

# NÚKIB



Národní úřad  
pro kybernetickou  
a informační  
bezpečnost

## ROZCESTNÍK PRO SENIORY

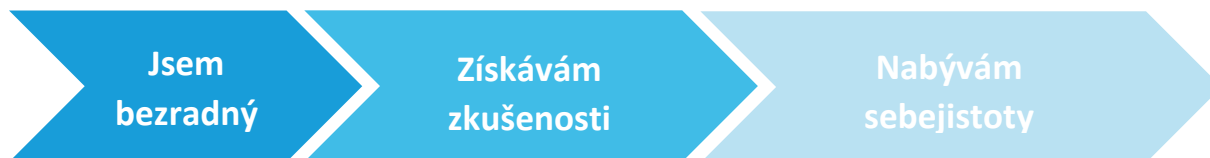
[www.nukib.cz](http://www.nukib.cz)

# ROZCESTNÍK PRO SENIORA

## ZAČÍNÁME

Pohyb na internetu přináší celou řadu výhod a příležitostí. Z pohledu seniora je například skvělé, pokud se může spojit se svoji vzdálenou rodinou nebo přáteli z mládí, kteří žijí v zahraničí. Nakupování on-line může usnadnit život těm, kdo jsou limitováni svým zdravím, sběratelé nejrůznějších věcí mohou získat na bazarových portálech úžasné kousky do svých kolekcí a internetové bankovníctví je při dodržení několika zásad mnohem bezpečnější než peníze uschované doma. Bez dodržování zásad bezpečného chování se však kybernetický prostor může stát i rizikovým. Zde seskupujeme doporučení, rady a tipy, které Vám pomohou případné nebezpečí včas odhalit a předejít nejrůznějším hrozbám. Internetu se nemusíte obávat – je však důležité pohybovat se na něm s rozumem a vědět, na co je potřeba si dávat pozor.

Tímto rozcestníkem prostupují tři znalostní úrovně, které symbolizují profil seniora (od člověka, který nemá žádné zkušenosti, až po člověka, který si je jistý svým jednáním). Nepovažujeme přitom za nezbytné jasně definovat skupinu „seniorů“, jelikož stěžejní jsou právě znalostní úrovně. Tyto úrovně Vám mohou pomoci při sebereflexi i s orientací v tématech, která jsou rozvržena tak, aby se náročnost obsahu systematicky stupňovala.



## TÉMATA ROZCESTNÍKU

V rozcestníku pracujeme s tématy, která považujeme za nosná a nejvíce relevantní. Tato témata dále dělíme do dílčích kapitol, které se snaží celou problematiku prezentovat v kontextu seniorů a jejich každodenního života na internetu. Pohybovat se mezi tématy a dílčími kapitolami můžete za využití navigace – viz dále.

## NAVIGACE



Kliknutím se přesunete na dílčí kapitolu.

Zpravodajství a informace na internetu	Bezpečný pohyb na internetu	Bezpečná komunikace na internetu	Bezpečné nakupování na internetu
Vyhledávání a ověřování informací	Hesla	E-mail	On-line nakupování
	Veřejné počítače a sítě	On-line sociální sítě	On-line platby
	Odkazy a přílohy	On-line seznamky	

## PROFIL SENIORA

**Jsem bezradný: Nemám povědomí o rizicích spojených s internetem.** Učím se obsluhovat digitální technologie a zatím nevyužívám internet k prohlížení zpráv, internetovému bankovníctví, nakupování ani k běžné komunikaci. Zakládám si profily s pomocí. Nevím, jak vypadá bezpečné heslo a neznám další zásady bezpečného chování – chodím na počítač v knihovně a tam mi nic nehrozí. Věřím všem informacím, proč by mi někdo lhal? Pokud mě někdo seriózní požádá o heslo ke kontrole jeho bezpečnosti, předám ho bez váhání. Myslím si, že fyzický a virtuální svět jsou vzájemně oddělené.

**Získávám zkušenosti: Mám povědomí o rizicích spojených s internetem a ovládám základy bezpečného chování.** Dokážu obsluhovat digitální technologie jako uživatel, ale jsem spíše samouk. Problémy mám až s náročnějšími úkony jako jsou třeba aktualizace nebo instalace. Využívám základní služby internetu, například zpravodajství, e-mail i sociální sítě, a mám povědomí o tom, že on-line prostor může být i rizikový. Chápu, že se na internetu můžu setkat i s podvodným jednáním, ale orientuji se jen v úzkém pásmu. Například vím, jak vypadá bezpečné heslo a nikomu ho neposkytnu, ale pod pojmem „Phishing“ si nic nepředstavím. Víím také, že ne všechny informace uvedené na internetu jsou pravdivé. Jenže co s tím?

**Nabývám sebejistoty: Chápu rizika spojená s internetem. Chovám se bezpečně.** Využívám paletu služeb, které internet nabízí – běžně komunikuji se svými přáteli na sociálních sítích, využívám internetové bankovníctví, nakupuji v e-shopech nebo navštěvuji on-line seznamku. Bezpečné heslo je pro mě samozřejmostí a nejsem přehnaně důvěřivý. Kontroluji certifikáty HTTPS, ověřuji si informace a vím, že existují i falešné profily, inzeráty či zprávy. Všechny zásady neznám jen teoreticky, ale dokážu je také použít ve svém každodenním životě. Fyzický a virtuální svět chápu jako silně propojené.

Tato ikona značí video, které si můžete pustit kliknutím.



# ZPRAVODAJSTVÍ A INFORMACE NA INTERNETU

## VYHLEDÁVÁNÍ A OVĚŘOVÁNÍ INFORMACÍ

Internet je zdrojem nepřehledného množství informací a zpráv, které se k příjemci dostanou přímo bleskově. Abychom však mohli hledat zprávy, obrázky nebo videa, je důležité vědět, [jak na to](#) – základní možnosti vyhledávání představuje přiložené video:



### Vyhledávání informací

To s sebou však nese i nevýhody, protože na internetu může psát a šířit informace v podstatě každý. Je tak nezbytné informace a zprávy ověřovat a nevěřit všemu, co vidíme. Můžeme totiž narazit i na záměrně zkreslené informace, které příjemce ovlivňují a manipulují – říkáme jim [dezinformace](#) či [fake news](#). Jiné zprávy mohou být jen šikovně ukrytou reklamou. O důvěryhodnosti internetu se více dozvíme [zde](#):



### Důvěryhodnost informací

Už víme, že informace je nutné ověřovat. Jak to ale prakticky udělat? Pro začátek doporučujeme pročíst [Surfařův průvodce po internetu](#) od iniciativy Zvol si info. Dalším užitečným vodítkem pro podporu kritického myšlení jsou následující manuály pro ověření [videa](#) a [obrázku](#). Jedná se o soubory otázek, které mohou napomoci rozpoznat například fotomontáž, tedy záměrně upravenou fotografii. Pokud některou odpověď neznáme, raději zbystríme. Precizní manuál pro ověřování nabízí třetí video:



### Vyhledávání informací pro pokročilé

## TIPY:

Máte vnouče nebo mladého člena rodina? Problematikou věrohodnosti informací na internetu můžete procházet společně a dobře se u toho pobavit! Podívat se můžete například na díly z cyklu „Nauč tetu na netu“ od České televize:



Nauč tetu na netu – Kdo řídí internet?



Nauč tetu na netu – Flame wars

Můžete si společně projít i [jednoduchou interaktivní hrou](#), která se zabývá dezinformacemi. Za pomoci jednoduchých zábavných úkolů uvidíte, jakým způsobem přemýšlí lidé, kteří šíří dezinformace a jaký z toho mají užitek a prospěch. Své znalosti o vyhledání a ověřování informací na internetu si můžete zopakovat, dále rozvíjet a jednoduchým kvízem ověřit [zde](#).

## DALŠÍ ZDROJE:

Nakolik jsou faktické a pravdivé výroky politiků? Na ověřování takových výroků se zaměřuje [Demagog.cz](#), kterého můžete sledovat i na [Facebooku](#). Zde pak naleznete brožury, které Vám usnadní ověřování informací tak, abyste na nic nezapomněli. Můžete si je stáhnout do svého počítače nebo i vytisknout. Vyhledávat informace Vám usnadní [tato brožura](#) a vyhýbat se podvodným zprávám a dezinformacím [tato brožura](#).

# BEZPEČNÝ POHYB NA INTERNETU

## HESLA, VEŘEJNÉ POČÍTAČE A SÍTĚ, ODKAZY A PŘÍLOHY

Pokud se chceme bezpečně pohybovat na internetu, naprostým základem je mít nastavená dostatečně silná a bezpečná hesla u každé služby, tedy například u e-mailu. Nepoužíváme stejná hesla všude, ani si je nepíšeme na kousek papíru, i to je nebezpečné – stáváme se snadnou obětí. Nikdy heslo nesdělujeme.




Bezpečná hesla 1



Bezpečná hesla 2

Ta nejvíce nebezpečná hesla vypadají například jako 123456, ABCDE, 123ABC a další podobná, anebo hesla, která vychází ze jména či adresy. **Ta nejlepší hesla mají vždy alespoň osm znaků, speciální znak, třeba hvězdičku, obsahují malá i velká písmena a také čísla. Další tip pro silné heslo je například část oblíbené písničky nebo upravená oblíbená filmová hláška.**

Při tvorbě hesla si můžeme jeho bezpečnost ověřit například na této [stránce](#). Do okna napíšeme heslo a pokud obrazovka zezelená, je silné. Pokud naopak zčervená, není dobré. Vymyslete lepší. Útočníci využívají i různé pokročilé metody – mohou nás oslovit například e-mailem, ve kterém se vydávají za Policii. V takovém případě si vše ověříme na čísle 158. V momentě, kdy v e-mailu nalezneme zprávu, která se tváří jako z banky, důkladně zkontrolujeme odkazy a hledáme tento zelený zámeček:  [Česká spořitelna a.s. \(CZ\)](#) Není ostuda zavolat i do banky a vše ověřit, stejně jako kamkoliv jinam. Existují totiž i podvodné stránky, které naše přihlašovací údaje odešlou útočníkovi, tomu říkáme Phishing.



Certifikáty

## TIPY

Máte vnouče nebo mladého člena rodina? Tématem bezpečných hesel můžete procházet společně a dobře se u toho pobavit! Objevujte spolu cestu bezpečného internetu za pomoci videí od České televize – Nauč tetu na netu nebo s Youtuberem Jiřím Králem a dalšími!



Nauč tetu na netu – Hesla



Hesla s Youtubery

## DALŠÍ ZDROJE

Své znalosti z oblasti bezpečnosti hesel si můžete zopakovat, rozvíjet a následně ověřit [krátkým kvízem](#) a kompletní a [pokročilejší manuál](#) pro tvorbu silného hesla pak přináší přímo společnost Google.



# BEZPEČNÝ POHYB NA INTERNETU

## HESLA, VEŘEJNÉ POČÍTAČE A SÍTĚ, ODKAZY A PŘÍLOHY

Ne každý má doma svůj vlastní počítač a připojení k internetu. To však nebrání tomu, abychom se na internetu mohli pohybovat – existují i jiné možnosti. Můžeme se připojit například z prostředí knihovny nebo kavárny. **V takovém případě jsme však obezřetní a sledujeme například i to, jestli se nám někdo nedívá přes rameno.** Možná to zní komicky, ale i to je způsob, jak získat něčí heslo. Další zásady zprostředkuje přiložené video:



Veřejné počítače

Základní zásadou je tedy neukládat hesla do veřejných počítačů a vždy se odhlašovat. Postup odhlašování určuje například [tento manuál](#). Pokročilejší zásady a rady se můžeme dočíst na stránce s názvem [Bezpečný internet](#). **Například ve vlaku nebo v obchodních centrech bývají i wi-fi sítě, tedy bezdrátové připojení k internetu, které nevyžadují heslo.** Nemusí být vždy nebezpečné, jsou ale zneužitelné. Proto pokud se připojíme na takovou síť, nepracujeme s internetovým bankovníctvím ani jinými citlivými službami, a nenavštěvujeme stránky, které nejsou zabezpečeny certifikátem (viz hesla a Phishing). Tyto veřejné wi-fi sítě jsou ideální například pro zjišťování dopravních spojů, otevírací doby a podobných informací.

Další pokročilejší rady představuje taktéž stránka [Bezpečný internet](#). Existují také programy, které nás na takových veřejných sítích chrání – [jeden z nich vyvinula společnost Avast](#). Je zdarma a po instalaci do našeho zařízení nám umožní z veřejné sítě vytvořit soukromou síť i s heslem. Chránit naše bezpečí na takových sítích může pomoci i anonymní režim, který v počítači nezanechá stopy o stránkách, které jste navštívili.

## TIPY

Máte vnouče nebo mladého člena rodina? Tématem veřejných sítí můžete procházet společně a dobře se pobavit! Objevujte spolu bezpečný internet s Youtuberem Jiřím Králem!



Jiří Král – Veřejné sítě

Své znalosti o veřejných počítačích a sítích si můžete zopakovat, dále rozvíjet a následně ověřit [krátkým kvízem](#). Další [rady a doporučení](#) jak rozeznat bezpečnou síť od potenciálně nebezpečné přináší společnost Google. A jak zapnout výše uvedený anonymní režim se dozvíte v následujícím odkazu – záleží však na tom, jaký používáte internetový prohlížeč. Jak tento režim [aktivovat Vám poradí](#) přímo Seznam.cz.

# BEZPEČNÝ POHYB NA INTERNETU

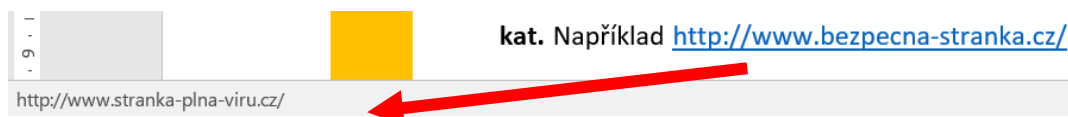
## HESLA, VEŘEJNÉ POČÍTAČE A SÍTĚ, ODKAZY A PŘÍLOHY

Internet tak, jak ho známe, funguje díky odkazům. Odkazy jsou v podstatě adresy jednotlivých internetových stránek. Příkladem takové adresy může být <http://www.nukib.cz>. Díky těmto odkazům, které jsou typicky modré, pak můžeme jednoduše procházet obsah internetu pouhým klikáním na tyto adresy, aniž bychom si museli adresy jednotlivých stránek pamatovat.



### Obezřetnost na internetu

S takovými odkazy je však možné poměrně jednoduše podvádět uživatele tím, že směřují někam jinam, než jak se na první pohled tváří. Některé služby na takový odkaz upozorní samy, ale je důležité být na pozoru. **Skutečný cíl odkazu si ověřujte na obrazovce vlevo dole – stačí na odkaz najet myší a na nic neklikat.** Například <http://www.bezpecna-stranka.cz/> může směřovat úplně jinam:



Existují i služby, které umí neprakticky dlouhý odkaz zkrátit. Na tom nemusí být nic špatného, ale i tohoto nástroje je možné zneužít k uschování odkazu, který je nebezpečný. Takový zkrácený odkaz může mít například tuto podobu: <https://bit.ly/2RTyxPR>, i když jeho původní podoba vypadá následovně: <https://www.govcert.cz/cs/informacni-servis/doporuceni/2325-phishing-stale-aktualni-hrozba/>. Na druhou stranu máme ale i nástroje, které naopak umí takové zkrácené odkazy rozbalit, k čemuž slouží například služba <https://www.expandurl.net>. Stačí sem vložit zkrácený odkaz ještě před jeho otevřením a ihned vidíme jeho pravou podobu a víme tedy, kam skutečně směřuje.

## TIPY

Máte vnouče nebo mladého člena rodina? Tématem výše uvedených praktik, Phishingu, můžete procházet společně a dobře se pobavit! Objevujte spolu bezpečný internet s Youtuberem Jiřím Králem!



Jiří Král – Phishing

## DALŠÍ ZDROJE

Vlastní [náповědu](#) k nebezpečným odkazům přináší přímo i Seznam.cz. Jak bylo výše uvedeno, s podvodnými odkazy často souvisí Phishing – přehledně [zpracované heslo](#) na toto téma připravila společnost ESET, která se specializuje na bezpečnost technologií. Mnohdy může být součástí e-mailu i nebezpečná příloha, která obsahuje škodlivý kód, kterému říkáme počítačový virus. Ten může ve Vašem počítači škodit různými způsoby, rozesílat z něj podvodné zprávy a tak dále. I toto [rozšiřující heslo](#) zpracovala společnost ESET.

# BEZPEČNÁ KOMUNIKACE NA INTERNETU

## E-MAIL, ON-LINE SOCIÁLNÍ SÍTĚ, ON-LINE SEZNAMKY A INTIMNÍ ŽIVOT

Internet umožňuje rychlou komunikaci. Základním způsobem takové komunikace je e-mail, tedy elektronická pošta. E-mail, zjednodušeně řečeno, funguje stejně jako klasická pošta – [i zde je odesílatel, obsah zprávy a příjemce](#). Základem bezpečné komunikace je pak silné a bezpečné heslo (viz hesla).



Bezpečný e-mail 1



Bezpečný e-mail 2

I naše e-mailová schránka se přitom může stát terčem nějakého útoku – poměrně častým jevem jsou právě odkazy, [které směřují jinam](#), než jak se tváří (viz odkazy). Útočník rozešle stovky e-mailů s podvodným odkazem a pouze čeká, kdo se chytí do pasti. Jedním z nejvíce palčivých problémů, které e-mailovou komunikaci postihují, je spam a hoax. Spam je nevyžádaná zpráva, která mívá obvykle reklamní charakter a často se snaží působit dojmem, že nám někdo něco nabízí zdarma nebo že jsme něco vyhráli.



Nigerijské dopisy



Kyberšmejdi

Hoax je naproti tomu poplašná zpráva, která se nás [snaží vyděsit a nabádá k jejímu sdílení](#). Takový hoax škodí například tím, že může poškodit něčí pověst – třeba nepravdivá zpráva o zapíchnuté injekční stříkačce v MHD vyvolává zbytečnou paniku. Příklady takových zpráv můžeme najít například [zde](#). Tyto zprávy nerozesíláme dál, i když máme chuť pomáhat a varovat ostatní. Pokud odesílatele takové e-mailu známe, zdvořile ho upozorníme a uklidníme.

## TIPY

Máte vnouče nebo mladého člena rodina? Problematikou e-mailu, jeho výhod a hrozeb můžete procházet společně a dobře se u toho pobavit! Objevujte spolu cestu bezpečného internetu za pomoci videí od České televize – Nauč tetu na netu!



Nauč tetu na netu - Email

## DALŠÍ ZDROJE

Skutečné příběhy lidí z České republiky, kteří se setkali s podvodným jednáním vykonaném za využití e-mailu, si můžete přečíst [zde](#). Dozvíte se i to, jak reagovat, pokud se stanete cílem podobného útoku.

Už víte, že e-mailová schránka umí spam včas rozlišit a uložit do příslušné složky, kde nikoho neobtěžuje. Existuje ale i [soubor doporučení](#), které tuto obranu učiní ještě více účinnou. Pokročilejší návod s komentářem, pomocí kterého můžete rozpoznat podvodný e-mail, poskytuje tento [článek](#). Zde pak naleznete [manuál v podobě plakátu](#), který může být užitečný při rozhodování, zda zpráva, kterou jste obdrželi, je pouhý hoax – plakát si můžete vytisknout a pověsit.

# BEZPEČNÁ KOMUNIKACE NA INTERNETU

## E-MAIL, ON-LINE SOCIÁLNÍ SÍTĚ, ON-LINE SEZNAMKY A INTIMNÍ ŽIVOT

Výhodou [on-line sociálních sítí](#) je skutečnost, že oproti e-mailu nabízí kromě komunikace i vyhledávání známých, například přátel ze školy, z vojny nebo vzdálených příbuzných. Musíme si však uvědomovat, že to, jakým způsobem se zde chováme, co píšeme a sdílíme, není oddělené od reality. Naopak. Mezi nejvíce rozšíření sítě patří [Facebook](#) nebo [Instagram](#), který slouží především ke sdílení fotografií.



**Etické sdílení**



**Sociální sítě - úvod**

Nicméně i on-line sociální sítě mohou útočnickům posloužit jako nástroj, který zvýší efektivitu jejich útoků. Prvotní zásadou je opět silné a bezpečné heslo. Heslo si neukládáme na veřejných počítačích a nezapomínáme se odhlašovat. Další zásadou je správné nastavení [soukromí, kterým můžeme určit, kdo a co vidí](#). V podrobnějším nastavení můžeme také určovat, kdo vidí, koho máme přidaného přátelích nebo co sledujeme. Konkrétní postup přináší přiložené video:



**Jiří Král – Sociální sítě**



**Rizika na sítích - úvod**

Měli bychom tedy být obezřetní při komunikaci s kýmkoliv, nejen s cizími lidmi. Mysleme také na to, že nás může ohrozit i odcizený profil někoho ze známých, kdo výše určené zásady nedodržel. [Tato stránka](#) nám pak přináší postupy a doporučení, jak správně nastavit zabezpečení sdílení u různých služeb, nejen u výše jmenovaných.

## TIPY

Máte vnouče nebo mladého člena rodina? Problematikou sociálních sítí, jejich rizik, zásad bezpečného chování či trendu tzv. Youtuberingu můžete procházet společně a dobře se u toho pobavit! Objevujte spolu cestu bezpečného internetu za pomoci videí od České televize – Nauč tetu na netu! Podívat se můžete také na další videa, kde vše řeší slavní čeští Youtubeři:



Nauč tetu na netu



Sociální sítě a Youtubeři 1



Sociální sítě Youtubeři 2

## DALŠÍ ZDROJE A TIPY

Své znalosti si můžete zopakovat a ověřit [krátkým testem](#). Nebo spolu s ratolestí kvízem Jirky Krále.



Jiří Král – opakování

Pokud jste na sociálních sítích, může být užitečné sledovat stránky, které se dotýkají problematiky bezpečného internetu. Udržíte si tak povědomí o aktuálním dění, dostanete včasné varování atp.:

- <https://www.facebook.com/kpbicz/>
- <https://www.facebook.com/PolicieCZ>
- <https://cs-cz.facebook.com/InternetemBezpecne/>
- <https://cs-cz.facebook.com/EBezpeci/>
- <https://cs-cz.facebook.com/saferinternet.cz>

Zde pak naleznete [stručnou brožuru](#), která Vám pomůže orientovat se na sociálních sítích a vyhodnocovat případná rizika – můžete si ji i vytisknout.



# BEZPEČNÁ KOMUNIKACE NA INTERNETU

## E-MAIL, ON-LINE SOCIÁLNÍ SÍTĚ, ON-LINE SEZNAMKY A INTIMNÍ ŽIVOT

Kromě vyhledávání přátel a příbuzných může internet posloužit i [pro navazování zcela nových známostí](#). K tomu slouží on-line seznamky, které umožňují najít nové životní partnery. I zde však existuje řada rizik, které bychom si měli uvědomovat – zmínit můžeme například různé formy [kybergroomingu](#). O tom pojednávají videa:



On-line seznamky



Kybergrooming

V momentě, kdy se s někým seznámíme on-line, bychom neměli být přehnaně důvěřiví. Útočník se typicky projevuje milým chováním a postupně si získává naši přízeň. Jeho cílem je osobní schůzka – na té může svou oběť obtěžovat, oloupit nebo jen vylákat mimo domov a vykrást. V případě, kdy si u oběti vybuduje citovou vazbu, může chtít například finanční půjčku, ke které si připraví [dlouhý a zamotaný příběh](#), jak se dostal do nepříznivé situace.

Vše ilustruje přiložené video:



Nauč tetu na tetu

Jak se tedy bránit? Při zakládání profilu na sebe [neprozrazujte více, než je nutné](#). Nikdy neposílejte žádné osobní či citlivé údaje, které by útočnickovi ulehčily práci. Ne každý, kdo se chce na internetu seznámit, musí být nutně nebezpečný. I přesto, pokud si sjednáte osobní schůzku, informujte o tom někoho ze svých blízkých a místo setkání zvolte tak, aby bylo neutrální a frekventované – ne u Vás před domem.

## TIPY

Máte vnouče nebo mladého člena rodina? Problematikou on-line seznamování a kybergroomingu můžete procházet i společně a dobře se u toho pobavit! Podívat se můžete například na videa, kde vše řeší slavní čeští Youtubeři:



**Kybergrooming a Youtubeři**



**Jiří Král - Kybergrooming**

[Minifilm](#) na toto téma natočil Seznam.cz. V případě, že Vás tato problematika zajímá více do hloubky, doporučujeme ho zhlédnout. Svě znalosti o bezpečném seznamování na internetu a souvisejících tématech si můžete také zopakovat a ověřit krátkým kvízem – [kapitoly 5 a 6](#).

# BEZPEČNÉ NAKUPOVÁNÍ NA INTERNETU

## NAKUPOVÁNÍ NA INTERNETU, INTERNETOVÉ PLATBY

[Nakupování na internetu nám přináší řadu výhod](#) – donáška zboží až domů se může hodit třeba v případě nepříznivého počasí nebo zdravotního znevýhodnění. Je však potřeba vnímat i rizika, která jsou s touto možností spojená a [vědět, na co si máme dávat pozor](#), aby Vám místo objednaného zboží nepřišla třeba zabalená cihla. Zásady bezpečného chování při nakupování přináší tato videa:



**Bezpečně nakupování**



**Aukce a bazary**

Dalším rizikem jsou kyberšmejdi – nekalí obchodníci, kteří se nás snaží podvést, třeba nalákat na zboží pochybné kvality s tím, že ho propagují jako exkluzivní. Typicky využívají oslovení e-mailem. O konkrétních praktikách pojednává [audionahrávka](#). Jednou z takových praktik může být návnada v podobě výhry. Znáмым podvodem jsou tzv. Nigerijské dopisy:



**Nigerijské dopisy**

Co tedy můžeme udělat pro svou obranu? Při nákupu postupujeme krok po kroku podle tohoto [desatera, jednoduchého manuálu](#). Pečlivě [vybíráme obchody](#), od kterých si zboží objednáme a sledujeme jejich recenze, tedy zkušenosti zákazníků. V tom nám pomůže například <https://www.heureka.cz/>, kde si můžeme jednotlivé obchody i jejich zboží vzájemně porovnat. Ještě lepším nástrojem je však <https://www.dtest.cz/eshopy>, kde si můžeme ověřit i zabezpečení obchodu, jeho historii, spokojenost zákazníků i vlastníka obchodu.

## TIPY

Máte vnouče nebo mladého člena rodina? Problematikou on-line nakupování můžete procházet společně a dobře se u toho pobavit! Podívat se můžete například na videa, kde vše řeší slavní čeští Youtubeři nebo na díl z „Nauč tetu na netu“ či „Bankovkovi“ od České televize:



**Nakupování on-line s Youtubery**



**Nauč tetu na netu – nakupování**



**Nakupování on-line „Bankovkovi“**

Své znalosti o bezpečném nakupování na internetu a souvisejících tématech si můžete dále rozvíjet [zde](#) a na závěr zopakovat a ověřit [krátkým testem](#).

Zde naleznete [stručnou brožuru](#), která Vám pomůže orientovat se v internetových obchodech, aukcích a vyhodnocovat případná rizika – můžete si ji vytisknout.

# BEZPEČNÉ NAKUPOVÁNÍ NA INTERNETU

## NAKUPOVÁNÍ NA INTERNETU, INTERNETOVÉ PLATBY

Internetové bankovníctví slouží pro správu našich peněz – [24 hodin denně, 7 dní v týdnu](#). Právě proto, že je tato služba založená na správě financí, je důležité důsledně [dodržovat všechna pravidla](#) s ní spojená. Při dodržování těchto pravidel [jsou naše peníze v bezpečí](#) mnohem více, než kdybychom je měli u sebe doma.



Internet banka 1



Internet banka 2

Jednomu z nejčastějších útoků, které se na internetové banky uskutečňují, říkáme Phishing ([odkaz na podrobný popis zde](#)). Útočník připraví stránku, která se tváří jako naše skutečná internetová banka, ale jedná se o podvrh, který má za úkol odcizit přihlašovací údaje. **V zájmu vlastní bezpečnosti bychom se do internetového bankovníctví neměli přihlašovat z veřejných počítačů a přes volně přístupné wi-fi sítě, které nevyžadují heslo.**

Platit na internetu můžeme však i dalšími způsoby, které jsou s internetovým bankovníctvím propojeny – například přímo [platební kartou nebo jinými službami](#). Tyto možnosti představuje další video:



Placení na internetu

## TIPY

Máte vnouče nebo mladého člena rodina? Problematikou on-line nakupování můžete procházet společně a dobře se u toho pobavit! Podívat se můžete například na díl z „Nauč tetu na netu“ či „Bankovkovi“ od České televize:



Nauč tetu na netu – Internet banka

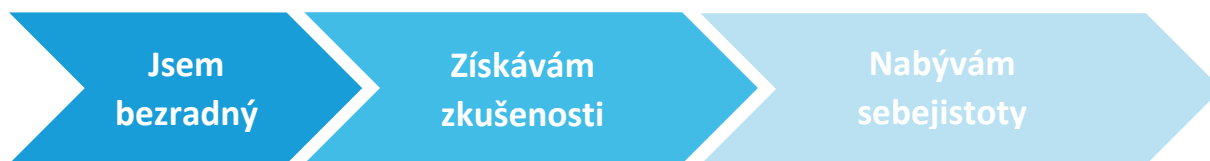


Díl z pořadu „Bankovkovi“ – Účet

Své znalosti o bezpečném internetovém bankovníctví, správě financí on-line a souvisejících tématech si můžete dále rozvíjet [zde](#) a na závěr zopakovat a ověřit krátkým [testem](#).

# ROZCESTNÍK ON-LINE SENIORA

## REKAPITULACE



Právě jste se svou pílí dopracovali až na samotný konec tohoto minikurzu, který Vám ukázal i další možnosti, kde je možné se dále vzdělávat a rozvíjet své znalosti. Věříme, že po průchodu naším rozcestníkem jste získali zkušenosti a nabrali určité sebejistoty, která Vám pohyb na internetu usnadní. Ačkoliv se může zdát, že je internet nebezpečný, nebojte se ho. Buďte však obezřetní. V momentě, kdy se budete chovat dle zásad, kterými jste si prošli, snížíte jeho rizika na minimum a řadě útoků se budete schopni vyhnout. Zkrácenou rekapitulaci toho, co jste se naučili, Vám přinese poslední přiložené video:



Obecné opakování

Stáhnout a vytisknout si můžete [také brožuru](#), která o všem, co v tomto minikurzu zaznělo, pojednává. Věříme, že Vám pomůže si uvědomovat, co vše jste se naučili, a přispěje k Vaší bezpečnosti na internetu v praxi a také vytisknout přiložené plakáty, které jste při cestě rozcestníkem potkávali.