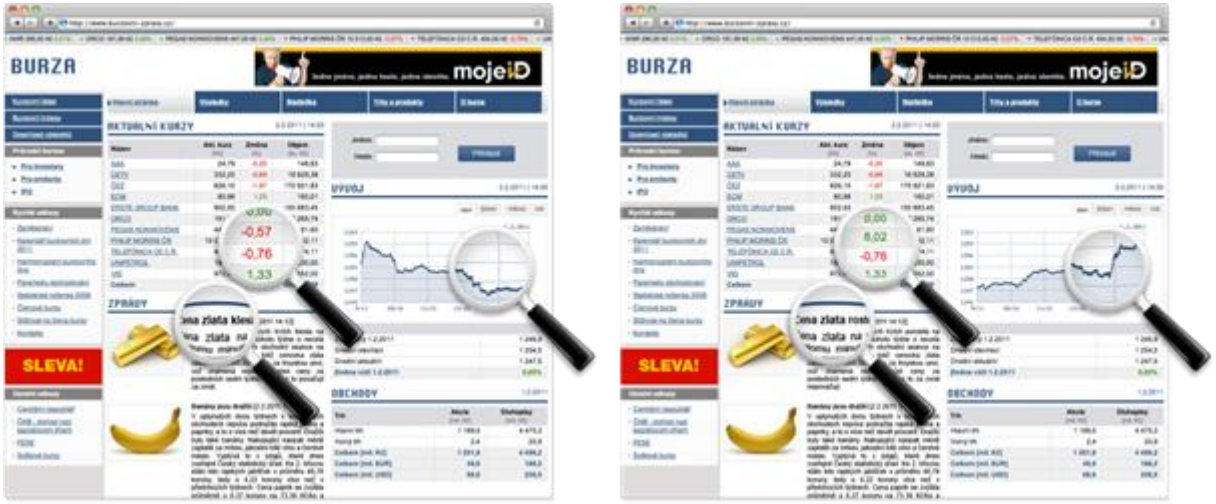
Bezpečné domény

I když uděláte maximum pro zabezpečení svého počítače, stále ještě na Vás uživatele internetu číhá nebezpečí. Je dobré o něm vědět a chovat se obezřetně alespoň u nejzásadnějších webových služeb, které používáte, jako je e-banking, e-mail a sociální sítě.

Jde o bezpečnost domén. Doména je součástí adresy, kterou vypisujete do Vašeho prohlížeče internetu a v rámci českého internetu obvykle končí písmeny „.cz“. Poměrně

nedávno se objevila bezpečnostní hrozba, která spočívá v podvodném přesměrování ze stránky, kterou chcete prohlížet, na jinou stránku. Hlavní nebezpečí spočívá v tom, že podvodník Vás obvykle přesměruje na stránky, které budou vizuálně k nerozeznání od Vaší původně zamýšlené stránky. Zde již dobrovolně vložíte Vaše přihlašovací údaje k emailu nebo bankovnímu účtu a ty obratem získá podvodník. Vy jako uživatel nemáte šanci zrakem poznat, že se nacházíte na jiném webu – dokonce i řádka s webovou adresou bude identická jako originální stránka!

Poznáte, která stránka je originál a která je podvodná?



Pokud útočník napadne podobnou stránku, která obsahuje důležité informace pro Vaše rozhodnutí o nákupu či prodeji cenných papírů, můžete nevědomky konat na základě podvržených informací.

Bohužel uživatelé s tímto problémem mohou udělat jen málo. Řešením je technologie DNSSEC, kterou musí zavést poskytovatelé webových služeb (webových stránek, které navštěvujete) a současně také Váš poskytovatel internetu. Pokud jsou splněny tyto dvě podmínky, budete mít absolutní jistotu, že pokud navštívíte např. zabezpečenou stránku Vaší banky, nebudete podvodně přesměrováni jinam.

Jak se proti podvodnému přesměrování chránit?

- Otestujte si, zda používáte zabezpečené připojení k internetu a také si otestujte Vaše oblíbené webové služby pomocí nástroje na www.bezpecnedomeny.cz. Zde se také dozvíte více informací o problematice zabezpečení domény.
- Pokud zjistíte, že Vaše připojení není zabezpečeno, kontaktujte svého poskytovatele připojení k internetu s žádostí o zavedení technologie DNSSEC.
- V průběhu roku 2011 bude k dispozici plug-in pro prohlížeč Internet Explorer 9, který Vám v rámci prohlížeče jednoduše ukáže, zda Vámi navštívená stránka je zabezpečena technologií DNSSEC.

On-line komunikace

Jednou z věcí, kterou internet světu přinesl, je právě usnadnění komunikace. V dnešní době byste asi hledali složitě někoho, kdo s on-line komunikací v jakékoli podobě nikdy nepřišel do styku. Díky komunikaci on-line se prodlevy mezi předáním jakékoli informace adresátovi zkrátily na naprosté minimum. Rychlostí, jakou předáváme zprávu, předáváme i obsah a vzhledem k povaze celé on-line komunikace již většinou nejsme schopni nijak sledovat další osud námi odesílaných informací. Usnadnění komunikace prostřednictvím internetu s sebou proto nese i jistá rizika a musíme s nimi počítat. Obezřetnost při posílání citlivějšího obsahu, jako jsou osobní data či soukromé materiály, je proto na místě.

Rizika on-line komunikace

Rozmyslete si, co na internetu sdělujete, komu co posíláte a do jaké míry chráníte svoje soukromí.

Díky možnostem, které internet nabízí, se můžete velice snadno seznámit, podělit se o své zážitky nebo sdílet obsah. Internet boří hranice i čas a umožňuje lidem po celém světě komunikovat v reálném čase. S nárůstem moderních technologií nebo aplikací to lze jednoduše přes e-mail, instant messaging, sociální sítě, chaty nebo třeba volání přes internet. S možností komunikace přes internet ale vznikají i určitá rizika, která si možná neuvědomujeme nebo nepřipouštíme. Následující rady by vám měly pomoci v orientaci v základních pravidlech bezpečné komunikace. Největším rizikem je totiž samotný uživatel a jeho chování na internetu.

Největší riziko, které na internetu podstupujete, je ztráta soukromí. Uvědomte si, že to, co na internetu zveřejňujete nebo posíláte, již **nelze ve většině případů vrátit zpět**. Pokud někomu na internetu pošlete fotografii nebo ji zveřejníte všem v síti, počítejte s tím, že jste ji vlastně publikovali. Kdokoli ji může zhlédnout, použít, nebo dokonce zneužít. Zastavit takový proces šíření zprávy nebo nějakého souboru je prakticky nemožný. Proto musíte nad případnými následky uvažovat už před samotným odesláním. Rozmyslete si proto, co na internetu sdělujete, komu co posíláte a do jaké míry chráníte svoje soukromí.

K rychlé komunikaci na internetu slouží mnoho nástrojů. Mezi nejvýznamnější patří e-mail, instant messaging, chaty nebo internetové volání.

E-mail

Je nejrozšířenější formou on-line komunikace. Stejně jako u jiných forem on-line komunikace je jeho výhodou rychlost a možnost posílání příloh. Obsah e-mailu je skrytý, a pokud ho nezveřejní některý z příjemců, nemusíte se obávat, že by byl dostupný všem na internetu.

Uvědomte si ale, že obsah vaší zprávy si může příjemce nejen ukládat, ale i přeposílat dál. Nesdělujte proto žádné citlivé údaje nebo obsah, který vás může poškodit.

Instant messaging

Umožňuje uživatelům sledovat, kteří jejich přátelé jsou právě připojeni, posílat zprávy, chatovat nebo posílat soubory. Výhodou je rychlost a okamžité odeslání zprávy nebo obsahu příjemci.

Mezi nejznámější instant messaging patří ICQ, AIM, Jabber, Windows Live Messenger nebo Skype.

Chat

Nabízí uživatelům možnost komunikovat s více lidmi najednou. Jeho předností je možnost interakce s uživateli. Výhodou pak může být zvýšená šance na seznámení nebo zábavu. Většina provozovaných chatů probíhá v anonymitě, tzn. lidé na nich vystupují pod přezdívkami, nikoli pod pravými jmény. Nikdy tedy nevíte jistě, s kým vlastně ve skutečnosti komunikujete.

Skype

Je program, který umožňuje provozovat internetovou telefonii. Program umožňuje telefonovat mezi svými uživateli zdarma nebo pomocí jiných služeb za poplatek, např. na pevné linky. Další výhodou je zasílání zpráv a souborů mezi uživateli sítě.

Pomocí Skypu můžete vést i videohovory. Ty mohou být rizikem zejména v případě, pokud sdělujete citlivé údaje nebo obsah, který vás může poškodit. Nezapomeňte, že druhá strana vás nejen vidí, ale může si vás i ukládat.

Závislost

Dá se na on-line komunikaci vybudovat závislost? Ano, dá. Existují desítky případů, kdy lidé podlehli výhodám on-line komunikace a tráví desítky hodin na chatech nebo sociálních sítích.

Rady pro rizikové situace

Nepotvrzujte nic, co neznáte. Může se stát, že odešlete do cizích rukou svoje osobní informace, nastavení nebo třeba svůj adresář.

Pamatujte, když se vám stane na internetu jakékoli příkoří, nikdy si ho nenechávejte pro sebe. Vždy existuje nějaké východisko nebo někdo, kdo vám může v dané situaci pomoci.

Mezi nejčastější rizika, se kterými se můžete setkat prostřednictvím on-line komunikace, patří:

Kyberšikana

Stejně jako v reálném životě, potkáte na internetu lidi, kteří se vám budou cíleně snažit ublížit.

Byť je to prostřednictvím internetu a zdá se, že ho stačí jen vypnout, realita je jiná.

- Dostáváte výhrůžky nebo vám na internetu někdo nadává?
- Zesměšňuje vás někdo v článcích, upravených fotkách?
- Někdo vás neustále prozvání a zahlcuje vaše e-maily?
- Zveřejňuje někdo filmy nebo fotky, které vás ponižují?
- Objevují se někde vaše osobní údaje?

Nikdy se nebojte kontaktovat provozovatele stránek, policii nebo se svěřit. Uvědomte si, že zatímco jste lhostejní a necháváte si problém pro sebe, může se zatím na internetu ubližovat někomu jinému.

Ztráta identity

Uvědomte si, že to, co na internetu zveřejníte, už většinou nemůžete vzít zpět. Pečlivě si proto rozmyslete, co o sobě chcete sdělovat.

Denně je prostřednictvím sociálních sítí ukradeno několik desítek identit. Mnohdy o tom uživatelé nevědí - a pokud ano, jen málokdo ví, jak se může bránit.

Jak se bránit v případě zneužití údajů:

- Kontaktujte technickou podporu služby s žádostí o smazání údajů.
- V závažných případech neváhejte kontaktovat policii.

Odcizení osobních údajů a hesel

Na internetu se vyplácí jedna věc. Být ostražitý a nedůvěřivý. Pamatujte, že žádný provozovatel e-mailu nebo jiné služby po vás nevyžaduje zasílání hesla na jiný e-mail. Na internetu jsou velice časté podvodné zprávy, které se tváří jako vzkaz od administrátora. Jedná se ale o podvod.

Svoje heslo nikomu neprozrazujte. Při tvorbě hesla se vyvarujte jeho jednoduché podobě, např. tvaru jména, data narození nebo třeba číslovek 123456.

Doporučujeme znát další údaje k účtům na internetu. Například kontrolní otázku k e-mailu, nejčastější kontakty, naposledy odeslané e-maily, nastavení. V případě ztráty hesla a odcizení e-mailu může znalost těchto informací napomoci k návratu účtu.

Rady pro bezpečnou on-line komunikaci

Pamatujte, když se vám stane na internetu jakékoli příkoří, nikdy si ho nenechávejte pro sebe. Vždy existuje nějaké východisko nebo někdo, kdo vám může v dané situaci pomoci.

Pro bezpečné používání internetu nebo komunikaci jeho prostřednictvím, stačí znát pár jednoduchých, a přesto účinných rad:

- Zvažte, zda je nutné zveřejňovat telefonní číslo nebo adresu.
- Neposílejte nikomu svoji intimní fotografii, nikdy nevíte, kde se může objevit.
- Udržujte hesla (k e-mailu i jiná) v tajnosti, nesdělujte je ani osobě blízké či kolegovi v práci.
- Nikdy neodpovídejte na neslušné, hrubé nebo vulgární maily či vzkazy.
- Nedomlouvejte si schůzku přes internet, aniž byste o tom řekli někomu jinému.
- Nevěřte každé informaci, kterou na internetu získáte.
- Když s někým nechcete komunikovat, nekomunikujte.
- Nesdělujte informace o tom, kde se pohybujete nebo že odjíždíte např. na dovolenou. Po návratu by vás mohlo čekat nepříjemné překvapení.
- Při používání webové kamery buďte obezřetní. Kdokoli může na druhé straně hovor nahrávat.
- Než cokoli potvrdíte, přečtěte si podmínky užívání.

Chat

Vždy je podezřelé, pokud vás budou kontaktovat uživatelé s žádostí o zaslání osobních nebo intimních materiálů. V žádném případě tyto informace neposkytujte. I když kontakt na druhé straně znáte, kdykoli se může stát, že informace o vás zveřejní.

Chat je komunikace v prostředí, ve kterém můžete vést rozhovor s jedním nebo více lidmi najednou. Uskutečňuje se vždy v reálném čase. Některé chaty nabízejí i audiochat nebo videochat. Největším chatem v České republice je chat Lidé.cz, jenž denně navštíví přes 50 tisíc lidí.

Ve špičkách, které jsou většinou ve večerních hodinách, mohou mít některé největší tematické místnosti i několik set chatujících zároveň.

Výhodou chatu je otevřenost a možnost rychlého seznámení a zábavy. Lidé většinou chatují v tematických skupinách. Skupiny se rozdělují např. podle měst, kde žijí, podle zálib, které sdílejí, nebo chatují třeba i o erotice.

Díky otevřenosti chatování je potřeba dát si pozor na zvýšené riziko nebezpečí. Ne každý, kdo na chatu komunikuje, vystupuje pod svou pravou identitou. Velice časté jsou případy, kdy jeden uživatel používá několik účtů (přezdívek/identit).

Rada

Nikdy neposílejte osobní informace nebo obsah, který vás může poškodit, někomu, koho znáte jen z internetu.

Pokud se chcete na internetu seznámit, je chat ideálním nástrojem. Vaše šance na seznámení se zvyšuje podle počtu vyplněných údajů nebo fotografií. Zamyslete se ale nad tím, zda informace, jež zveřejňujete ostatním, nejsou právě ty, které může někdo zneužít.

Rada

Když vás na internetu někdo obtěžuje, neodpovídejte mu. Většina těchto služeb nabízí funkci ignorace.

Na internetových chatech můžete narazit na různé nabídky nebo odkazy na neznámé webové stránky. Stejně jako jinde v prostředí internetu neotevírejte nic, co dobře neznáte. Na pochybné nabídky nereagujte.

Důležité:

Na chatu se můžete setkat s případy páchání trestné činnosti. Spousta uživatelů bere chat jako anonymní médium a pokouší se na něm překračovat meze zákona. Mezi takové činnosti patří např. shánění dětské pornografie, nabídky k prostituci nezletilých nebo prodej kradeného zboží. Pokud se s podobnými případy setkáte, kontaktujte technickou podporu služby nebo se obraťte prostřednictvím formuláře o pomoc: seznamsebezpecne.cz/nahlaste-zavadny-obsah.

E-mail

Při používání internetu se stala hlavním komunikačním kanálem elektronická pošta. Prostřednictvím e-mailu komunikujeme nejen soukromě, ale hlavní roli hraje i v profesní komunikaci. E-mail slouží k odesílání, doručování a přijímání elektronických zpráv. Jeho běžnou součástí se dnes stala i příloha. E-mailem je možné bez problémů poslat soubor menších datových rozměrů, jako jsou dokumenty. Pro posílání příloh s větším objemem dat je ale lépe použít jiné možnosti, které nabízí internet.

E-mailová komunikace je natolik rozšířená a běžná, že najít člověka v produktivním věku, který nemá ani jednu e-mailovou schránku, je poměrně neobvyklé. Například na jednoho člověka připadají na Seznamu dvě e-mailové schránky. Není proto divu, že má Seznam.cz aktuálně cca 7 milionů aktivních e-mailových schránek (za aktivní schránku je považován účet, kde byla zaznamenána aktivita minimálně jednou za dva měsíce).

Stejně jako je tomu všude v prostředí internetu, jsou i s e-mailovou schránkou spojena určitá rizika. Některá jsou jen obtěžujícího charakteru, jako je např. spam. Některá nevyžádaná pošta má ale za účel získat od vás osobní data, či dokonce přihlašovací údaje. Podrobněji se o této kategorii dozvíte v rubrice Phishing. I zde je tedy nutné mít se na pozoru a věnovat pozornost potenciálním rizikům, která se pojí s prostředím internetu, konkrétně e-mailem.

E-mailová komunikace

Věnujte pozornost tomu, zda se při odpovědi na e-mail propíše shodná cílová adresa s adresou, z níž odešel e-mail, na který právě odpovídáte.

Jednou z velkých výhod internetu je usnadnění a zrychlení komunikace. Nejpoužívanější formou komunikace na internetu je e-mail. Slouží k elektronické komunikaci, k odesílání, doručování a přijímání elektronických zpráv. První e-mail se objevil v roce 1965, je tedy starší než samotný internet. S příchodem sítě internet se stal e-mail velmi oblíbeným, protože umožňoval snadný přenos elektronických zpráv mezi různými počítači přes síť. Rychlost doručování informací se tak zkrátila z několika dní na několik vteřin. Proto je zcela logické, že e-mail zcela nahradil některé dosavadní typy předávání informací. Například telegram se stal díky novým formám komunikace už jen vzpomínkou.

V dnešní době je elektronická pošta velmi populární a rozšířená mezi lidmi. Firmy většinou využívají komerční řešení (placené), soukromí uživatelé využívají freemailových služeb jako email.seznam.cz (zdarma).

Jak e-mail funguje?

E-mailová adresa je nedílnou součástí e-mailu. Je ve tvaru uzivatel@domena.cz.

Každá adresa obsahuje údaje:

- jméno uživatele,
- @ - „zavináč“ - tj. znak oddělující uživatelské jméno a jméno domény,
- jméno domény.

Jak vypadá e-mailová zpráva?

E-mailová zpráva se skládá ze dvou částí:

Hlavička - v hlavičce e-mailu jsou uloženy důležité informace pro odesílaní e-zprávy. Skládá se obvykle z následujícího:

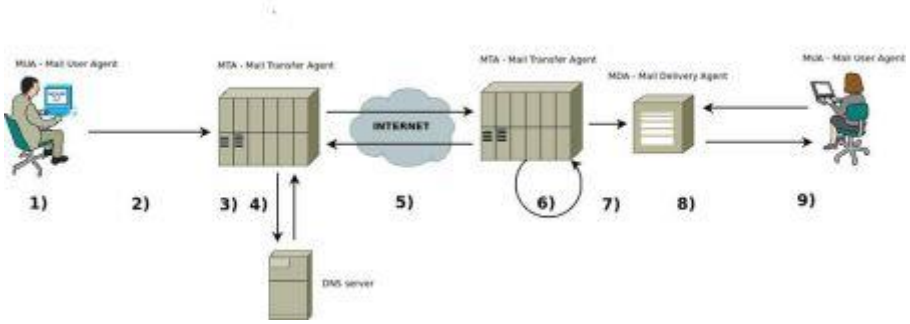
- From: e-mailová adresa odesílatele, případně odesílatelů. Ta je převážně vyplňována automaticky.
- To: e-mailová adresa příjemce nebo více příjemců. Tu vyplňuje uživatel, který zprávu odesílá.
- Subject: předmět dané zprávy. Není povinné ho uvádět, ale patří to k netiketě (internetové etiketě). Vyplňuje odesílatel.
- Date: datum odeslaní zprávy, které se vyplňuje automaticky.
- Může obsahovat další informace, jako je odesílající server, kopie e-mailu, skryté kopie e-mailu, reputace e-mailu, skutečné informace, od koho byla zpráva odesílána. Pokud vám přijde od někoho e-mail, uvedený odesílatel nemusí být skutečně ten, který e-mail odesílal. Je poměrně snadné tuto hlavičku modifikovat. Této slabiny využívají především lidé rozesílající spam.

Tělo - tělo e-mailu je obsah zprávy. Lze ho psát jako obyčejný text nebo je podporován HTML kód, formátování textu.

Jak probíhá odesílání a příjem pošty?

- ❖ Vytvoříte zprávu buď v e-mailovém klientovi (MUA – Mail User Agent), jako je Outlook či Thunderbird, nebo přes webové rozhraní, tzv. webmail.
- ❖ Váš e-mailový klient zprávu předá poštovnímu serveru (MTA – Mail Transfer Agent). **E-mail je odeslán**.
- ❖ Server si ze zprávy zjistí, komu má být e-mail doručen (identifikuje e-mailovou adresu a zjistí doménu, tedy co je za znakem @).
- ❖ Nyní si server z domény zjistí, kam a na jaký server má e-mail začít doručovat.
- ❖ Začne komunikace mezi poštovními servery. Naváže se spojení, odesílající server se „představí“ a požádá o odeslání e-mailu. Pokud vše proběhne v pořádku, e-mail se předá příchozímu serveru. **E-mail je předán**.
- ❖ Příchozí server přijal novou zprávu, proběhne ověření, zdali se nejedná o spam (skupina analýz, porovnávání obsahu zprávy, test existence odesílatele, reputace odesílatele a jiné - to vše vede k vyhodnocení, zda se jedná o spam nebo regulérní e-mail, který má být doručen). **E-mail je poté doručen**.
- ❖ Pokud e-mail není vyhodnocen jako spam, je doručen do inboxu (do doručené pošty) a čeká na vyzvednutí a přečtení uživatelem.
- ❖ Příjemce se přihlásí do své schránky (přes webmail nebo přes e-mailového klienta jako např. Outlook) a zjistí, jestli mu nepřišla nová pošta.
- ❖ MDA odpoví, že má nový e-mail. **E-mail je přečten**.

Všechny kroky jsou znázorněny na obrázku:



Ve skutečnosti je vše ještě složitější, než je zde popsáno, příchozí servery mají obvykle různá zabezpečení proti spamu (používají greylisty), server může odpovědět různými chybovými hlášeními. Proto se občas stane, že e-mail se musí odesílat vícekrát nebo odchozí server musí počkat, než je příchozí server dostupný. Nejenom z těchto důvodů se e-maily mohou zařazovat do tzv. fronty odeslaných či příchozích zpráv, které čekají na odeslaní či přijetí, a může vznikat zpoždění při doručování zpráv příjemci pár minut nebo i několik hodin.

Zabezpečení ke službě e-mail

Pokud se připojujete k e-mailu jinde než na svém osobním počítači v zabezpečené síti, používejte vyšší úroveň zabezpečení.

Myslete na to, že opatrnost je namístě i v případě e-mailové komunikace. Pokud se přihlašujete do e-mailu klasickou formou, tj. nejčastěji přes přihlašovací formulář na webové stránce www.seznam.cz (viz obr. níže), nemusíte se o své přihlašovací údaje obávat. Na server jsou data vždy odesílána zabezpečenou formou. Tedy nikdo vaše heslo nemůže odposlechnout.

Pár základních pojmů, které se týkají zabezpečení e-mailu:

- SSL (Secure Sockets Layer) – je protokol nejčastěji používaný pro bezpečnou komunikaci s internetovými servery pomocí HTTPS.
- HTTPqes je zabezpečená verze protokolu HTTP, který běžně používáte pro prohlížení internetových stránek. Tedy při použití protokolu HTTP a SSL vznikne HTTPS spojení. Po vytvoření spojení mezi klientem (vaším PC) a serverem je veškerá komunikace šifrovaná, a tedy i zabezpečená.

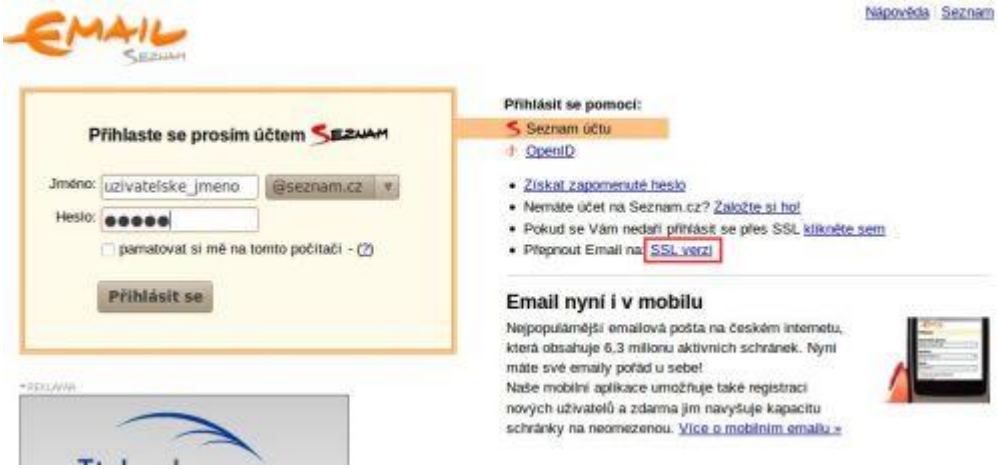
Proč je dobré použít SSL verzi přihlášení?

Při použití SSL verze přihlášení do služby e-mail *získáte vyšší úroveň zabezpečení*. Například pokud budete připojeni k internetu v internetové kavárně nebo v jakékoli nezabezpečené wi-fi síti, může kdokoli v blízkosti získat vaše osobní údaje, jako jsou přijaté e-maily, odeslané e-maily, které vy si prohlížíte. *V žádném případě nemůže zjistit vaše heslo do e-mailové služby*. Internet není jako diskuse mezi kamarády, ale vaše informace putují skrze neznámé servery. Předejít nepříjemným situacím lze jednoduše kliknutím na jeden odkaz - Přepnout e-mail na: SSL verzi.

Jak se bezpečně přihlásit do e-mailu?

Přihlášení do webmailu - přes internetový prohlížeč:

- otevřete ve svém internetovém prohlížeči webovou stránku login.szn.cz/,
- klikněte na tlačítko SSL verzi (viz obrázek),



- po přihlášení se zobrazí adresa odkazu ,

- nyní jste přihlášeni zabezpečeně a veškerá data (čtení e-mailů, odesílání e-mailů na serveru) jsou přenášena šifrovanou formou.

Spam

- Buďte opatrní a přemýšlejte, neotevírejte jakoukoli příchozí poštu.
- Nezveřejňujte zbytečně svou e-mailovou adresu na internetu.

Co je to spam?

Spam je masově odesílaná nevyžádaná elektronická pošta, tedy e-mail odeslaný na obrovské množství e-mailových schránek. Společným znakem těchto e-mailů je to, že spammeři odesílají zprávy na obrovské množství e-mailů. Nejedná se o žádnou cílenou reklamu na vytipovaný okruh lidí, ale o masové rozesílání dané zprávy (reklamy) komukoli. Dalším společným znakem spamu je, že adresa odesílatele je podvržená. Bývá nahrazena neexistujícím odesílatelem nebo nahrazena e-mailem příjemce. Rozesílání spamu je chápáno jako obtěžování, tedy kdyby spammeři odesílali spamy ze své e-mailové adresy, bylo by snadné je dohledat a odpojit od internetu. Hlavním důvodem rozesílání spamu je zisk.

Co spam není?

Spamem v žádném případě není reklamní sdělení, které jste si vyžádali, když jste odsouhlasili posílání reklamních e-mailů např. od firmy, kde jste v minulosti nakupovali. Dále spamem není klasická soukromá nebo obchodní e-mailová komunikace.

Jak se proti spamu bránit?

- Zbytečně nezveřejňovat svou e-mailovou adresu na internetu, tj. neregistrovat se v podezřelých, neznámých formulářích nebo soutěžích. (Na internetu jsou roboti, kteří sbírají e-mailové adresy za účelem rozesílání spamu.)
- Na konci zprávy bývá tlačítko Odhlásit (Unsubscribe). Správně by vás po kliknutí na odhlášení měla tato funkce skutečně odhlásit, ale pokud se jedná o podvodný e-mail, často se přihlásíte jen k odebírání dalších spamových zprav. Pokud si tedy

nejste stoprocentně jisti, že jde o newsletter či obchodní sdělení, k jehož zasílání jste dali dříve souhlas, neklikejte.
- Přemýšlejte, buďte ostražití a neotevírejte jakoukoli příchozí spamovou zprávu.
- Většina spamů je odesílána z uživatelova počítače bez jeho vědomí, protože je jeho počítač napaden virem. Doporučuje se tedy používat aktualizovaný operační systém + firewall + aktualizovaný antivir, jinak může rozesílat spam i váš počítač.

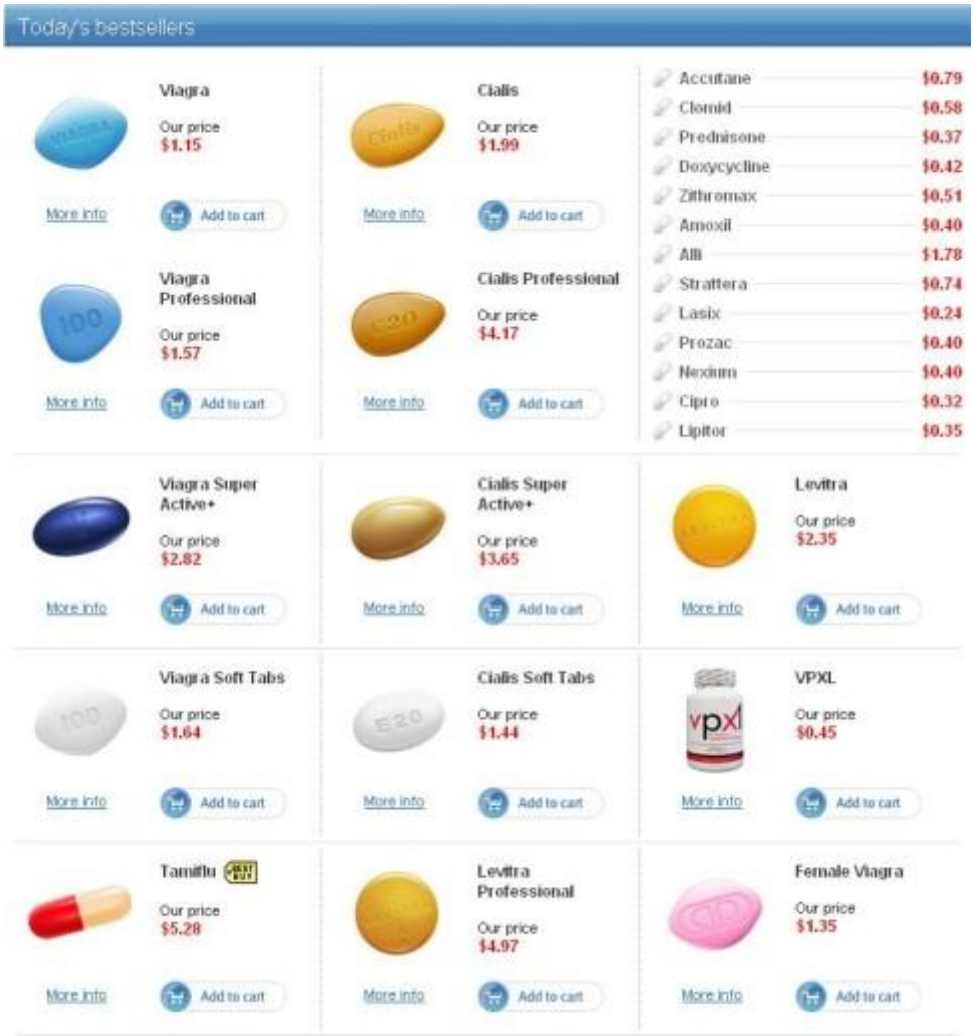
Spam není jen v elektronické poště

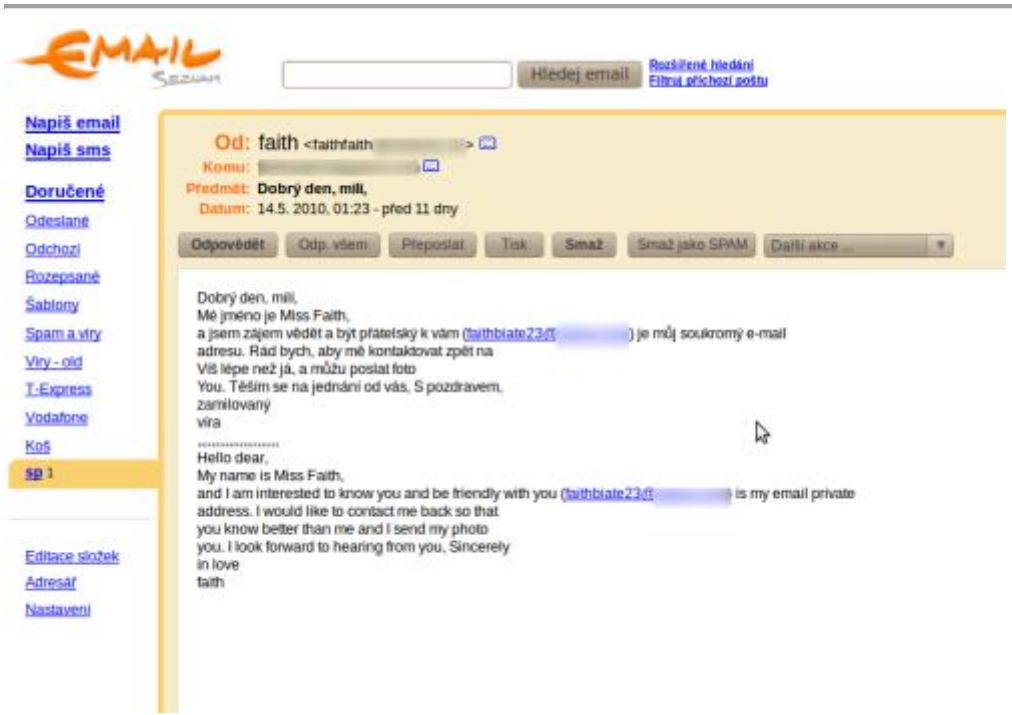
Dříve slovo spam poukazovalo pouze na e-mail, dnes je rozšířené na celém internetu. Spam - tedy nevyžádaný obsah - se objevuje i v diskusních skupinách, instant messagingu (ICQ), blozích, návštěvních knihách a na fórech. Nejnovější trend spamu je SMS spam.

Zajímavosti

- V současné době je celosvětový poměr z celkového počtu e-mailů: nevyžádaná pošta, spam, 93 % a vyžádaná pošta, HAM, 7 %. Ze 100 e-mailů je tedy 93 spamových zpráv a pouze 7 regulérních e-mailů!
- Převážná většina spamu obsahuje reklamu na farmaceutické výrobky.
- Každý den je odesláno 107 miliard spamu.
- Více než 95 % spamu je psáno v anglickém jazyce.

Ukázky spamů:





Spam - právní obrana

- Ne každý „spam“ je spamem podle práva. Vždy se přesvědčte, zda jste někomu nedali v minulosti souhlas (vedlejší podmínky smluv).

- Podejte stížnost k ÚOOÚ a pomozte v boji se spammingem.

Již vás nebaví nalézat každý den ve své e-mailové schránce velké množství otravného spamu? S většinou se sice vypořádá váš počítačový filtr, ale vždy se nakonec objeví nějaké to „smetí“, které vás bude obtěžovat znovu a znovu. Právní rámec nabízí sice pomalejší řešení, ale mívá dlouhodobější a účinnější efekt. Podáte-li správně stížnost, můžete pomoci v dlouhodobém boji se spamem. V určitých případech se můžete dokonce pokusit o dosažení náhrady škody.

V prvé řadě je nutné určit, zda se vůbec jedná o spam. V mnoha případech se stává, že dotyčný dal někdy v minulosti souhlas, byť nevědomky, se zasíláním obchodních sdělení, a to ať již formou e-mailu, SMS, nebo telefonicky. V těchto případech lze vždy jednoduchým způsobem zažádat o vyřazení ze zasílání obchodních sdělení, tzv. opt-out. Vesměs lze nalézt stručné informace např. v patičce e-mailu a často postačí kliknout na zmiňovaný odkaz. V případě, že se opt-out možnost nenabízí, jedná se o porušení zákona o některých službách informační společnosti a lze přinejmenším podat stížnost k Úřadu pro ochranu osobních údajů (ÚOOÚ).

Stížnost

V případě, že obdržíte nevyžádané obchodní sdělení od konkrétního subjektu, lze doporučit vyplnit tento formulář ÚOOÚ. Úřad se se šiřitelem spamu vypořádá veřejnoprávní cestou. Vyplnění formuláře má smysl jen v případech, kdy se jedná (i) o subjekt, který podléhá českému právu, (ii) z obsahu obchodního sdělení vyplývá, že podporuje zboží, služby nebo image subjektu. V případě spamu pocházejícího z jiné země doporučujeme alespoň nahlásit spam na SpamCop (US). Jedná se o projekt, který vytváří globální blacklisty zdrojů spamu.

Náhrada škody

Jestliže žádáte určitou finanční náhradu, musíte se již obrátit k soudu. V tomto případě musíte identifikovat žalovaného a unést důkazní břemeno, tzn. prokázat, že vám žalovaný způsobil svým jednáním škodu. Žalujete tedy z titulu obecné náhrady škody, a musíte tak vyčíslit konkrétní škodu, kterou vám spam způsobil, a to včetně příčinné souvislosti s jednáním spammera. Veškeré tyto věci se bohužel v dnešní době stále velice těžce prokazují. Nutno taktéž upozornit, že soudní proces může trvat relativně dlouhou dobu.

Phishing

Žádná instituce, a už vůbec ne bankovní instituce, po vás nikdy nebude žádat poslání přihlašovacích údajů e-mailem.

Co je to phishing?

Výraz phishing pochází ze slova fishing, tj. rybaření. Přeneseně můžeme říct, že útočník hodí návnadu a čeká, než se uživatel (oběť) „chytí“.

Jedná se o speciální techniku (sociálního inženýrství) používanou na internetu se snahou získat citlivé údaje (přihlašovací údaje, hesla, čísla kreditních karet). Principem těchto zpráv je věrohodné napodobení oficiální žádosti banky nebo podobné instituce a vynutit si od adresáta jeho přihlašovací údaje na odkazované stránce. Po zadání údajů oběti útočník získává přihlašovací údaje. Velkým problémem phishingu je to, že podvržené stránky jsou velmi věrohodné a těžko rozeznatelné. Proto musíte vědět, jak phishing rozeznat a jak se mu bránit.

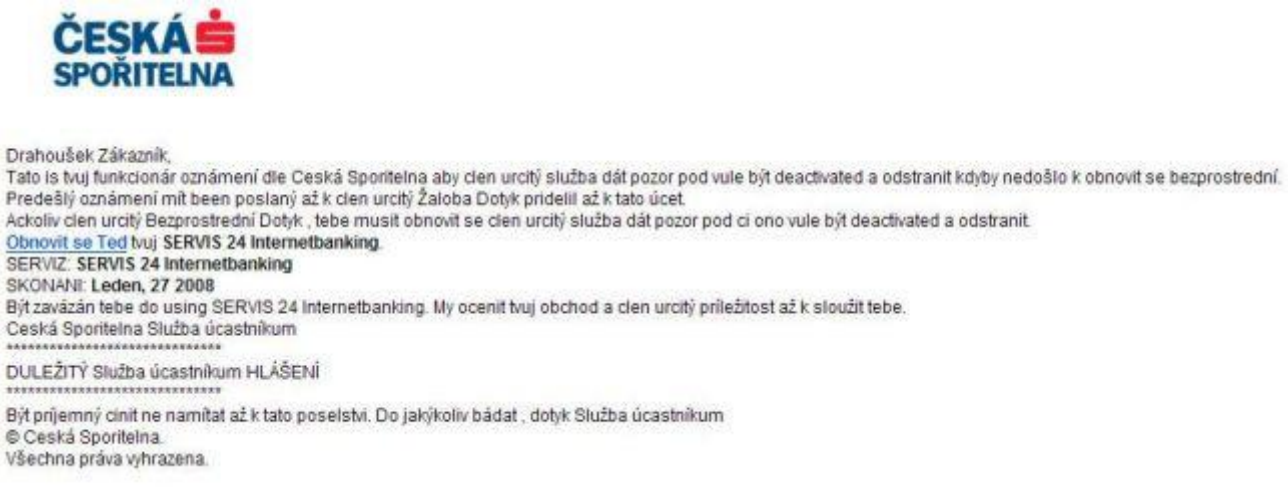
Jak se proti phishingu bránit?

- Doručené e-maily ignorujte, „neklikejte“ na žádné odkazy v e-mailu, pro přihlášení používejte oficiální stránky.
- Buďte opatrní. Mějte na paměti, že phishing nemusí být spojen jen s tématem elektronického bankovnictví, ale je to např. i snaha o získání hesla do e-mailu nebo jiných služeb.
- Buďte opatrní, než se někde přihlásíte či zaregistrujete.
- Myslete na to, že žádná instituce, a už vůbec ne bankovní instituce, po vás nikdy nebude žádat přihlašovací údaje e-mailem. Toto se řeší oficiální formou, nikoli e-mailem.
- Používejte zabezpečené spojení.
- Když phishing pochází ze zahraničí, většinou ho rozeznáte díky špatné češtině, jako je skloňování slov atd.
- Aktualizovaný internetový prohlížeč a e-mailový klient informují uživatele, že se jedná o phishing.
- V neposlední řadě mějte za každých okolností aktualizovaný operační systém, firewall a aktualizovaný antivirus.

Zajímavosti

- Phishingových zpráv je 0,25 % z celkového počtu e-mailů.
- Většina phishingových útoků je na bankovní sektor nebo na služby s ním spojené. Často se také pojí se službami spojenými s penězi, např. Paypal, Paysec aj.
- Několikrát do měsíce objevíme nový typ phishingu.

Ukázka phishingu



Drahoušek Zákazník,
Tato is tvuj funkcionár oznámení dle Ceská Sporitelna aby clen urcitý služba dát pozor pod vule být deactivated a odstranit kdyby nedošlo k obnovit se bezprostrední.
Predešlý oznámení mít been poslaný až k clen urcitý Žaloba Dotyk pridelil až k tato úcet.
Ackoliv clen urcitý Bezprostrední Dotyk , tebe musit obnovit se clen urcitý služba dát pozor pod ci ono vule být deactivated a odstranit.
Obnovit se Ted tvuj **SERVIS 24 Internetbanking**.
SERVIZ: **SERVIS 24 Internetbanking**
SKONANI: **Leden, 27 2008**
Být zavázán tebe do using SERVIS 24 Internetbanking. My ocenit tvuj obchod a clen urcitý príležitost až k sloužit tebe.
Ceská Sporitelna Služba úcastníkum
****
DULEŽITÝ Služba úcastníkum HLÁŠENÍ
****
Být príjemný cinit ne namítat až k tato poselství. Do jakýkoliv bádat , dotyk Služba úcastníkum
© Ceská Sporitelna.
Všechna práva vyhrazena.

From: Ceská sporitelna [mailto:info@csas.cz]
Sent: Monday, May 17, 2010 8:33 AM
To: Sosňak Ivan
Subject: Mate 1 nova

Mate 1 nová VÝSTRÁŽNÁ zpráva
Prosíme obnovujete Vaš účet.
Váš Účet Internetbanking je momentálně zamčený.
K Přihlášení , prosíme kliknete na dole uvedený záznam:

https://www.servis24.cz/ebanking-s24/dispatcher?aid=19991999

© Česká spořitelna a.s. Všechna práva vyhrazena. Materiály určené pro veřejnost.

Sociální sítě

Sociální sítě umožňují sdílení zážitků s vašimi přáteli, ale i s cizími lidmi, kterým to dovolíte. Existuje mnoho tematických sítí - určených k seznámení, hledání a udržování vztahů mezi spolužáky či známými, sítě minoritních či nějakou formou odborných skupin.

Různé společenské sítě mají také různá pravidla a zvyklosti. Proto nemůžeme očekávat, že pro odlišné sítě platí zcela identická pravidla jejich bezpečného užívání. I tak bychom ale našli několik společných bezpečnostních doporučení, která platí pro všechny sítě bez výjimky. Týkají se opatrného sdílení soukromého obsahu či osobních informací.

Co jsou sociální sítě

Sociální sítě slouží k setkávání, k diskusím a chatování. Dnes můžete sdílet i multimediální obsah. Tím ale často přestáváte být anonymní. Seznamte se s potenciálními riziky a myslete na ně při svém pohybu na sociálních sítích.

Sociální sítě jsou na internetu místem k setkávání lidí, sdílení zážitků, obsahu. Očekává se zde vzájemná interakce. Existuje mnoho typů sociálních sítí. Některé vznikají na základě rodinných vazeb, kamarádů, témat, jiné se zaměřují na seznámení.

Původně byly sociální sítě určeny k setkávání lidí, diskusím a chatování. Později s rozvojem moderních technologií došlo k boomu používání a sdílení multimédií. Sociální sítě se staly prostředkem k používání jiných služeb a staly se významným nástrojem k seznámení a udržování vzájemných vazeb.

Mezi významné české sociální sítě patří **Lidé.cz**. Je to síť, která je jasně profilována jako rychlá a anonymní seznamka. Dále **Spolužáci.cz**, jež udržují vazby se současnými i minulými spolužáky. Ze zahraničních sítí tvoří významnou roli **Facebook**, **Twitter** nebo **QQ**.

Používání vícero sociálních sítí se nevylučuje, naopak je v poslední době aktuálním trendem. V České republice používají sociální sítě téměř 3 miliony aktivních uživatelů.

Ochrana osobních údajů na sociálních sítích

Pečlivě si zkontrolujte podmínky užívání služby. V případě porušení podmínek nebo nalezení závadného obsahu, kontaktujte technickou podporu. V závažných případech kontaktujte i policii.

Při registraci na sociální síti jsou vyžadována různá data a údaje. Jejich uvedení je často nepovinné, ale může rozhodovat o úspěšnosti vyhledání nebo zviditelnění uživatele. Mezi takové údaje patří např. jméno a příjmení, telefon, adresa bydliště nebo další osobní údaje.

Před zaregistrováním na některou síť se ubezpečte, jak je v licenčním ujednání popsáno nakládání s osobními údaji ze strany provozovatele. **Mnohé sociální sítě**

používají údaje z profilů uživatelů a nabízejí je třetím stranám. Může se tedy stát, že vaše telefonní číslo nebo adresa zveřejněná na síti budou poskytnuty pro reklamní účely.

Některé sítě nabízejí ve svém rozhraní jiné aplikace. Například hraní her, lokalizaci na mapě nebo sdílení obsahu. Pečlivě si proto zkontrolujte, zda nedáváte svolení k odeslání vašich osobních dat, nebo dokonce neposkytujete adresář vašich přátel.

Obecně platí, že čím méně toho o sobě vyplníte, tím méně se vám může stát. Nejčastěji je zveřejněný obsah zneužit pro vytváření falešných identit nebo ke kyberšikaně.

Rizika sociálních sítí

O rizicích na internetu byl natočen film Seznam se bezpečně, který ve třech příbězích zobrazuje podle reálných událostí rizika spojená s používáním internetu.

Většina sociálních sítí je určena k seznámení a udržování vztahů s kamarády. Údaje, které o sobě vyplníte, sdílíte se všemi přáteli. V případě otevřených sociálních sítí je sdílíte se všemi uživateli celé služby. Díky možnostem, jež sociální sítě nabízejí, se můžete velice snadno seznámit, podělit o své zážitky nebo sdílet obsah.

Uvědomte si, že to, co na internetu zveřejníte, už většinou nemůžete vzít zpět. Pečlivě si proto rozmyslete, co o sobě chcete sdělovat.

Denně je prostřednictvím sociálních sítí ukradeno několik desítek identit. Mnohdy to uživatelé ani netuší. Pokud to zjistí, jen málokdo ví, jak se může bránit.

Rada

Jak se bránit v případě zneužití údajů

- Kontaktujte technickou podporu služby s žádostí o smazání údajů.
- V závažných případech neváhejte kontaktovat policii.

Mýtus: Internet je anonymní.

Skutečnost: Nikdo není na internetu anonymní. Většina provozovatelů udržuje logy k jednotlivým uživatelským účtům a ty pak na základě žádostí předává policii. Informace získané z připojení, mohou významně přispět k dopadení pachatele.

Osobní spory uživatelů provozovatelé sociálních sítí ve většině případů neřeší. Nicméně téměř všechny sítě nabízejí možnost **ignorace**. Pokud vás tedy někdo obtěžuje, tuto možnost využijte. Rozhodně na nevhodné nabídky nebo vulgární zprávy neodepisujte.

Nejčastěji jsou vystaveny rizikům na internetu děti. Informace o školácích denně vyhledává několik set slídilů a mohou cíleně sbírat osobní údaje, fotografie nebo intimní materiály.

Rady pro bezpečné používání sociálních sítí

O rizicích na internetu byl natočen film Seznam se bezpečně, který ve třech příbězích zobrazuje podle reálných událostí rizika spojená s používáním internetu.

Pokud se vám stane na internetu nějaké příkoří nebo se stanete svědky nějaké nestandardní situace, nenechte si ji pro sebe. Vždy můžete kontaktovat technickou podporu, policii nebo Linku bezpečí.

- Neuvádějte na veřejném profilu telefonní číslo nebo adresu.
- Neposílejte nikomu svoji intimní fotografii, nikdy nevíte, kde se může objevit.
- Udržujte hesla (k e-mailu i jiná) v tajnosti, nesdělujte je ani osobě blízké či kolegovi v práci.

- Nikdy neodpovídejte na neslušné, hrubé nebo vulgární maily a vzkazy.
- Nedomlouvejte si schůzku přes internet, aniž byste o tom neřekli někomu jinému.
- Nevěřte každé informaci, kterou na internetu získáte.
- Když s někým nechcete komunikovat, nekomunikujte.
- Nesdělujte informace typu, kdy jedete na dovolenou, po návratu by vás mohlo čekat překvapení.
- Při používání webové kamery buďte obezřetní, kdokoli může na druhé straně hovor nahrávat.
- Než cokoli potvrdíte, přečtěte si podmínky užívání.

Nejčastější příběhy podle Seznam.cz

„Na internetu kolují moje intimní fotky. Zastavte to, smažte je."

Obrátil se na nás Lukáš, že po internetu kolují jeho intimní fotografie. Požádal nás, abychom je smazali. Nic takového není bohužel možné. Pokud na internetu něco zveřejníte, jedná se většinou o nevratnou akci. Lukáš posílal své fotografie dívkám v seznamce. Chtěl tedy po nás, abychom zablokovali dívkám jejich e-maily. Osobní spory, tedy ani soukromou komunikaci, nemůžeme řešit, ani kvůli tomu uživatele blokovat. Dovedete si představit, že by Seznam.cz řešil osobní spory všech svých šesti milionů uživatelů?

Fotografie se mohou se rychle rozšířit, třeba do zaměstnání, školy nebo po celém internetu. Poradili jsme Lukášovi, ať se obrátí na policii. Šíření fotek sice už asi nezabrání, ale s přihlédnutím k závažnosti té či oné situace to může řešit dál.

Pokud vás někdo fotkami vydírá, nebojte se a vše oznamte. Jestliže někdo tvrdí, že je na internetu anonymní, není to pravda. Rozmyslete si tedy, co komu posíláte.

Falešný profil

„Našel jsem svoje fotky v cizím profilu."

Často se na nás uživatelé obracejí s tím, že na internetu našli svoje fotografie v cizím profilu. Stačí, když si někdo stáhne vaše veřejné fotky a doplní k nim odlišné informace. V takovém případě doporučujeme si svůj originální profil ověřit a nechat ten falešný smazat. A jak postupovat? Pokud provozovatel sociální sítě neodstraní falešné informace z internetu, kontaktujte policii. Zde se již jedná o trestný čin.

Někdo mi nadává

„Vadí mi, že mě tahle holka uráží, píše mi, jak jsem ošklivá, a nadává mi. Zablokujte ji."

Zablokovat uživatele na základě soukromé komunikace nelze. Pokud to služba umožňuje, doporučujeme ignoraci. Rozhodně na podobné zprávy nereagujte.

Podvedli mě

„Přišla mi zpráva, že mi bude zrušen účet, pokud nepošlu SMS na uvedené číslo. Mělo to být zdarma, ale tato SMS stála 99 korun. Chci peníze zpět."

Většina služeb je zdarma a administrátoři podobné zprávy neposílají. Jedná se o podvod. Pokud se vám něco takového stane, kontaktujte technickou podporu služby. Provozovatel služby navíc po nikom nechce jeho heslo.

Návod pro nahlášení nevhodného obsahu na sociální síti Facebook

Hej, chceš se pochlubit cool fotkama kámošům? Ale bacha, můžou je vidět i ostatní a třeba i nalákat nebezpečný týpky.

- Pod příspěvkem nevhodného obsahu stačí kliknout na Možnosti a vybrat možnost Nahlásit/Odebrat označení
- Otevře se menu, kde je potřeba označit důvod, proč chceš fotografii nahlásit
- V poslední fázi se zde objeví hláška (poděkování za nahlášení) je potřeba odkliknout OK.

Zabezpečení počítače

Stejně jako si chráníte své domovy pomocí dveří a zámků, je nutné chránit i svůj počítač a data v něm uložená. Podcenit zabezpečení počítače může vést ke ztrátě citlivých dat, ztrátě přihlašovacích jmen a hesel a jejich následné zneužití k nedovolenému obohacení nebo páchání trestné činnosti vaším jménem. Osvojte si základní pravidla pro zabezpečení vašeho počítače.

Aktualizace systému a programů

Pravidelně aktualizujte svůj operační systém a programy v něm nainstalované!

Váš počítač obsahuje operační systém a programy v něm nainstalované. Přestože se jejich tvůrci snaží o maximální zabezpečení, ve většině případů se najdou bezpečnostní chyby, díky nimž lze např. infikovat počítač nežádoucím softwarem a následně ho ovládnout nebo získat přístup k vašim datům. Většina výrobců softwaru poskytuje bezpečnostní aktualizace, které opravují případné chyby. Je však na vás, abyste pravidelně zajišťovali aktualizaci těchto programů a lépe se tak chránili před riziky napadení nežádoucím softwarem.

V případě, že používáte operační systém Windows, je dobré mít zapnuté automatické aktualizace. Ty vás automaticky upozorní na dostupnost aktualizace a provedou její instalaci. Nemusíte se v podstatě o nic starat, pouze zapnout tuto funkci ve vašem systému. Zapnutí této funkce provedete v Ovládacích panelech systému Windows. Více informací najdete v nápovědě k dané verzi vašeho systému.

Pravidelně aktualizujte své programy, zejména pak internetové prohlížeče a jejich doplňky, kancelářské sady, jako je Microsoft Office nebo Open Office. V případě, že daný program nabízí automatické aktualizace, zapněte tuto funkci, tak abyste měli neustále nejnovější verzi se všemi potřebnými bezpečnostními aktualizacemi. Podrobnější informace o aktualizaci jednotlivých programů najdete v nápovědě k danému programu nebo na stránkách jeho výrobce.

Uživatelské účty a nastavení hesla

Nepoužívejte účet administrátora pro běžnou práci s počítačem!

Každý uživatel počítače by měl mít vytvořen vlastní účet, v němž má své osobní nastavení, nainstalované programy a svá data. Většina operačních systémů rozlišuje dva typy uživatelů.

Prvním typem uživatele je administrátor, který má neomezený přístup k systému, může instalovat, odinstalovávat programy a měnit nastavení a oprávnění pro ostatní uživatele.

Druhým typem je standardní uživatel, který má omezená práva. Pro zachování bezpečnosti je žádoucí, aby při běžné práci uživatel pracoval jako standardní uživatel, tak dochází ke snížení rizika infikování počítače. Oba typy uživatelů by pak měly být chráněny dostatečně silným heslem, které nelze jednoduše odhalit a získat tak přístup k danému uživatelskému účtu.

Při nastavení uživatelských účtů a hesel je pak dobré dodržovat tyto zásady:

- Každý uživatel počítače má svůj vlastní účet zabezpečený dostatečně silným heslem.
- Heslo k danému uživatelskému účtu není jednoduše dostupné, např. nalepené na počítači nebo nástěnce.
- Heslo k uživatelskému účtu jednotliví uživatelé, nemají-li k tomu důvod, nesdílejí.

- Pro běžnou práci s počítačem je dobré pracovat jako standardní uživatel, nikoli jako administrátor.

Antivirová ochrana

Udržujte svůj antivirový program stále aktualizovaný!

Viry, červy a jiný nežádoucí software jsou dnes nejběžnějším způsobem, jak získat přístup k počítači a citlivým datům. Je proto nutné hned po instalaci počítače nebo jeho prvním spuštění doinstalovat antivirový program, v případě, že ho neobsahuje. Jestliže je součástí nového počítače i operační systém a antivirový program, je nutné provést jeho okamžitou aktualizaci. Po zapnutí a aktualizaci antivirového programu je teprve možné začít s instalací dalších potřebných programů. Na trhu jsou dostupné komerční antivirové programy, za něž se platí, nebo programy určené pro domácí použití, které mohou být zdarma, např. Microsoft Security Essentials.

Pro maximální ochranu vašeho počítače proto dodržujte tyto zásady:

- Používejte antivirový program hned od prvního okamžiku.
- V případě, že váš nový nebo přeinstalovaný počítač neobsahuje antivirový program, proveďte jeho instalaci jako první krok. Následně můžete začít stahovat a instalovat další programy.
- Je-li součástí vašeho počítače i antivirový program, stáhněte si okamžitě poslední aktualizace, tak abyste byli chráněni i proti nejnovějším hrozbám.
- Pravidelně aktualizujte váš antivirový program, a je-li to možné, zapněte si jeho automatické aktualizace.

Odstranění škodlivého softwaru

Chraňte svůj počítač před nežádoucím softwarem. Nástroj Windows Live OneCare Safety Scanner vám zkontroluje počítač a upozorní vás na případné problémy.

Váš počítač nemusí být vždy dokonale chráněn. Může nastat situace, kdy v počítači budete mít škodlivý software, aniž byste o tom věděli. Takto „nakažený počítač“ může zdánlivě fungovat normálně. Proto doporučujeme využít nástroje Windows Live OneCare, pomocí něhož zkontrolujete svůj počítač na výskyt škodlivého a potenciálně nežádoucího softwaru z webu.

Windows Live OneCare Safety Scanner je on-line služba umožňující zkontrolovat počítač a zajistit jeho ochranu, bezpečnost a maximální výkon. Využijte tento bezplatný nástroj ke kontrole a případnému odstranění virů, spywaru a dalšího potenciálně nežádoucího softwaru a k nalezení slabých míst zabezpečení ve vašem připojení k internetu.

Nástroj pro odstranění škodlivého softwaru v systému Microsoft Windows kontroluje počítače se systémy Windows 7, Windows Vista, Windows XP, Windows 2000 a Windows Server 2003 a napomáhá odstranit některé rozšířené škodlivé programy, jako jsou např. Blaster, Sasser či Mydoom. Jakmile dokončí vyhledávání a odstranění, zobrazuje tento nástroj zprávu popisující výsledek včetně nalezených a odstraněných typů škodlivého

softwaru. Nejnovější verzi tohoto nástroje naleznete na webu služby Stažení softwaru (Microsoft Download Center).

K zajištění ochrany počítače před dalším škodlivým softwarem je k dispozici zdarma ke stažení aktuální antivirový program Microsoft Security Essentials.

Spyware

Používejte antispywarový software, který by měl odhalit spyware ve vašem počítači a odstranit ho!

Spyware je program v počítači, jenž bez vědomí uživatele odesílá data přes internet. Ta jsou většinou následně analyzována a zneužita k různým účelům, jako je přístup k citlivým datům, heslům nebo v některých případech pouze k lepšímu cílení reklamy. V minulosti byl často spyware využíván také ke změně čísla vytáčeného připojení a to pak bylo ve srovnání s běžnou cenou několikanásobně vyšší. Ve všech případech se však jedná o nežádoucí software ve vašem počítači. Mezi časté příznaky výskytu spywaru v počítači může být jeho pomalý start, dlouhé načítání internetových stránek, dále pak změna domovské stránky, kterou jste neprovedli sami, časté pády systému nebo časté vyskakování reklamních oken při procházení internetu.

Do počítače se nejčastěji spyware dostane při instalaci různých programů. Ty mohou mít buď podobu originálního programu, jejich kód byl však částečně změněn a přidán právě spyware, nebo se jedná o programy, které sice poskytují určitou funkcionalitu, ale zároveň obsahují část kódu, jež např. nabízí ve větší míře reklamní okna nebo různé komerční nabídky. Tyto programy bývají také někdy označovány jako adware.

Proti spywaru se dá bránit dodržováním několika zásad, které se v podstatě neliší od ochrany proti jakémukoli nežádoucímu softwaru. Jedná se především o používání antispywarového softwaru v počítači, firewallu, provádět pravidelně aktualizaci operačního systému a internetového prohlížeče, používat nejnovější verzi preferovaného internetového prohlížeče, jež ve většině případů obsahuje pokročilejší způsoby ochrany uživatele. Dále pak neinstalovat podezřelé programy, neoriginální programy nebo programy z neznámých zdrojů, které jsou nabízeny např. na peer-to-peer sítích, nebo nenavštěvovat stránky s podezřelým obsahem, jako jsou erotické stránky nebo stránky nabízející nelegální software, tzv. warez.

Odstranit spyware z počítače lze prostřednictvím některého antispywarového programu. K dispozici jsou placené verze programů i programy zdarma. Jedním takovým programem je i Microsoft Security Essentials, který zároveň funguje jako antivir. Vedle toho lze použít i některé specializované programy na spyware, které mohou doplnit váš antivirový program, např. Microsoft Windows Defender.

Tři způsoby, jak zabezpečit notebook na cestách

Chraňte svůj počítač na cestách. Před každou cestou zabezpečte svůj notebook silným heslem a zazálohujte si svá data na externí disk.

Notebooky již jsou stejně výkonné jako stolní počítače. Navíc jsou lehké a tenké, a proto s nimi můžete vyrážet na cesty. Můžete s nimi cestovat letadlem, autem nebo jakýmkoli jiným dopravním prostředkem. Tato jejich velká výhoda s sebou přináší i velkou nevýhodu a tou je možnost odcizení dat, nebo rovnou celého notebooku.

Mezi základní prvky ochrany se počítá lidská ostražitost. To neznamená nic jiného než to, že svůj notebook budeme mít stále na očích, ne-li při sobě. I přes všechny vaše přípravy se může stát, že vám notebook bude přece jenom ukraden.

Proto doporučujeme před každou cestou, na kterou si berete váš notebook, věnovat krátký čas zabezpečení. Pokud tak neučiníte, v případě krádeže riskujete ztrátu osobních a finančních dat. Buďte proto opatrní a věnujte před každou cestou 5 minut svému notebooku a zabezpečte si svá data.

Zde uvádíme několik nejlepších tipů, jak zabezpečit informace ve vašem notebooku:

Chraňte informace. Pokud máte v počítači uloženo mnoho osobních a finančních informací, investujte do operačního systému zahrnujícího ochranu souborů. Systémy Windows 7 a Windows Vista obsahují nástroje chránící informace pomocí procesu zvaného šifrování. Jedná se o aplikaci Bitlocker.

Chraňte přenosný počítač pomocí složitého hesla. Jestliže s notebookem často cestujete, měli byste jej zabezpečit pomocí složitého hesla. Vyhledejte informace ve službě *Nápověda a podpora vašeho počítače o přidání či změně systémového hesla*. Postup pro vytvoření hesel, jejichž rozluštění bude pro hackery obtížné, ale která si snadno zapamatujete, najdete ve článku Vytvoření silného hesla a jeho vlastnosti.

Před cestou vytvořte zálohu. Před cestováním s přenosným počítačem vždy zálohujte informace. Finanční ztrátě související se zařízením se nemůžete vždy vyhnout, můžete však zabránit ztrátě informací. Operační systémy Windows 7, Windows Vista, Windows XP vám pomohou zazálohovat vaše informace např. na externí disk, USB disk atd.

Zabezpečení bezdrátového připojení

Zamezte, aby neoprávnění uživatelé přistupovali do vaší bezdrátové sítě.

Domácí bezdrátová síť přináší mnoho výhod a lze ji snadno zřídit. Je však důležité bezdrátovou síť správně zabezpečit, jinak kdokoli může přistupovat ke všem vašim síťovým prostředkům, včetně citlivých dat.

- **Nedovolte cizím lidem využívat vaši bezdrátovou síť**. Zabezpečte vaši bezdrátovou síť pomocí hesla. Zapněte zabezpečení pomocí technologie WEP nebo WPA na všech vašich bezdrátových zařízeních.
- **Změňte umístění vašeho bezdrátového zařízení**. Bezdrátovou anténu umístěte vhodně do středu vašeho bytu či domu a omezte tak pokrytí signálem na místech, kde není potřeba.
- **Chraňte vás počítač**. Mějte zapnuté automatické aktualizace. Používejte bránu firewall, antivirový a antispywarový software. Dejte si pozor na falešný bezpečnostní software, který se vydává za produkt od renomovaných výrobců, ale ve skutečnosti ohrožuje váš počítač.

Nastavení brány Windows Firewall

Zapnutá brána Windows Firewall výrazně snižuje riziko napadení počítače prostřednictvím sítě nebo internetu.

Brána firewall pomáhá zabránit počítačovým podvodníkům nebo škodlivému softwaru (např. červům) v získání přístupu k počítači prostřednictvím sítě nebo internetu. Brána firewall může rovněž zabránit tomu, aby počítač odesílal škodlivý software do jiných počítačů.

Brána Windows Firewall má dostupná tři základní nastavení:

- **Zapnuto (doporučeno)** Toto nastavení je vybráno jako výchozí. Když je brána Windows Firewall zapnutá, u většiny programů je komunikace přes bránu firewall zablokována. Pokud chcete zrušit blokování programu, můžete jej přidat do seznamu výjimek.

- **Blokovat všechna příchozí připojení** Toto nastavení blokuje všechny nevyžádané pokusy o připojení k vašemu počítači. Toto nastavení použijte, vyžadujete-li maximální ochranu počítače, např. připojujete-li se k veřejné síti v hotelu nebo na letišti nebo šíří-li se po internetu počítačový červ.
- **Vypnuto (není doporučeno)** Vyhněte se používání tohoto nastavení, pokud není v počítači spuštěna jiná brána firewall. Po vypnutí brány Windows Firewall bude počítač mnohem méně chráněn před počítačovými podvodníky a škodlivým softwarem (jako jsou červi).

Zákony

Na internetu vznikají právní vztahy v mnoha oblastech života. Zákony České republiky tyto vztahy regulují. V současnosti je velmi diskutovanou otázkou zejména zákonná ochrana autorských práv a trestní odpovědnost.

Autorský zákon

Autorský zákon upravuje tzv. autorská práva. To jsou práva autorů k jejich dílům. Dílo je zákonem definováno jako literární a jiné dílo umělecké a dílo vědecké, které současně je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně vnímatelné podobě. Dílem je např. dílo slovesné (např. román), grafické (např. kresba), hudební (např. znělka), choreografické (např. baletní choreografie), fotografické, audiovizuální (např. film), architektonické (stavba) nebo počítačový program. Autorským dílem není pouhý nápad nebo myšlenka, dílo musí být vyjádřeno tak, aby jej někdo jiný mohl vnímat. Od tohoto okamžiku je dílo chráněno autorským právem, není tedy nutná žádná registrace, jako např. u patentů.

Autorská práva se dělí na osobnostní a majetková. Osobnostní zahrnují především právo osobovat si autorství, rozhodnout o zveřejnění díla, právo na nedotknutelnost díla, zejména právo udělit souhlas ke změně nebo jinému zásahu do díla. Majetková práva zahrnují hlavně právo dílo užít a udělit souhlas k užití.

Autorský zákon stanoví, že nikdo nesmí užívat autorská díla bez souhlasu držitele autorských práv, není-li zákonem stanovena výjimka. Pojem „užívání“ přitom znamená:

- **rozmnožování** - zhotovování dočasných nebo trvalých, přímých nebo nepřímých rozmnoženin díla nebo jeho části,
- **rozšiřování** - zpřístupňování díla v hmotné podobě převodem vlastnického práva,
- **pronájem** - zpřístupňování díla za účelem hospodářského nebo obchodního prospěchu poskytnutím originálu nebo rozmnoženiny díla,
- **půjčování** - zpřístupňování nikoli za účelem zisku,
- **vystavování** - umožnit dílo zhlédnout nebo jinak vnímat,
- **sdělování díla veřejnosti** - zpřístupňování díla v nehmotné podobě, živě nebo ze záznamu.

Autorský zákon upravuje udělování licencí k užití díla a stanovuje také případy, kdy licence není třeba. Protože není možné, aby si každý autor ohlídal, zda jeho dílo není užíváno bez jeho souhlasu, ustanovuje zákon tzv. kolektivní správu autorských práv. Pověřená sdružení pak vybírají poplatky za užívání děl (např. od rozhlasových stanic) a zisk rozdělují mezi autory.

Proč a jak chránit na internetu své osobní údaje[2]

Osobní údaje se dnes stávají tou nejcennější komoditou, a to nejen na černém trhu, kde se s nimi obchoduje ve velkém. Při troše „umu“ se totiž dají zneužít při uzavírání, respektive padělání nejrůznějších smluv, při kontrole revizory v MHD a podobně. Lidé, jejichž osobní údaje se dostaly do nepovolaných rukou, se pak nestačí divit. Na internetu o ně můžete přijít neuvěřitelně snadno.

Co jsou a nejsou osobní údaje

Osobním údajem je ve smyslu zákona o ochraně osobních údajů *jakákoliv informace týkající se určeného nebo určitelného subjektu údajů, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu*. V praxi se tedy jedná o kombinaci údajů, která je právě pro vás unikátní. Zdaleka tedy nemusí jít jen o rodné číslo. Osobním údajem pro vaši jednoznačnou identifikaci může být třeba i jméno a vaše adresa, či dokonce e-mailová adresa, pokud je například na firemní doméně a nikdo se stejným jménem u vás ve firmě nepracuje. Na druhou stranu „Jan Novák“ a „Praha 5“ pravděpodobně osobním údajem nebude, protože v této městské části by mohlo Janů Nováků bydlet více.

Co si nejvíce střežit a proč

Nejdůležitější je střežit si ty osobní údaje, které se obvykle dají použít do smluv a při nahlášení identity například revizorům. Zejména je důležité střežit si rodné číslo, adresu trvalého bydliště, místo narození, případně rodné příjmení. Lepší je nedávat z ruky ani přesné datum narození. Bohužel někteří občané mají kvůli aktivitám Ministerstva spravedlnosti a Ministerstva průmyslu a obchodu v tomto ohledu situaci značně ztíženou. Jejich data narození a adresy trvalého bydliště jsou totiž snadno dohledatelné ve veřejném rejstříku, respektive registru živnostenského podnikání.

Vyplatí se ale dávat si pozor i na další údaje – čísla bankovních účtů, čísla platebních karet, na registrační značku vašeho vozidla, čárové kódy na letenkách a palubních vstupenkách, čísla karet do nejrůznějších věrnostních programů a zejména na osobní doklady a jejich případné skeny, kopie a fotografie. Všechny tyto údaje se totiž dají zneužít k získání podrobnějších informací o vás i vašich osobních údajů.

Pozor na stránky a formuláře bez šifrování

Osobní údaje zadáváme na internetu vůbec nejčastěji při nakupování v e-shopech či při registraci do nejrůznějších věrnostních programů. Dávejte proto pozor, zda když svá data, třeba i obyčejnou poštovní adresu, vyplňujete do nějakého registračního formuláře, daná stránka využívá šifrování. Jak to poznáte? Její adresa bude místo http:// začínat https:// a ve webovém prohlížeči uvidíte vedle adresy zelený visací zámeček, někdy doplněný o nápis: „Zabezpečeno“.

Používejte silná hesla, i do věrnostních programů

U všech webů, jimž se rozhodnete svěřit své osobní údaje, tedy i u webů věrnostních programů, cestovních kanceláří, e-shopů a zejména webů leteckých společností, také dbejte na volbu velmi silných hesel. Nepoužívejte stejná hesla pro různé služby. Že si silné heslo pak nebudete pamatovat? Buď můžete používat tzv. správce hesel, speciální program, který si hesla bude pamatovat za vás (dnes to běžně umí i webové prohlížeče), nebo si můžete v případě zapomenutí hesla nechat prostě vygenerovat nové. Z tohoto důvodu je také vhodné, abyste měli velmi silné heslo především ke své e-mailové schránce, kterou používáte pro obnovu přihlašovacích údajů.

[2] http://www.vimkamklikam.cz/soukromi/proc-a-jak-chranit-na-internetu-sve-osobni-udaje 21. 6. 2018

Pomůže i elektronická identita

Cestou, jak si nemuset pamatovat desítky hesel a jak zároveň nedávat z ruky své osobní údaje kdekomu, je tzv. elektronická identita. V Česku je hodně populární a rozšířené mojeID. To provozuje sdružení CZ.NIC, které má na starosti českou národní doménu. Zřídit si ho můžete zcela zdarma a přihlásíte se s jeho využitím na stovky českých webů.

S ochranou údajů brzy pomůže i legislativa

S ochranou osobních údajů vám navíc brzy pomůže i nová evropská legislativa. Nařízení GDPR vstoupí v účinnost po celé Evropské unii během května. Pro správce osobních údajů stanovuje podstatně přísnější pravidla a řádově vyšší sankce než současná česká legislativa a občanům dá nové možnosti, jak si, třeba i prostřednictvím Úřadu pro ochranu osobních údajů, vymoci vymazání jejich osobních údajů z databází nejrůznějších společností.

Mějte osobní údaje pod kontrolou. Jaká práva vám dává GDPR?[3]

Dne 25. května 2018 vstupuje v účinnost ve všech státech EU nařízení Evropského parlamentu a Rady (EU) o ochraně fyzických osob, osobních údajů a o volném pohybu těchto údajů neboli tzv. GDPR. Občanům poskytuje lepší ochranu osobních údajů i řadu nových práv. Chcete vědět, jaká jsou?

Právo přesně vědět, k čemu firma údaje bude využívat

Toto právo pro nás není novinkou, nebo přesněji by nemělo být. 1. června 2000 nám ho dal zákon 101/2000 Sb., o ochraně osobních údajů, který byl ve skutečnosti přeměnou jednotné evropské směrnice 95/46/ES, o ochraně osobních údajů. Každý, kdo po vás chce jakékoliv vaše osobní údaje, je povinen vám přesně popsat, pro jaké konkrétní účely je hodlá využít. Dále je pak za žádných okolností nesmí využít pro účely jiné. To platilo i dříve. Teď za to mohou být jen o několik řádů vyšší pokuty.

Nejen v Česku bylo ale v módě předkládat občanům k podpisu několikastránkové nesrozumitelné souhlasy se zpracováním osobních údajů, nové nařízení GDPR má proto na formu souhlasu se zpracováním osobních údajů poměrně jasně stanovené požadavky. Informace o využití vašich údajů musí naplňovat zásadu transparentnosti a musí být „stručné, snadno přístupné a srozumitelné, podávané za použití jasných a jednoduchých jazykových prostředků a ve vhodných případech navíc i vizualizované“, jak říká odst. 58 preambule.

Mám právo na lepší ochranu svých osobních údajů

GDPR také zvyšuje nároky na následné nakládání s osobními údaji uvnitř firmy. Ta musí zajistit jejich maximální bezpečnost. GDPR doporučuje (avšak nenařizuje) využívat například šifrování a pseudonymizaci dat (zavedení nesrozumitelných identifikátorů pro jednotlivé subjekty údajů). Údaje na papíře by zase měly být pod zámkem. Firmy i úřady musí vést také záznamy o činnostech zpracování (viz článek 30), tedy vědět, kde jsou údaje uloženy, kdo přesně, kdy a proč k nim přistupuje atd.

Právo vědět, když firma neochrání moje údaje

Dřív se mohlo občas stát, že firma vaše údaje neuhlídala. Vy jste se to však nedozvěděli. To s nástupem GDPR už nebude možné. Každý, kdo spravuje vaše údaje, má nově povinnost ohlásit každé porušení zabezpečení a únik osobních údajů Úřadu pro ochranu osobních údajů (ÚOOÚ). A to nejpozději do 72 hodin od doby, kdy se o incidentu dozví. Kromě toho však má v řadě případů povinnost informovat o tomto incidentu i přímo vás. Podrobnosti stanoví článek 34.

Právo být zapomenut

Důležitou novinkou je tzv. právo být zapomenut. GDPR vám v článku 17 dává právo být „bez zbytečného odkladu“ vymazán. Ten, kdo spravuje vaše osobní údaje, tak musí učinit, a to nejen v případě, kdy odvoláte svůj souhlas s jejich zpracováním. To mimochodem můžete učinit kdykoliv. Správce má povinnost vaše osobní údaje vymazat i tehdy, nejsou-li už potřeba pro účely, pro které byly shromážděny. Stejně tak je musí vymazat, když vznesete námitku proti jejich zpracovávání (např. když vás někdo bude

[3] http://www.vimkamklikam.cz/soukromi/mejte-osobni-udaje-pod-kontrolou-jaka-prava-vam-dava-gdpr 22.5.2018

obtěžovat s nevyžádanou telefonickou nabídkou), ale i v některých dalších případech. O takovémto výmazu má zároveň povinnost vás informovat (viz článek 19). Samozřejmě existují i určité výjimky. Nemůžete se třeba vyhnout soudnímu řízení tím, že soudu zakážete zpracovávat vaše osobní údaje.

Právo vědět, co o mě firma eviduje

Jak už jste možná zaznamenali v médiích, umožňuje vám Facebook nově zjistit, jaké všechny údaje o vás eviduje. Přesný návod na to najdete zde. Tato možnost se na Facebooku objevila proto, že vám GDPR dává ve svém článku 15 právo získat od správce údajů potvrzení, zda osobní údaje, které se vás týkají, jsou, či nejsou zpracovávány. Pokud ano, máte také právo získat přístup ke všem těmto osobním údajům i k celé řadě dalších informací, které o vás má správce údajů k dispozici. A přesně to vám teď dává Facebook v této nové položce v menu.

Právo upravovat údaje, které o mě firma má

Pro někoho může být také důležité právo na opravu nepřesných osobních údajů, které o vás někdo spravuje. Pokud jste například členy nějakého věrnostního klubu a ve svém jméně objevíte překlep nebo chcete třeba změnit adresu či doplnit nějaké další údaje, musí vám to ten, kdo tyto vaše údaje spravuje, ze zákona umožnit.

Právo vyjmout své údaje z automatizovaného zpracování

GDPR se zabývá i moderními technologickými trendy v oblasti zpracování osobních údajů za využití umělé inteligence. Zavádí proto pojem „profilování“, což je označení pro jakoukoli formu automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě. Profilování se užívá zejména k rozboru nebo odhadu aspektů týkajících se pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se osoba nachází, nebo pohybu. To je něco, co v minulosti dělala nechvalně proslulá společnost Cambridge Analytica s osobními údaji lidí, které získala bez jejich souhlasu z Facebooku. Od 25. 5. 2018 by jí za to hrozila pokuta ve výši 20 milionů eur nebo 4 % z celkového ročního obratu (podle toho, co je vyšší). Občané EU mají díky článku 22 možnost zakázat správcům údajů podobné profilování nad jejich údaji provádět.

Kde se domáhat svých práv

Pokud jste sdělili své osobní údaje nějaké firmě, nebo se k ní dokonce dostaly bez vašeho souhlasu, a tato firma vám některá z výše uvedených práv upírá, máte právo obrátit se na dozorový úřad. Ten pak prostřednictvím dostatečně silných nástrojů ve formě astronomických pokut vaše právo vynutí. Tento dozorový úřad si každý členský stát stanovuje sám, v České republice je to ÚOOÚ. Důležité je, že vaše práva jsou ve všech členských státech EU identická, stejně jako jsou shodná pravidla, kterými se všichni správci osobních údajů musí řídit. Navíc nová pravidla platí nejen pro firmy, ale také pro veřejné instituce a úřady, i když v případě některých úřadů a zejména soudů platí určité výjimky. Všechny jsou ale vždy v GDPR přesně popsané.

Online vzdělávání aneb kde se zdarma něco naučit[4]

Nikdy nebylo snazší se něco nového naučit. Internet nám otevřel další možnosti, jak se učit nové věci, aniž bychom museli chodit do školy, třeba i o prázdninách. Výhodu přitom mají ti, kdo vládnou angličtinou. I v češtině se však dá najít celá řada zajímavých projektů.

Wikipedia jako zdroj všeho vědění

Asi neexistuje člověk, který by pracoval s internetem a neznal Wikipedii. Wikipedie, bezplatná encyklopedie, nabízí odpověď skoro na všechno, a to i v českém jazyce. Důležité ale je si uvědomit několik základních věcí. Předně Wikipedie je encyklopedie, nikoliv učebnice. Zatímco u klíčových dějinných událostí to tolik vadit nemusí, v případě fyziky, chemie, medicíny a celé řady dalších témat může být pochopení jednotlivých pojmů bez souvisejících znalostí obtížnější. Wikipedie existuje v mnoha různých jazycích. V každém z nich však bývají popisy jednotlivých termínů odlišné a různě rozsáhlé. Je to dané tím, že Wikipedie je otevřená encyklopedie, její obsah závisí na tom, kdo tam co napíše. S tím souvisí i to, že zde mohou být faktické chyby a nepřesnosti. Proti nim se Wikipedie snaží bojovat opravnými mechanismy. Každý, kdo tam najde chybu, ji ostatně může opravit.

Khan Academy / Khanova škola

Na internetu však existují i místa, kde se skutečně můžete něco systematicky učit. Zajímá vás matematika, fyzika, chemie, ekonomie, počítače či dějepis? Na základoškloské a středoškolské úrovni je už mnoho let za nejlepší zdroj učení považována Khan Academy. Ta je, podobně jako Wikipedie, dostupná v celé řadě jazyků včetně češtiny. Podobně jako u Wikipedie, u obou verzí je „studium“ k dispozici zdarma. Původní anglická Khan Academy je zajímavá ještě tím, že nabízí odlišný přístup pro studenty, učitele a rodiče. Rodiče, kteří se tak učí například matematiku se svými dětmi, zde mohou dostat tipy, jak danou látku potomkům lépe vysvětlit.

Coursera

Když se s úrovní znalostí, které chceme získat, posuneme až doslova na univerzitní úroveň, dostáváme se k projektu Coursera. Ten původně vytvořili dva profesoři ze slavné Stanfordovy univerzity, kteří byli nadšeni odezvou na online kurzy, jež univerzita otevřela na podzim 2011. Slovo dalo slovo a dnes na Courseře naleznete kurzy z mnoha nejlepších amerických i světových univerzit. Má to ale háček – v drtivé většině případů jsou anglicky. Často jsou však k dispozici i španělské, francouzské, čínské, arabské a ruské verze. Rychle se rozšiřuje i portugalština, turečtina, ukrajinština, hebrejština, němčina a italština. Pokud ovládáte aspoň jeden z těchto jazyků, může být Coursera tím pravým místem pro vás. Drtivá většina kurzů je přitom opět zdarma. Platí se obvykle jen tehdy, chcete-li získat certifikát o absolvování kurzu, za samotné znalosti ovšem neplatíte.

Jednotlivé kurzy jsou buď kopiemi stejnojmenných předmětů na jednotlivých univerzitách, nebo jsou speciálně vytvořeny jen pro Courseru. Přednášejí zde slavní učitelé z těchto škol, které obvykle znáte jen z jejich knih. Studium je vždy rozděleno do týdnů a v jeho průběhu musíte plnit i domácí úkoly a psát testy. Zejména na amerických školách nechybí časté eseje, jež si hodnotí studenti navzájem. Samotná studijní část v sobě obvykle kombinuje videa (vždy opatřená anglickými titulky), samostudium nejrůznějších statí, vědeckých studií a podobně. Součástí platformy jsou i diskusní fóra.

[4] http://www.vimkamklikam.cz/rady-a-tipy/online-vzdelavani-aneb-kde-se-zdarma-neco-naucit 14. 6. 2018

EdX

Ve stejné době jako Coursera vznikla v USA i studijní platforma EdX. I ta se zaměřuje na online kurzy předních světových univerzit a také za ní stojí slavná americká univerzita, dokonce dvě – Harvard a MIT. Studovat zde můžete i na řadě jiných slavných světových univerzit, včetně těch evropských. Studium probíhá primárně v angličtině. K dispozici bývají i překlady do čínštiny, francouzštiny, španělštiny a hindštiny.

Na rozdíl od Coursery se tu příliš nesetkáte s eseji. Samotný systém, který EdX využívá, totiž nenabízí možnost hodnocení práce spolužáků, na němž stojí bodování esejů u Coursery. O to záludnější tu však bývají testy. Každá otázka je bodovaná zvlášť (u Coursery se test hodnotí jako celek) a můžete na ni mít i více pokusů. Časté jsou otázky s více správných odpovědí. Pro získání bodu ovšem musíte označit všechny správné odpovědi (a jen ty správné). I v tomto případě je drtivá většina kurzů zcela zdarma a platí se jen za získání certifikátu.

Obsah