

Hodina	Téma	Vazby na OVU v RVP	Učivo k dosažení OVU	Možné školní OVU
1.	Co v digitálním světě chráníme?	VO: INF-INF-004-ZV9-013 KK: KOB-ODP-000-ZV9-001	Zařízení, data, účty, finanční hodnoty, soukromí, identita a lidé; vlastní a svěřené hodnoty, význam a priority ochrany.	Rozpozná hodnoty ohrožené v digitálním prostředí, porovná jejich význam pro různé uživatele a podle okolností určí priority jejich ochrany.
2.	Útočníci, hrozby, zranitelnosti a rizika	VO: INF-INF-004-ZV9-013	Vnější a vnitřní útočníci, cíle a následky útoků, hrozba, zranitelnost a riziko, pravděpodobnost a závažnost následků	Rozliší útočníka, hrozbu, zranitelnost, riziko a následek a podle pravděpodobnosti a závažnosti porovná rizika v modelových situacích.
3.	Škodlivý software a jeho druhy	VO: INF-INF-004-ZV9-013	Malware, virus, červ, trojský kůň, ransomware, spyware a adware; způsob fungování, rozmnožování, maskování a dopady	Rozpozná škodlivý software a podle jeho chování a způsobených následků rozliší základní druhy malwaru.
4.	Jak se škodlivý software šíří	VO: INF-INF-004-ZV9-013 KK: KDI-BZK-000-ZV9-001	Přílohy, odkazy, aplikace, média, sdílené soubory, napadené weby a škodlivé reklamy; varovné projevy a první bezpečná reakce	Určí možné cesty šíření malwaru, rozliší přenos nebo stažení od spuštění škodlivého obsahu a zvolí bezpečnou první reakci.
5.	Když útočník využívá člověka	VO: INF-INF-004-ZV9-013 Přesah VO: JJK-CJL-001-ZV9-013 KK: KDI-BZK-000-ZV9-001	Sociální inženýrství, zneužití důvěry a autority, strach, naléhavost, utajení, zvědavost, odměna, FOMO; nezávislé ověření požadavku	Rozpozná sociální inženýrství a použité manipulační prostředky, určí požadované jednání a zvolí nezávislý způsob ověření.
6.	Pozor na phishing	VO: INF-INF-004-ZV9-013 KK: KDI-BZK-000-ZV9-001	Phishing v e-mailu, SMS, chatu, telefonátu, QR kódu a na webu; skutečný odesílatel, adresa, požadované údaje a úkony, nahlášení	Rozpozná phishing v různých komunikačních kanálech, posoudí odesílatele, cíl odkazu a požadovaný úkon a zvolí bezpečné ověření a nahlášení.
7.	Hesla a vícefaktorové ověření	VO: INF-INF-004-ZV9-013 KK: KDI-BZK-000-ZV9-001	Mnemotechnická hesla, číslice a symboly, jedinečnost hesel, prioritní účty, správce hesel, ověřovací faktory, reakce na únik	Vytvoří dlouhé a obtížné odhadnutelné heslo, zdůvodní jedinečnost hesel, rozliší ověřovací faktory a zvolí bezpečný postup při úniku přihlašovacích údajů.
8.	Uživatelské účty, role a oprávnění	VO: INF-INF-004-ZV9-013 KK: KDI-BZK-000-ZV9-001	Typy účtů a jejich role, princip nejmenších oprávnění, oprávnění aplikací, uzamčení, přepnutí účtu a odhlášení	Podle situace zvolí vhodný účet, roli a rozsah oprávnění, posoudí požadavky aplikace a rozhodne mezi uzamčením, přepnutím účtu a odhlášením.
9.	Aktualizace, antivir a další vrstvy ochrany	VO: INF-INF-004-ZV9-013 KK: KDI-BZK-000-ZV9-001	Bezpečnostní aktualizace, antivirová ochrana, firewall, původ aplikace a oficiální zdroje vývojáře, prevence, odhalení, omezení následků, záloha a vícevrstvá ochrana	Vysvětlí význam a omezení aktualizací, antiviru a firewallu, posoudí původ aplikace a pro modelovou situaci sestaví přiměřenou vícevrstvou ochranu.
10.	Bezpečně v prohlížeči a na webu	VO: INF-INF-004-ZV9-013 KK: KDI-BZK-000-ZV9-001	Doména, subdoména, cesta a parametry webové adresy, HTTPS, varování prohlížeče, stahované soubory a oprávnění webů	Orientuje se ve webové adrese, vysvětlí význam a omezení HTTPS a podle původu, účelu a varování posoudí stažení souboru nebo udělení oprávnění webu.
11.	Když dojde k bezpečnostnímu incidentu	VO: INF-INF-004-ZV9-013 KK: KDI-BZK-000-ZV9-001	Bezpečnostní incident, riziko, varovný signál a technická porucha; omezení škody, zaznamenání skutečností, uchování podkladů, nahlášení a bezpečný návrat do provozu	Rozpozná možný bezpečnostní incident, zvolí kroky k omezení škody, uchová potřebné informace, vybere vhodného příjemce hlášení a posoudí podmínky bezpečné obnovy.
12.	Člověk, účet, profil a digitální identita	VO: INF-INF-004-ZV9-013 Přesah VO: CZB-VZB-003-ZV9-010 KK: KDI-BZK-000-ZV9-001	Člověk, účet, profil, avatar a digitální identita; ověřená totožnost, bankovní identita, pseudonymita, anonymita a zneužití identity	Rozliší člověka, účet, profil, avatar a digitální identitu, porovná tvrzenou a ověřenou totožnost a rozpozná pseudonymitu, vydávání se za jinou osobu a zneužití identity.
13.	Digitální stopa, osobní údaje a soukromí	VO: INF-INF-004-ZV9-013 KK: KDI-BZK-000-ZV9-001	Přímá a nepřímá identifikace člověka, kombinace osobních údajů, metadata, aktivní a pasivní digitální stopa, zamýšlené a skutečné publikum, další šíření a nastavení soukromí	Rozpozná osobní údaje a metadata, rozliší aktivní a pasivní digitální stopu, předvídá další šíření obsahu a podle účelu upraví rozsah sdílení a publikum.
14.	Rizikové kontakty a nátlak online	VO: CZB-VZB-003-ZV9-010 VO: CZB-VZB-001-ZV9-004 VO: CZB-VZB-003-ZV9-011	Získávání důvěry, osobní údaje a poloha, soukromý obsah a souhlas, nátlak, vydírání, ukončení kontaktu a pomoc	Rozpozná varovné projevy rizikového kontaktu, odmítne sdílení citlivých údajů a soukromého obsahu a při nátlaku bezpečně ukončí komunikaci a vyhledá pomoc.
15.	Kyberšikana: jak reagovat a kde hledat pomoc	VO: CZB-VZB-003-ZV9-009 VO: CSP-OSV-001-ZV9-002 Přesah VO: CZB-VZB-003-ZV9-010	Kyberšikana, role účastníků, jednání svědka, zastavení útoku, uchování důkazů, blokování, nahlášení a dostupné zdroje pomoci	Rozliší kyberšikana od jiných problematických situací, posoudí jednání účastníků a bezpečnou reakci, uchování podkladů a vhodnou pomoc.

Legenda ke zkratkám

VO = vzdělávací obory
KK = klíčové kompetence
ZG = základní gramotnosti
PT = průřezová témata

Plné znění nejčastějších OVU VO a KK

INF-INF-004-ZV9-013
KDI-BZK-000-ZV9-001
CZB-VZB-003-ZV9-010
CZB-VZB-003-ZV9-009

= Navrhne základní způsoby zabezpečení zařízení a systémů, se kterými pracuje, na základě posouzení rizik ztráty, poškození či zneužití dat.
= Předchází situacím ohrožujícím bezpečnost zařízení a dat nebo jeho tělesné či duševní zdraví.
= Identifikuje nebezpečné aktivity a situace vyskytující se v digitálním prostředí a odůvodní, proč je důležité chránit zde bezpečí své i ostatních, včetně ochrany osobních údajů.
= Zaujímá odmítavý postoj vůči nevhodnému chování a v modelových situacích používá vhodné způsoby, jak se vůči takovému chování vymezit.