

NÚKIB



Národní úřad
pro kybernetickou
a informační
bezpečnost

PROFIL UČITELE STŘEDNÍ ŠKOLY

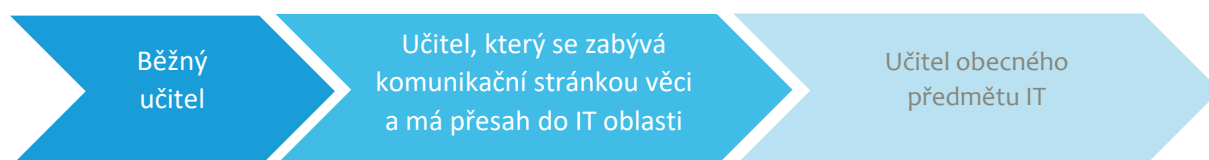
www.nukib.cz

PROFIL UČITELE STŘEDNÍCH ŠKOL

Profil není určen pro správce sítě, ICT koordinátora ani pro IT specialistu. Vycházíme z toho, že běžný učitel má vyšší znalosti práce s PC, než většina populace.

Toto tvrzení můžeme opřít o velmi jednoduché poznatky. Každý učitel musí připravovat věci do výuky a ty se dnes již bez výjimky dodávají v počítačové, často tištěné podobě, včetně ověření na Internetu. Musí tedy ovládat Office a v řadě předmětů ještě specializované aplikace. K tomu řada škol využívá elektronický vzdělávací systém.

Pochopitelně používá stravovací objednávkový systém, intranet školy a mailovou komunikaci. Samozřejmostí je k tomu elektronická klasifikace, je-li třídním učitelem, pak i docházka, a na většině středních škol kompletní elektronická třídní kniha. K tomu si připočtíme práci se školní matrikou nebo knihovním systémem a dostáváme takový objem aplikací, který by řada uživatelů odmítla používat.



BĚŽNÝ UČITEL

Nepotřebuje znát technické podrobnosti nastavení sítě, ani svého počítače. Od toho má správce sítě. Pokud tedy neučí předměty, spojené s IT, vystačí se základními zásadami péče o software, zálohováním a archivací a zásadami tvorby hesel. Velmi pěkné shrnutí je [v tomto článku](#).

Po jeho pročetí je dobré absolvovat například kurz pro učitele na webu [Kraje pro bezpečný Internet](#).

Tvorba hesel je popsána například [tady](#). Další návod najdeme v tomto [článku](#).

UČITEL, KTERÝ SE ZABÝVÁ KOMUNIKAČNÍ STRÁNKOU VĚCI A MÁ PŘESAHA DO IT OBLASTI

Učí tedy všeobecný společenský základ nebo právní nauky, popřípadě jazyky. Musí znát přesah do trestního zákoníku, tedy autorský zákon, postihy za neoprávněné využití výpočetní techniky, zejména dat a další podrobnosti. Současně by měl znát i nástroje sociálního inženýrství a techniky fake news, kterým se nelze vyhnout. Těžiště jeho práce a znalostí tedy bude v oblasti cybercrime, nikoliv v technických podrobnostech. Nesmí se pokoušet jevy, které do oblasti cybercrime patří, řešit. To spadá do kompetence metodika prevence nebo výchovného poradce. Je nutné jevy pouze vysvětlit, zasadit do společenského kontextu a popřípadě zdokumentovat a ohlásit jejich výskyt.

Tady už nevystačíme s kurzem pro běžné učitele. Je dobré znát alespoň základy techniky. Najdeme je na [Khanově akademii](#).

[WikiSofia](#) obsahuje velmi stručnou charakteristiku sociálního inženýrství a celou řadu odkazů na zdroje.

Aby učitel získal odpovídající přehled, doporučujeme projít kurz na [KISK](#).

Vazbu na trestní zákoník lze najít na stránkách Policie.cz, konkrétně na odkazu ke [kybekriminalitě](#).

Protože ale nejde pouze o vazby na zákon, ale o celou kategorii závadového chování, musíme se podívat i na další odkazy. Web [Illinčev](#) obsahuje základy závadové komunikace. Dále se můžeme podívat na stránky [E-bezpečí](#), kde je výzkum ohledně závadového chování na Internetu.

UČITEL OBECNÉHO PŘEDMĚTU IT

Musí znát i technické podrobnosti, a to do takové hloubky, aby dokázal předvídat reakce žáků na různé restrikce a hrozby. Měl by umět vysvětlit jednotlivé typy útoků a to včetně následků a popsat přesně typy závadového chování.

Začít by měl samozřejmě od testu na stránce [Kraje pro bezpečný Internet](#), pokračovat přes kurz [KISKu](#) a dále se pak zaměřit na specifika svého předmětu. Častým jevem je nedostatečná průprava z pohledu technických aspektů bezpečnosti. Lze využít například [Moodle firmy CZ.NIC](#), kde jsou popsány IP adresy včetně systému jejich přidělování a správy. **Pozor ale na to, že pro žáky je text příliš složitý, k přímé výuce na střední škole jej nelze použít bez dalšího výkladu!**

Častým terčem útoku na školách jsou WiFi sítě. Návod na zabezpečení lze najít na následujících stránkách: [Internetem bezpečně](#) a podrobnější je pak například zde: [Jak zabezpečit WiFi](#) ovšem školní WiFi zabezpečuje správce IT, v žádném případě mu učitel nesmí mluvit do kompetencí a nastavení měnit.

Aby učitel šel s dobou a měl přehled, je vhodné sledovat jednak Informační servis NÚKIB, jednak další servery. Je vhodné občas mrknout na [HOAX.cz](#) a kromě toho sledovat i některé další stránky, třeba [s3c](#)

Je nutné mít stále na paměti, že **učitel IT není správce sítě a ani ICT koordinátor**. Na tyto činnosti musí mít uzavřeny další smlouvy a neměl by své povinnosti přenášet do výuky a už vůbec ne na žáky. Obvyklá praxe, že žáci pomáhají s nastavením stanic, je cestou k vytvoření velkých problémů.

Bezpečnost na škole není ale pouze o technice. Je nutné ji vnímat vždy jako celek – od zabezpečení přístupů až po sociální aspekty komunikace. Tady lze pouze doporučit spolupráci s učiteli jiných předmětů. **Metodik IT** by měl být schopen stanovit, kam patří jaká oblast a kdo ji bude učit. V hodinách IT bychom neměli učit autorský zákon, který patří do oblasti jazyka a právní nauky a stejně tak například šifrování ve smyslu rozvoje logiky a využití jednoduchých algoritmů patří spíš pod matematiku nebo obecně pod přírodní vědy. **Učitel IT není psycholog ani preventista a jeho úkolem není řešit závadové chování.** Výuka musí být vedena s upozorněním na možná rizika, s podchycením případných závadových jevů, ale jejich řešení patří do rukou odborníkům.