#SECFEST 2020

Školení IT bezpečnosti

Jiří Čepák / 3. 12. 2020

Dotazy

Své případné dotazy průběžně pište na https://sli.do/SF20

Motivace a použití

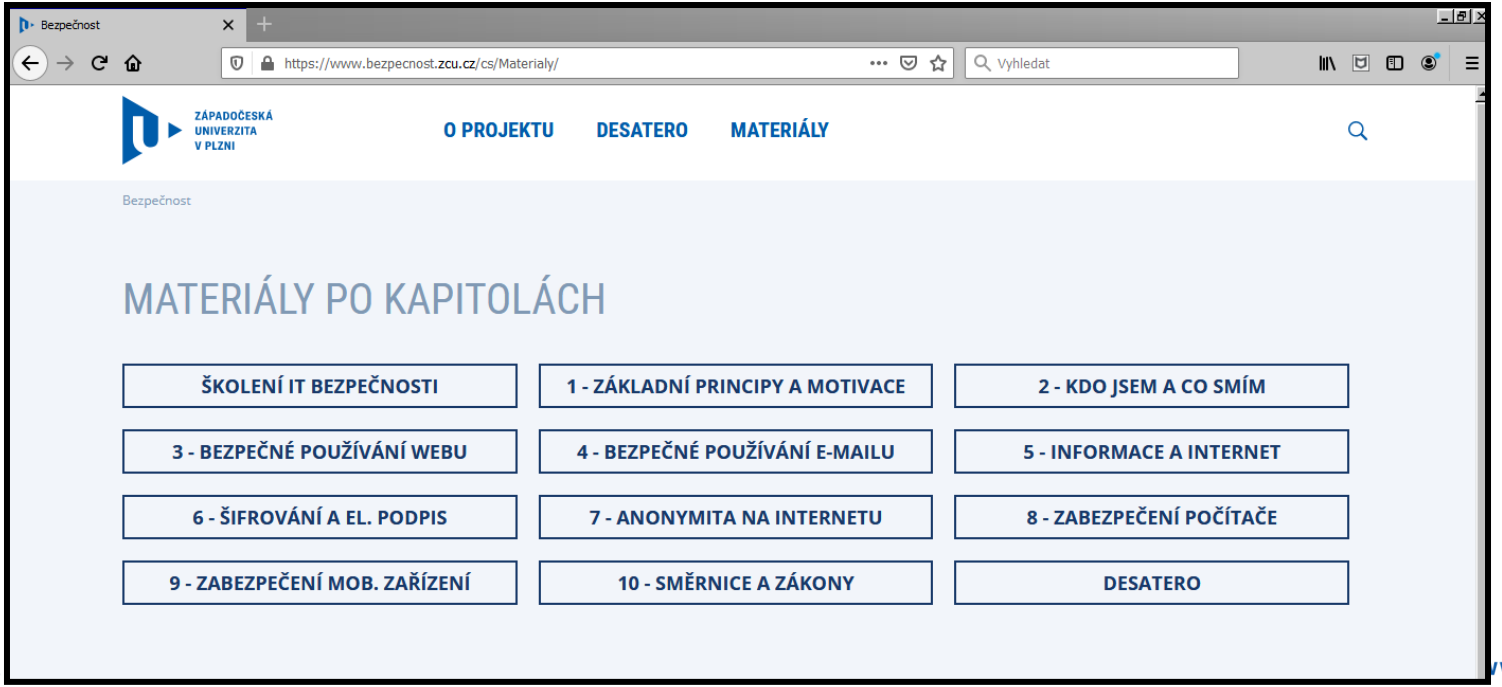
- IT oddělení ZČU nemělo k dispozici materiály, pomocí kterých by periodicky vzdělávalo uživatele v oblasti IT bezpečnosti
- Podobně jako se školí BOZP, PO, řidiči referenti

O co jde?

- Projekt spolufinancovaný Agenturou fondu rozvoje CESNET a Západočeskou univerzitou v Plzni
- Školicí materiály
  - Pro prezenční školení
  - Pro samostudium
  - Pro přípravu lektora školení
- Ucelený soubor 10 témat,
  - Brožura s plným textem
  - Leták s grafikou
  - Prezentace
- Desatero

Kde najdete materiály?

- Web projektu https://bezpecnost.zcu.cz
- Sekce Materiály



1 - ZÁKLADNÍ PRINCIPY A MOTIVACE

Internet je jen dalším prostředím v reálném světě. A stejně jako v reálném světě se v něm pohybují lidé dobří i zlí. A jelikož se ve světě Internetu často přidává předpona kyber, můžeme se u těch zlých setkat s pojmy jako kyberpodvodník nebo kyberkriminálník.

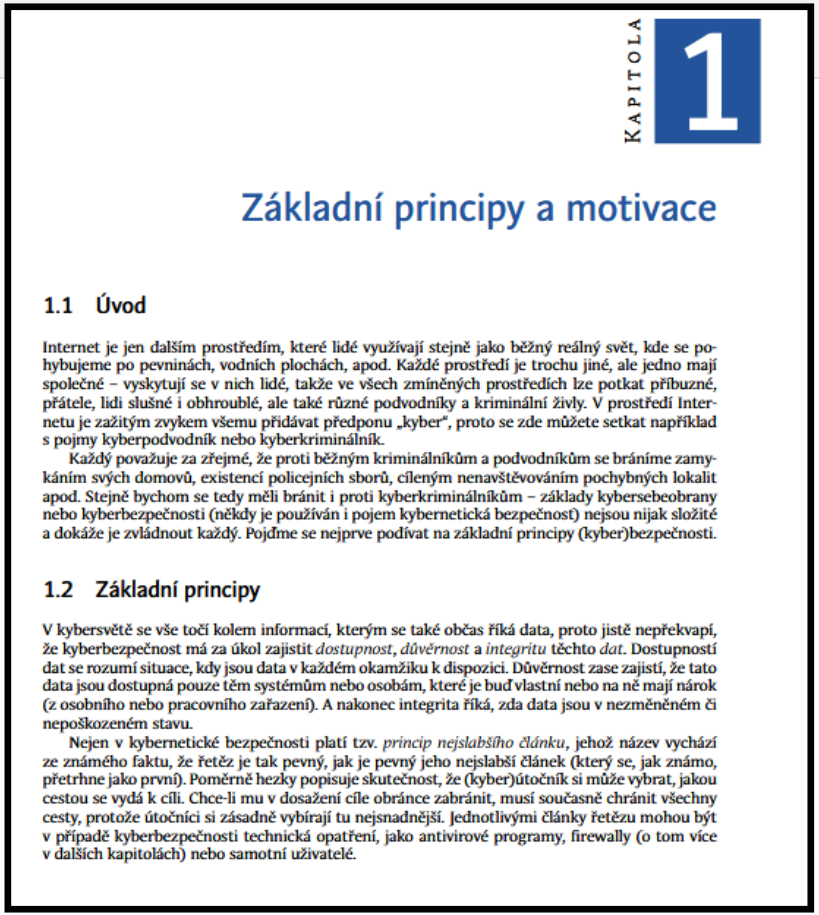
Proti těmto kyberkriminálníkům je nutné se bránit a tato série vzdělávacích materiálů by čtenářovi měla ukázat, že základy kyberbezpečnosti zvládne každý.

KE STAŽENÍ

KAPITOLA 1: BROŽURA PDF 222,66 KB 30. 7. 2020	ZOBRAZIT	STÁHNOUT
KAPITOLA 1: LETÁK PRO MONITOR PDF 1,13 MB 1. 12. 2020	ZOBRAZIT	STÁHNOUT
KAPITOLA 1: LETÁK PRO TISK PDF 1,18 MB 1. 12. 2020	ZOBRAZIT	STÁHNOUT
KAPITOLA 1: PREZENTACE PDF 1,58 MB 29. 7. 2020	ZOBRAZIT	STÁHNOUT

Typy materiálů

- Brožura
  - Elektronická forma pro tisk na A4
  - Kvalitně typograficky vysázený text pro získání všech informací o tématu
- Leták
  - Elektronická forma pro tisk na skládanou 2/3 A4 nebo pro zobrazení na monitoru
  - Obsahuje nejdůležitější informace o tématu obohacené o obrázky a komiksy



KAPITOLA 1

Základní principy a motivace

1.1 Úvod

Internet je jen dalším prostředím, které lidé využívají stejně jako běžný reálný svět, kde se pohybujeme po pevninách, vodních plochách, apod. Každé prostředí je trochu jiné, ale jedno mají společné – vyskytují se v nich lidé, takže ve všech zmíněných prostředích lze potkat příbuzné, přátele, lidi slušné i obhroublé, ale také různé podvodníky a kriminální živly. V prostředí Internetu je zažitým zvykem všemu přidávat předponu „kyber", proto se zde můžete setkat například s pojmy kyberpodvodník nebo kyberkriminálník.

Každý považuje za zřejmé, že proti běžným kriminálníkům a podvodníkům se bráníme zamykáním svých domovů, existencí policejních sborů, cíleným nenavštěvováním pochybných lokalit apod. Stejně bychom se tedy měli bránit i proti kyberkriminálníkům – základy kybersebeobrany nebo kyberbezpečnosti (někdy je používán i pojem kybernetická bezpečnost) nejsou nijak složité a dokáže je zvládnout každý. Pojďme se nejprve podívat na základní principy (kyber)bezpečnosti.

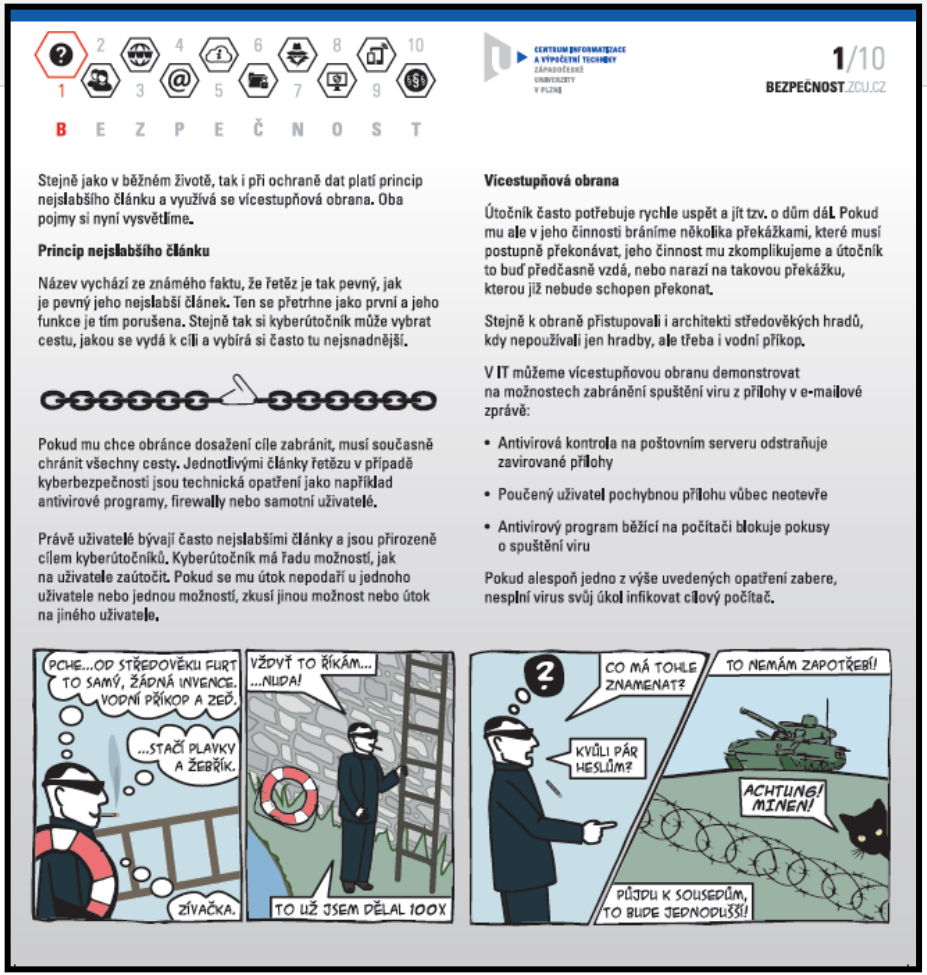
1.2 Základní principy

V kybersvětě se vše točí kolem informací, kterým se také občas říká data, proto jistě nepřekvapí, že kyberbezpečnost má za úkol zajistit *dostupnost*, *důvěrnost* a *integritu* těchto *dat*. Dostupností dat se rozumí situace, kdy jsou data v každém okamžiku k dispozici. Důvěrnost zase zajistí, že tato data jsou dostupná pouze těm systémům nebo osobám, které je buď vlastní nebo na ně mají nárok (z osobního nebo pracovního zařazení). A nakonec integrita říká, zda data jsou v nezměněném či nepoškozeném stavu.

Nejen v kybernetické bezpečnosti platí tzv. *princip nejslabšího článku*, jehož název vychází ze známého faktu, že řetěz je tak pevný, jak je pevný jeho nejslabší článek (který se, jak známo, přetrhne jako první). Poměrně hezky popisuje skutečnost, že (kyber)útočník si může vybrat, jakou cestou se vydá k cíli. Chce-li mu v dosažení cíle obránce zabránit, musí současně chránit všechny cesty, protože útočníci si zásadně vybírají tu nejsnadnější. Jednotlivými články řetězu mohou být v případě kyberbezpečnosti technická opatření, jako antivirové programy, firewally (o tom více v dalších kapitolách) nebo samotní uživatelé.

Typy materiálů

- Brožura
  - Elektronická forma pro tisk na A4
  - Kvalitně typograficky vysázený text pro získání všech informací o tématu
- Leták
  - Elektronická forma pro tisk na skládanou 2/3 A4 nebo pro zobrazení na monitoru
  - Obsahuje nejdůležitější informace o tématu obohacené o obrázky a komiksy



1 2 3 4 5 6 7 8 9 10

B E Z P E Č N O S T

CENTRUM INFORMATIZACE A VÝPOČETNÍ TECHNIKY ZÁPADOČESKÉ UNIVERZITY V PLZNI

1/10

BEZPEČNOST.ZCU.CZ

Stejně jako v běžném životě, tak i při ochraně dat platí princip nejslabšího článku a využívá se vícestupňová obrana. Oba pojmy si nyní vysvětlíme.

Princip nejslabšího článku

Název vychází ze známého faktu, že řetěz je tak pevný, jak je pevný jeho nejslabší článek. Ten se přetrhne jako první a jeho funkce je tím porušena. Stejně tak si kyberútočník může vybrat cestu, jakou se vydá k cíli a vybírá si často tu nejsnadnější.

Pokud mu chce obránce dosažení cíle zabránit, musí současně chránit všechny cesty. Jednotlivými články řetězu v případě kyberbezpečnosti jsou technická opatření jako například antivirové programy, firewally nebo samotní uživatelé.

Právě uživatelé bývají často nejslabšími články a jsou přirozeně cílem kyberútočníků. Kyberútočník má řadu možností, jak na uživatele zaútočit. Pokud se mu útok nepodaří u jednoho uživatele nebo jednou možností, zkusí jinou možnost nebo útok na jiného uživatele.

Vícestupňová obrana

Útočník často potřebuje rychle uspět a jít tzv. o dům dál. Pokud mu ale v jeho činnosti bráníme několika překážkami, které musí postupně překonávat, jeho činnost mu zkomplikujeme a útočník to buď předčasně vzdá, nebo narazí na takovou překážku, kterou již nebude schopen překonat.

Stejně k obraně přistupovali i architekti středověkých hradů, kdy nepoužívali jen hradby, ale třeba i vodní příkop.

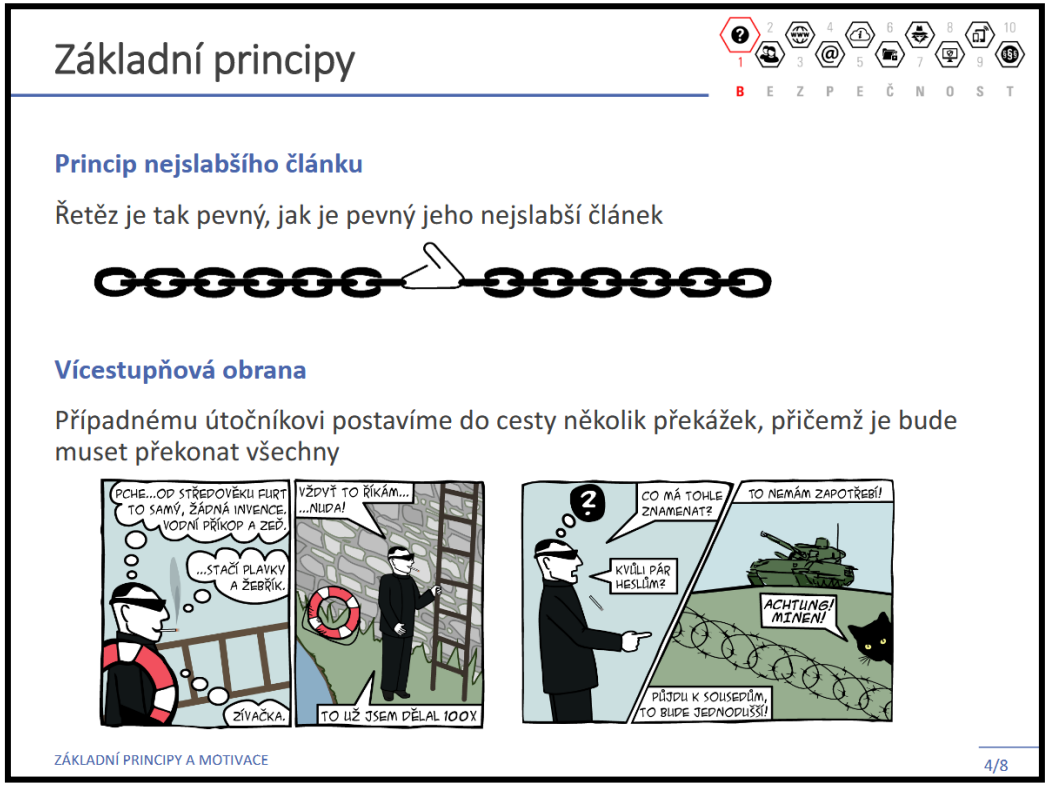
V IT můžeme vícestupňovou obranu demonstrovat na možnostech zabránění spuštění viru z přílohy v e-mailové zprávě:

- Antivirová kontrola na poštovním serveru odstraňuje zavirované přílohy
- Poučený uživatel pochybnou přílohu vůbec neotevře
- Antivirový program běžící na počítači blokuje pokusy o spuštění viru

Pokud alespoň jedno z výše uvedených opatření zabere, nesplní virus svůj úkol infikovat cílový počítač.

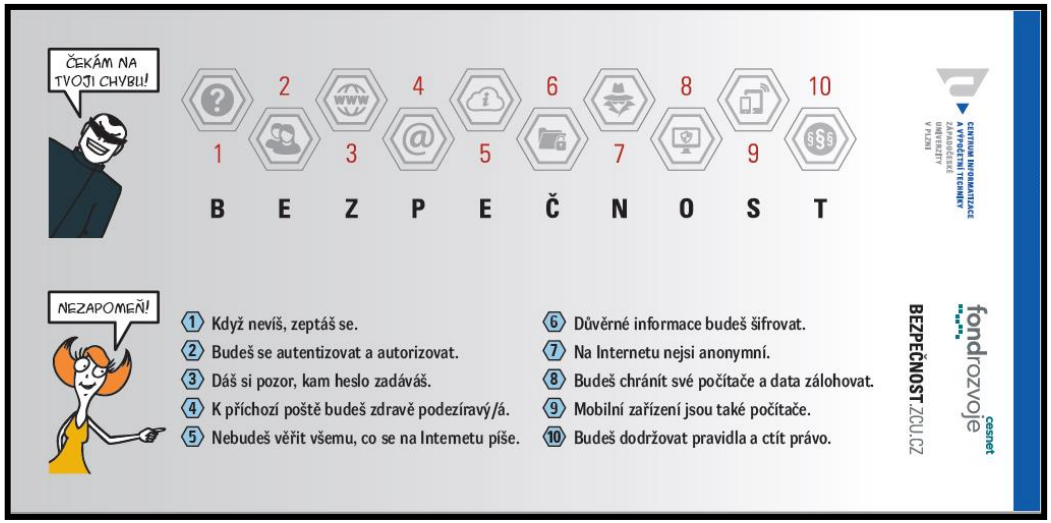
Typy materiálů

- Prezentace
  - Elektronické v pdf formátu
  - Připravené snímky pro prezentaci v rámci prezenčního školení
- Záložka a samolepky
  - Účastníci školení si odnesou záložku a z každého školení samolepku, kterou si do záložky nalepí



Typy materiálů

- Prezentace
  - Elektronické v pdf formátu
  - Připravené snímky pro prezentaci v rámci prezenčního školení
- Záložka a samolepky
  - Účastníci školení si odnesou záložku a z každého školení samolepku, kterou si do záložky nalepí



Kapitola 1 – Základní principy a motivace

- Úvodní kapitola
- Pojmy z kyberbezpečnosti
  - Dostupnost
  - Důvěrnost
  - Integrita
- Základní principy
  - Princip nejslabšího článku
  - Princip vícestupňové obrany
- Cena za bezpečnost
- Prevence
- Řešení problémů

Kapitola 2 – Kdo jsem a co smím

- Kdo jsem = autentizace
  - Prokázání vlastnictví elektronické identity
- Problematika hesel
  - Co musí splňovat kvalitní heslo
    - Dlouhé
    - Jedinečné
    - Složité
    - Pravidelně měněné
  - Jakým typům útoku musí odolat
- Co smím = autorizace
  - Oprávnění k provádění akcí například v informačním systému

Kapitola 3 – Bezpečné používání webu

- Co je to web
- Co je to webová adresa
  - Z jakých částí se skládá
  - Důležitost doménového jména
  - Zkracovače URL
  - Protokoly HTTP vs. HTTPS
- Webové certifikáty

Kapitola 4 – Bezpečné používání e-mailu

- Jak funguje elektronická pošta
- Jak ji správně používat
- Jak je to s odesílatelem zprávy
- E-mail a jeho digitální stopa
- Přílohy e-mailů
- Jak na hromadnou korespondenci
- Co je to…
  - spam
  - phishing
  - hoax

Kapitola 5 – Informace a Internet

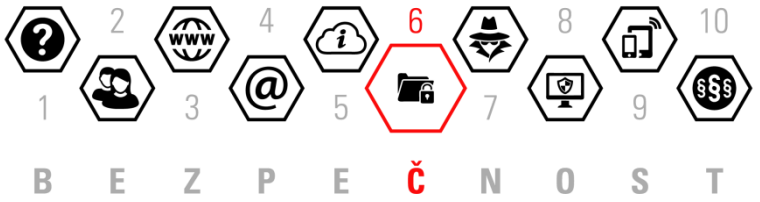
- Věrohodnost získávaných informací
- Klasifikace informací - Důvěrnost
  - Veřejné
  - Interní
  - Chráněné
- Dostupnost informace
  - Dostanu se k informaci když ji potřebuji?
- Změna informace - Integrita
- Poskytování informace
  - Informace jednou na Internet vypuštěná již nikdy nelze vzít zpět

Dotazy

Své případné dotazy průběžně pište na https://sli.do/SF20

Kapitola 6 – Šifrování a elektronický podpis

- Proč některé informace šifrujeme nebo potřebujeme šifrovat?
- Co je šifrování
- Princip symetrického a asymetrického šifrování
- Proč elektronicky podepisujeme?
  - Zajištění autenticity
  - Zajištění integrity
  - Nepopiratelnost
  - Časové ukotvení



Kapitola 7 – Anonymita na Internetu

- Anonymita je schopnost být odlišitelný od ostatních
- Na Internetu nejsme anonymní a postupně se snižuje
- Ke komunikaci na Internetu potřebujeme IP adresu
- Záznamy o používání internetových služeb
- Otisky prohlížečů
- Zveřejňování informací

Kapitola 8 – Zabezpečení počítače

- Počítač je třeba chránit z hlediska
  - fyzického přístupu
  - Přístupu po síti
- Pravidelné aktualizace
  - Operačního systému
  - Všech dalších aplikací
- Aplikace pro zabezpečení zařízení
  - Antivirový program
  - Firewall
  - WebControl
- Oddělení admin a user účtů

Kapitola 9 – Zabezpečení mobilních zařízení

- Co je mobilní zařízení
- Má svůj operační systém a další aplikace
- Přístup k zařízení musí být chráněn
  - PIN
  - Gesto
  - Otisk prstu
  - Rozpoznání obličeje
- Ochrana dat v telefonu
- Zeměpisná poloha
- Dvoufázová autentizace na mobilním zařízení

Kapitola 10 – Směrnice a zákony

- Do kybersvěta se přenáší zákony z reálného světa
- Princip teritoriality
- Autorský zákon
- Zákon o ochraně osobních údajů
- Zákon o kybernetické bezpečnosti
- Interní pravidla organizací
- Pravidla použití služby
- Odkaz na další informace

Bonus – Desatero

- Když nevíš, zeptáš se.
- Budeš se autentizovat a autorizovat.
- Dáš si pozor, kam heslo zadáváš.
- K příchozí poště budeš zdravě podezíravý/á.
- Nebudeš věřit všemu, co se na Internetu píše.
- Důvěrné informace budeš šifrovat.
- Na Internetu nejsi anonymní.
- Budeš chránit své počítače a data zálohovat.
- Mobilní zařízení jsou také počítače.
- Budeš dodržovat pravidla a ctít právo.

ZÁPADOČESKÁ
UNIVERZITA
V PLZNI

Děkuji za pozornost

Jiří Čepák / cepakj@civ.zcu.cz