Digitální hygiena odpovědného občana ČR

Červenec 2025

DIGITERRA INSTITUTE

Účel příručky

Cílem této příručky je zvýšit povědomí občanů o digitálních rizicích, naučit je chránit sebe, své blízké i osobní údaje při každodenním používání digitálních technologií, a zároveň přispět k celkovému zvyšování kybernetické bezpečnosti České republiky.

Obsah

1. Úvod: Co je digitální hygiena?

- Definice a důležitost
- Paralela s fyzickou hygienou
- Proč se to týká každého (od žáků po seniory)

🔷 Co znamená pojem „digitální hygiena“?

Digitální hygiena označuje soubor návyků, pravidel a chování, které nám pomáhají bezpečně, zodpovědně a zdravě používat digitální technologie – počítače, mobilní zařízení, internet a online služby. Podobně jako fyzická hygiena chrání naše tělo před nemocemi, **digitální hygiena chrání naše osobní údaje, duševní zdraví, finance i reputaci** před riziky digitálního světa.

🔷 Proč je digitální hygiena důležitá?

- **Kybernetické hrozby jsou všude.** Útoky typu phishing, malware nebo podvodné zprávy cílí nejen na firmy, ale i na běžné občany – děti, rodiče, seniory.
- **Povědomí veřejnosti je často nízké.** Mnoho lidí se stále spoléhá jen na antivir a slabá hesla. Přitom největším rizikem bývá lidská chyba.
- **Důsledky bývají vážné.** Krádeže identit, zneužití osobních údajů, finanční ztráty, narušení soukromí, nebo i psychické problémy.

Digitální hygiena **neznamená být odborníkem na IT** – jde o to osvojit si pár jednoduchých zásad a návyků, které významně snižují riziko a zvyšují komfort a bezpečí v online prostředí.

🔷 Digitální hygiena je pro každého

Digitální hygiena není jen pro “ajťáky”. Týká se **každého občana**, který:

- používá internetové bankovnictví,
- komunikuje přes e-mail, sociální sítě nebo chatovací aplikace,
- sdílí data, fotky nebo pracovní informace online,
- čte zprávy a informace z internetu,
- nakupuje v e-shopech nebo se přihlašuje do online služeb.

Ať je vám 13 nebo 73, používáte-li mobil, tablet nebo počítač, **digitální hygiena by měla být stejně běžná jako čistění zubů**.

🔷 Digitální hygiena = bezpečnost + zdraví + ohleduplnost

Digitální hygiena má **tři základní pilíře**:

1. **Bezpečnostní hygiena**

   – ochrana zařízení, dat, hesel a identity (např. silná hesla, aktualizace, zabezpečené připojení)

2. **Mentální hygiena**

   – vyvážené a zdravé používání technologií (např. digitální rovnováha, omezení závislosti na mobilu)

3. **Etická hygiena**

   – odpovědné a slušné chování online (např. nešíření dezinformací, respekt k soukromí ostatních)

🔷 Praktické příklady digitální hygieny

Špatná praxe	**Dobrá praxe – digitální hygiena**
Používám stejné heslo všude	Mám správce hesel a každé heslo jiné
Klikám na odkazy v neznámých mailech	E-mail prověřím a odkazy neotevírám bez ověření
Sdílím svou polohu a fotky v reálném čase	Sdílím zážitky až po návratu domů
Spím s mobilem u hlavy	V noci mám telefon v tichém režimu mimo ložnici

🔷 Cíl příručky

Tato příručka vám krok za krokem ukáže, **jak si vytvořit bezpečné, zdravé a zodpovědné digitální návyky**, které ochrání nejen vás, ale i vaše okolí – rodinu, kolegy, komunitu.

Digitální hygiena je investice do vlastní bezpečnosti a pohody v digitálním světě.

2. ZÁKLADY BEZPEČNÉHO CHOVÁNÍ V DIGITÁLNÍM PROSTŘEDÍ

- Silná hesla a jejich správa
- Dvoufázové ověření (2FA)
- Rozpoznání podezřelých e-mailů a podvodů (phishing)
- Bezpečné chování na sociálních sítích
- Zásady stahování a instalace aplikací
- Vypínání automatického připojování k Wi-Fi
- Pravidelné aktualizace systému a aplikací

🔐 2.1 Silná hesla a jejich správa

Proč na heslech záleží:

- Hesla chrání přístup k vašim osobním údajům, penězům i soukromí.
- Útočníci často používají automatické nástroje, které zkoušejí běžná a slabá hesla.

Jak na silné heslo:

- Minimálně 12 znaků, ideálně více.
- Kombinace velkých a malých písmen, čísel a speciálních znaků.
- Vyhněte se jménům, datům narození, názvům domácích mazlíčků atp.

Jak hesla bezpečně spravovat:

- **Nikdy nepoužívejte jedno heslo pro více služeb.**
- Používejte **správce hesel** (např. Bitwarden, 1Password, KeePass).
- Hesla si **nepište na papír** ležící u počítače.

🛡️ **Tip:** Místo hesla používejte větu – např. „**MilujiKafeRano@6!**“

🔑 2.2 Dvoufázové ověření (2FA)

Co to je:

Dvoufázové ověření znamená, že kromě hesla potřebujete při přihlášení ještě druhý faktor – např. kód z mobilní aplikace nebo potvrzení přes SMS.

Proč je to důležité:

I když útočník získá vaše heslo, bez druhého faktoru se do účtu nedostane.

Kde ho zapnout:

- E-maily (Gmail, Seznam, Outlook)
- Sociální sítě (Facebook, Instagram)
- Bankovnictví, úložiště, správci hesel

Tip: Nejbezpečnější jsou aplikace jako **Google Authenticator** nebo **Authy** – místo SMS, které se dají snadněji napadnout.

2.3 Rozpoznání podezřelých e-mailů a podvodů (phishing)

Co je phishing:

Podvodné e-maily, které vás lákají ke kliknutí na falešný odkaz nebo zadání údajů (např. „vaše banka“, „pošta“, „Microsoft“).

Jak ho poznat:

- Naléhavý tón („okamžitě zadejte údaje“)
- Chyby v gramatice, podivná adresa odesílatele
- Přílohy nebo odkazy, které nečekáte

Tip: Na podezřelé e-maily **neklikejte**. Ověřte si je u dané instituce jinou cestou.

2.4 Bezpečné chování na sociálních sítích

Proč být opatrný:

- Sociální sítě zrcadlí váš život – co sdílíte, může být zneužito (např. pro krádež identity, cílení útoků nebo dokonce fyzickou krádež při dovolené).

Co nedělat:

- Nesdílejte svou přesnou polohu v reálném čase.
- Nezveřejňujte dokumenty, letenky, vstupenky s QR kódy.
- Nezveřejňujte osobní data – rodné číslo, adresu, e-mail, číslo účtu.

Tip: Zkontrolujte si nastavení soukromí – například seznam lidí, kteří vidí vaše příspěvky.

2.5 Zásady stahování a instalace aplikací

Rizika:

- Infikované aplikace mohou špehovat, krást data nebo zařízení uzamknout.
- Falešné aplikace často napodobují originály.

Jak postupovat:

- **Stahujte jen z oficiálních obchodů** (Google Play, App Store).
- Před instalací zkontrolujte recenze a oprávnění aplikace.
- **Nepovolujte zbytečný přístup** (např. ke kameře, kontaktům, poloze).

Tip: Pravidelně odinstalujte aplikace, které nepoužíváte.

2.6 Vypínání automatického připojování k Wi-Fi

Riziko:

Zařízení se může připojit automaticky k síti se známým názvem, i když ji vytvořil útočník (např. „Starbucks_WiFi“).

Řešení:

- Vypněte automatické připojení v nastavení Wi-Fi.
- Před připojením k neznámé síti si ověřte, zda je skutečně důvěryhodná.

Tip: Pokud musíte používat veřejnou síť, **vždy používejte VPN**.

2.7 Pravidelné aktualizace systému a aplikací

Proč:

Aktualizace opravují chyby a zabezpečují systém proti novým typům útoků.

Co aktualizovat:

- Operační systém (Windows, Android, iOS, macOS)
- Webové prohlížeče
- Antivirové programy a bezpečnostní aplikace
- Všechny aplikace, které pravidelně používáte

Tip: Zapněte si automatické aktualizace, pokud je to možné.

3. OCHRANA SOUKROMÍ A OSOBNÍCH ÚDAJŮ

- Základní principy GDPR pro běžného uživatele
- Co o vás ví internet?
- Jak omezit stopu: nastavení soukromí, cookies, sledování
- Falešné soutěže, ankety, testy osobnosti – proč bývají nebezpečné

V digitálním prostředí dnes sdílíme více informací než kdy dřív – často nevědomky. Zároveň se zvyšuje riziko, že s těmito daty bude někdo neoprávněně nakládat, prodávat je nebo je zneužije k manipulaci či podvodu. Tato kapitola vám pomůže **pochopit rizika**, **rozpoznat nevhodné praktiky** a **nastavit digitální prostředí tak, aby chránilo vás, ne vás sledovalo**.

3.1 Základní principy GDPR pro běžného uživatele

GDPR (Obecné nařízení o ochraně osobních údajů) chrání práva každého občana EU při zpracování jeho osobních údajů.

Co je „osobní údaj“:

- Jméno, příjmení, adresa, rodné číslo
- IP adresa, e-mail, cookies, poloha
- Fotka, hlas, biometrické údaje

Vaše práva podle GDPR:

- **Právo vědět**, jaká data o vás někdo zpracovává
- **Právo požádat o výmaz** („být zapomenut“)
- **Právo na opravu a přenositelnost** údajů
- **Právo nesouhlasit** se zpracováním pro marketing
- **Právo podat stížnost** u Úřadu pro ochranu osobních údajů (www.uoou.cz)

Tip: Vždy si ověřte, komu údaje dáváte – a proč.

3.2 Co o vás ví internet?

Příklady informací, které o vás může internet sbírat:

- Historie vyhledávání a navštívených stránek
- Zájmy (např. ze sledování zboží)
- Lokace, zařízení, operační systém
- Chování na sociálních sítích (komentáře, lajky, přátelé)

Kdo tyto data sbírá:

- Weby, které navštěvujete (cookies, analytika)
- Sociální sítě (Facebook, Instagram, TikTok)
- Mobilní aplikace (výměnou za „bezplatnost“)
- Reklamní sítě a data brokery

Tip: Používejte anonymní režim prohlížeče, blokátory reklam a sledujte nastavení soukromí.

🔧 3.3 Jak omezit digitální stopu: nastavení soukromí, cookies, sledování

Co můžete udělat:

✅ V nastavení prohlížeče:

- Vymazat historii a cookies
- Nastavit „Nesledovat“ („Do Not Track“)
- Zablokovat sledovací skripty (rozšíření jako **uBlock Origin**, **Privacy Badger**, **Ghostery**)

✅ Na sociálních sítích:

- Omezit viditelnost profilu a příspěvků (např. jen pro přátele)
- Vypnout personalizaci reklam
- Zkontrolovat oprávnění aplikací, které mají přístup k vašemu účtu

✅ Na webových stránkách:

- Při výběru cookies klikněte na „Odmítnout vše“ nebo „Nastavit“ – ne „Přijmout vše“
- Vyhýbejte se stránkám, které bez souhlasu cookies nasazují

🛡️ **Tip:** Jednou za čas projděte, kterým aplikacím a stránkám jste udělili přístup k datům – a zrušte přístupy, které nepotřebujete.

🎯 3.4 Falešné soutěže, ankety, testy osobnosti – proč bývají nebezpečné

Typické scénáře:

- „Vyhraj nový iPhone!“ – za vyplnění krátkého formuláře
- „Zjistěte, jaký jste typ osobnosti“ – přes Facebook
- „Odpověz na 3 otázky a vyhraj!“ – s nutností zadat e-mail, telefon, adresu

Rizika:

- Vaše údaje mohou být:
  - prodány třetím stranám,
  - použity k cíleným podvodům (spear phishing),
  - zneužity pro spam nebo falešné nabídky.
- Některé formuláře slouží jako **návnada pro sběr dat** a **ověření funkčních kontaktů**.

🛡️ **Tip:** Soutěže a kvízy najdete i u seriózních firem – ale **vždy si ověřte, kdo je organizátor**, jak se s daty nakládá a jestli má reálné obchodní zázemí.

📌 Shrnutí kapitoly:

- Chraňte svá data jako by šlo o vaši občanku – **na internetu má každé kliknutí svou cenu.**
- **Ověřujte, zvažujte a nastavujte** – vaše soukromí závisí hlavně na vašich volbách.
- Naučte se poznat, **kdy vám něco nabízí hodnotu – a kdy si bere hodnotu z vás.**

4. DIGITÁLNÍ HYGIENA V RODINĚ

- Pravidla pro děti (věkově přizpůsobená)
- Digitální gramotnost dospívajících
- Jak mluvit s dětmi o rizicích internetu
- Doporučení pro rodiče: rodičovské zámky, bezpečný režim, dohled
- Senioři online – jednoduchá pravidla pro ochranu před podvodníky

Rodina je základní jednotkou společnosti – a v digitálním věku i základem bezpečného chování online. Děti se učí napodobováním, teenageři často testují hranice a senioři se s technologiemi učí „za pochodu“. Právě doma proto vznikají základy digitálních návyků, které přetrvávají celý život.

👶 4.1 Pravidla pro děti (věkově přizpůsobená)

Pro děti do 6 let:

- Používat zařízení pouze s rodičem.
- Čas u obrazovky max. 30–60 minut denně.
- Jen aplikace určené pro daný věk (např. YouTube Kids, edukativní hry).

Pro děti 6–12 let:

- Stanovit časový limit a pravidla (např. 2 hodiny denně, žádná zařízení v ložnici).
- Nepoužívat sociální sítě bez dozoru.
- Učit děti rozeznávat reklamu a podvodné nabídky.

Společná pravidla:

- Rodinná dohoda o používání zařízení (např. pravidla chování online, časy bez mobilu).
- Žádná zařízení u stolu nebo před spaním.
- Děti musí vědět, že se na rodiče mohou obrátit, když se setkají s něčím podivným.

🚦 **Tip:** Ptejte se dětí, co sledují a co je baví. Zájem a důvěra je základ prevence.

🧠 4.2 Digitální gramotnost dospívajících

Teenageři jsou pokročilí uživatelé technologií, ale to neznamená, že jsou imunní vůči rizikům.

Co je potřeba rozvíjet:

- **Kritické myšlení** (rozeznání fake news, manipulace, hoaxů).
- **Kyberetika** (respekt, souhlas, zodpovědnost za obsah).
- **Správa digitální identity** (co sdílejí, jaké aplikace používají, kyberšikana).
- **Bezpečnost účtů** (hesla, 2FA, soukromí na sítích).

🚦 **Tip:** Diskutujte s nimi. Nezakazujte, ale vysvětlujte a naslouchejte.

🗣️ 4.3 Jak mluvit s dětmi o rizicích internetu

Důležité zásady:

- Mluvte otevřeně, bez strašení, ale pravdivě.
- Zajímejte se o to, **co děti online dělají**, nejen kolik času tam tráví.
- Učte je říkat „NE“ – i v online světě.
- Vysvětlujte, **co je soukromé a co ne**, a že sdílení může být nevratné.

Příklady témat pro rozhovor:

- „Co bys dělal, kdyby ti někdo neznámý napsal?“
- „Co by tě přimělo sdílet heslo?“
- „Znáš někoho, komu se stalo něco nepříjemného online?“

🚦 **Tip:** Používejte konkrétní situace (např. zpráva od neznámého člověka) a společně hledejte řešení.

🛠️ 4.4 Doporučení pro rodiče: rodičovské zámky, bezpečný režim, dohled

Technické nástroje:

- **Rodičovské zámky a správa času** (např. Google Family Link, Apple Screentime, Qustodio).
- **Bezpečný režim vyhledávání** na YouTube, Google apod.
- **Filtrování obsahu** (blokace nevhodných stránek, limit na aplikace).

Praktická opatření:

- Pravidelná kontrola historie a nastavení zařízení.
- Vysvětlení důvodů technických omezení – není to o kontrole, ale o ochraně.
- Vytváření důvěry: děti by neměly tajit, když se něco děje.

🚦 **Tip:** Nejlepší dohled je zájem. Technika je jen podpora, ne náhrada vztahu.

👴 4.5 Senioři online – jednoduchá pravidla pro ochranu před podvodníky

Senioři jsou stále častějším cílem podvodníků. Věřivost, méně zkušeností a často i osamělost hrají roli.

Hlavní hrozby:

- Falešné SMS nebo e-maily (pošta, banka, vnuk v nouzi)
- Telefonické podvody (např. falešní operátoři nebo policisté)
- Podvodné e-shopy, investiční „nabídky“

Doporučení:

- Nikdy **neklikat na odkazy v e-mailech nebo SMS od neznámých osob**.
- **Neposkytovat údaje po telefonu**, a už vůbec ne přihlašovací údaje nebo kódy.
- **Nakupovat jen z důvěryhodných e-shopů** – ideálně známých.
- Instalace **antiviru a aktualizace zařízení**.

🛡️ **Tip:** Vysvětlujte starším lidem, že **nemusí odpovídat na každou zprávu ani být neustále „online“.** Pomozte jim nastavit bezpečné prostředí a buďte jim oporou.

📌 Shrnutí kapitoly:

- Digitální hygiena začíná doma – **děti, rodiče i prarodiče jsou spojení jedním digitálním prostředím.**
- Nastavení techniky je důležité, ale **zásadní je dialog, důvěra a společné hranice.**
- Každý člen rodiny potřebuje jiný přístup, ale cíl je společný: **bezpečnější, zdravější a odpovědnější digitální svět pro všechny generace.**

5. FINANČNÍ BEZPEČNOST

- Jak poznat falešné e-shopy
- Bezpečné platby kartou online
- Investiční a loterijní podvody
- Podvodné SMS a telefonáty („vishing“, „smishing“)

V digitálním světě jsou vaše peníze ohroženy nejen na účtu, ale i v e-mailech, SMS zprávách nebo reklamách na sociálních sítích. Tato kapitola vás naučí, jak rozeznat podvod od reality, chránit svou platební kartu a nenaletět na moderní formy finanční kriminality.

🛒 5.1 Jak poznat falešné e-shopy

Typické znaky podvodných e-shopů:

- Podezřele nízké ceny (např. nový mobil za třetinu ceny)
- Chybějící nebo neúplné kontaktní údaje
- Doména podezřelé kvality (např. .shop, .store, překlepy v názvu)
- Web bez zabezpečeného připojení (chybí „https“)
- Požadavek na platbu **pouze předem** (bez dobírky)
- Chybí obchodní podmínky nebo odkaz na reklamační řád

Co zkontrolovat:

- Existenci firmy (např. na www.justice.cz nebo www.ares.cz)
- Recenze mimo daný web (např. Heureka, Zbozi.cz, Google)
- Jak dlouho doména existuje (např. pomocí doménového nástroje)

🚦 **Tip:** Pokud si nejste jisti, nenakupujte. Nevěřte příliš výhodným nabídkám a podezřelým slevám.

💳 5.2 Bezpečné platby kartou online

Základní zásady:

- Nikdy **nezadávejte kartu do neznámého nebo podezřelého formuláře**.
- Používejte pouze **ověřené platební brány** (např. GoPay, ComGate, PayPal).
- Sledujte, zda je adresa stránky zabezpečena (https://) a má důvěryhodnou doménu.
- Aktivujte si **notifikace o platbách**, ideálně i **limity pro internetové platby**.

Moderní ochrana:

- Většina bank dnes využívá **3D Secure** – potvrzení platby pomocí SMS, biometrie nebo mobilní aplikace.
- Pokud je možné, používejte **virtuální kartu** pro jednorázové platby.

🚦 **Tip:** Nikdy neposílejte **kopii karty, přední i zadní stranu ani CVC kód** přes e-mail, chat ani WhatsApp.

🎰 5.3 Investiční a loterijní podvody

Jak vypadají:

- „Zaručená investice s výnosem 200 % za měsíc“
- „Slavná osobnost doporučuje investici do kryptoměny“ (často falešné)
- Falešné aplikace na „obchodování“ – po vložení peněz se ztratí kontakt
- Loterie, které jste **nikdy nehráli**, ale „vyhráli jste“

Co si pamatovat:

- **Nikdo vám nedá peníze jen tak.**
- Investice vždy nese riziko. Pokud někdo tvrdí opak – je to lež.
- Pokud něco zní **až moc dobře**, je to **určitě podvod**.

🚦 **Tip:** Investujte jen přes licencované firmy – ověřte si je na webu České národní banky (www.cnb.cz).

📱 5.4 Podvodné SMS a telefonáty („vishing“, „smishing“)

Co je „vishing“:

Telefonát, který se **tváří jako z banky, pošty, policie nebo operátora**, ale ve skutečnosti se vás snaží přimět, abyste někam poslali peníze nebo sdělili citlivé údaje.

Co je „smishing“:

Podvodná **SMS zpráva**, často obsahující odkaz – např. z falešné pošty, přepravní služby nebo banky.

Příklady podvodných tvrzení:

- „Došlo k podezřelé aktivitě na vašem účtu, klikněte zde.“
- „Máte nedoplatek na doručení zásilky.“
- „Vaše banka potřebuje ověřit vaši identitu.“

Jak reagovat:

- **Nikdy neklikejte na odkazy v podezřelých SMS**.
- **Nikomu do telefonu nesdělujte hesla, kódy ani čísla karty** – banka to po vás nikdy chtít nebude.
- Vždy si kontakt ověřte z oficiálního webu nebo aplikace.

🚦 **Tip:** Podvodníci dnes dokáží zfalšovat i číslo, z něhož volají nebo píší – buďte vždy ve střehu.

📌 Shrnutí kapitoly:

- **Podvodníci neustále mění formu, ale principy zůstávají stejné**: vzbudit důvěru, spěch, paniku – a připravit vás o peníze.
- Finanční bezpečnost začíná u **pozornosti a ověřování**. Pokud si nejste jistí, vždy **raději ověřte u důvěryhodného zdroje** – než přijdete o peníze.

- **Buďte obezřetní, ale ne paranoidní** – zdravá digitální hygiena vám umožní využívat výhody online světa bezpečně.

6. Kyberšikana, manipulace, dezinformace

- Co je kyberšikana a jak ji řešit
- Jak poznat manipulativní obsah
- Jak ověřit informace (fact-checking, důvěryhodné zdroje)
- Kde nahlásit závadný obsah (např. CZ.NIC, Policie ČR)

Digitální prostor není jen technický – je především **sociální**. V online světě jsme vystaveni nejen virům a hackerům, ale také **tlaku, nátlaku, lžím a útokům** od jiných lidí nebo automatizovaných systémů. Tato kapitola vás naučí rozpoznat, jaké chování je nepřijatelné, jak se bránit a kde hledat pomoc.

🧨 6.1 Co je kyberšikana a jak ji řešit

Co je kyberšikana:

Záměrné a opakované **ubližování pomocí digitálních technologií**, např. přes:

- sociální sítě (Instagram, Facebook, TikTok),
- zprávy (WhatsApp, Messenger, SMS),
- e-maily, blogy, fóra, hry.

Typické formy:

- Urážky, výsměch, zesměšňování
- Sdílení citlivých fotek bez souhlasu
- Vydírání nebo vyhrožování
- Falešné profily nebo šíření pomluv

Co dělat:

- **Uložit důkazy** (screenshoty, zprávy, příspěvky)
- **Zablokovat a nahlásit** útočníka na dané platformě
- **Mluvit o tom** – s rodičem, učitelem, důvěryhodnou osobou
- **Kontaktovat odbornou pomoc** – Linka bezpečí 116 111, E-Bezpečí, Policie ČR

🛡️ **Tip:** Nikdy na útočníka nereagujte agresí. To ho může povzbudit. Reagujte taktickou obranou a vždy si hledejte spojence.

🧠 6.2 Jak poznat manipulativní obsah

Manipulace v online prostoru je často skrytá. Cílem je **ovlivnit vaše emoce, názor nebo chování**, aniž byste si toho byli vědomi.

Typické znaky manipulativního obsahu:

- Vyvolává **strach, hněv, šok** nebo silné emoce
- Obsahuje **jednostranné názory**, často bez důkazů
- Útočí na určitou skupinu (např. uprchlíky, politiky, menšiny)

- Používá výkřiky typu „Pravda, kterou nechtějí, abyste věděli!“
- Tváří se jako běžná zpráva, ale chybí autor, zdroj nebo kontext

🚦 **Tip:** Zkuste si položit otázku: **„Komu to slouží? Kdo na tom vydělá?“**

🔎 6.3 Jak ověřit informace (fact-checking, důvěryhodné zdroje)

Praktické postupy:

- **Zadejte klíčová slova do vyhledávače** a hledejte, jestli se o dané zprávě píše i jinde.
- **Ověřte autora** – má jasné jméno, historii, kontakt?
- **Hledejte datum a zdroj** – je zpráva aktuální? Je to známé médium?

Užitočné fact-checking nástroje:

- **Manipulátoři.cz**
- **Demagog.cz**
- **Snopes.com**
- **Ověřovna ČT**
- **AFP Fact Check (cz)**

Jak poznat důvěryhodný zdroj:

- Redakce má **jména autorů, editory, kontakt**
- Je **transparentní** v tom, kdo je vlastníkem
- Opravuje chyby, nepíše anonymně
- Rozlišuje **zpravodajství a komentář**

🚦 **Tip:** Pokud vám zpráva zní podezřele, **nesdílejte ji**, dokud si ji neověříte.

🚨 6.4 Kde nahlásit závadný obsah (např. CZ.NIC, Policie ČR)

Závadný obsah může být:

- Dětská pornografie, nenávistné projevy, výzvy k násilí
- Falešné profily, vydírání, kyberšikana
- Podvodné stránky, phishing

Kam nahlásit:

- **Policie ČR** – linka 158 nebo e-mail kriminalistika@pcr.cz
- **Linka bezpečí (děti)** – 116 111 (nonstop, zdarma, anonymně)
- **CZ.NIC / STOPonline.cz** – hlášení závadného obsahu
- **Bezpečnostní tým CSIRT.CZ** – incidenty ve veřejném prostoru
- **Sociální sítě** – všechny mají možnost nahlášení nevhodného chování

🚦 **Tip:** I jedno nahlášení může zachránit někoho dalšího. **Neváhejte jednat.**

📌 Shrnutí kapitoly:

- **Kyberšikana není „legrace“, ale skutečné nebezpečí**, které ničí životy – zejména dětí a mladistvých.
- Manipulativní a lživý obsah ovlivňuje naši náladu, vztahy i demokracii – **musíme se naučit ho rozpoznat a nepodléhat mu.**
- **Ověřování informací je základní dovednost 21. století** – stejně důležitá jako čtení a psaní.
- Nejsme v tom sami – **existují nástroje, instituce a lidé, kteří pomohou.**

7. PRÁCE A DIGITÁLNÍ HYGIENA

- Bezpečné připojení při práci na dálku (home office)
- Zacházení s firemními daty na osobním zařízení
- Pracovní komunikace – co nepatří do e-mailu
- Používání veřejných zařízení a sítí

S rostoucím trendem práce na dálku, flexibilních pracovních režimů a využívání osobních zařízení pro firemní úkoly je nutné dodržovat zásady digitální hygieny, které chrání nejen zaměstnance, ale i firmu před kybernetickými hrozbami.

🔒 7.1 Bezpečné připojení při práci na dálku (home office)

Základní pravidla:

- **Používejte zabezpečené připojení – VPN**, které šifruje datový provoz mezi zařízením a firemní sítí.
- Vyhýbejte se veřejným Wi-Fi sítím nebo používejte VPN i na nich.
- Používejte **firewall a aktualizovaný antivirový software**.
- Pravidelně aktualizujte operační systém a aplikace.
- Nepoužívejte veřejné počítače nebo sdílená zařízení k práci s citlivými daty.

🚦 **Tip:** Při práci mimo domov mějte vždy po ruce záložní způsob připojení, pokud by VPN selhala.

💾 7.2 Zacházení s firemními daty na osobním zařízení

Co dodržovat:

- Ukládejte firemní data pouze do schválených aplikací a cloudů s odpovídajícím zabezpečením.
- Nepřenášejte citlivé dokumenty přes nechráněné kanály (e-mail, USB bez šifrování).
- Používejte silná hesla a dvoufaktorové ověření pro přístup k firemním systémům.
- Vyvarujte se ukládání pracovních dat na veřejně přístupných místech.
- V případě ztráty nebo odcizení zařízení ihned kontaktujte IT oddělení.

🚦 **Tip:** Pokud je to možné, používejte oddělené profily nebo virtuální plochy pro práci a soukromí.

💬 7.3 Pracovní komunikace – co nepatří do e-mailu

Obsah, který by neměl být v e-mailové komunikaci:

- Citlivé informace, jako jsou hesla, PIN kódy, finanční údaje.
- Informace chráněné zákonem o ochraně osobních údajů (GDPR).
- Interní strategie, smlouvy a jiné důvěrné dokumenty bez šifrování.
- Nepotvrzené informace, spekulace nebo osobní názory, které mohou poškodit firmu.
- Přílohy ve formátech, které nejsou zabezpečené nebo mohou obsahovat malware.

🚦 **Tip:** Používejte firemní šifrované komunikační nástroje (např. Microsoft Teams, Slack) a ověřujte příjemce e-mailu.

🖥️ 7.4 Používání veřejných zařízení a sítí

Rizika veřejných zařízení (např. v knihovnách, kavárnách, na letištích):

- Mohou být infikována malwarem nebo keyloggery.
- Nejsou pod kontrolou vašeho IT oddělení.
- Data mohou být zachycena nebo zkopírována.

Doporučení:

- Vyhněte se práci s citlivými daty na veřejných počítačích.
- Pokud musíte, používejte anonymní relace (inkognito), neukládejte hesla ani osobní data.
- Vždy používejte VPN, pokud přistupujete k firemním systémům přes veřejnou Wi-Fi.
- Po skončení práce si vždy vymažte historii a odhlaste se ze všech účtů.

🚦 **Tip:** Veřejné nabíjecí stanice (USB) mohou být také zdrojem útoků (tzv. „juice jacking“) – používejte raději vlastní nabíječku.

📌 Shrnutí kapitoly:

- Digitální hygiena v práci je klíčová nejen pro ochranu vašich dat, ale i pro reputaci a bezpečnost celé organizace.
- Dodržováním jednoduchých pravidel můžete výrazně snížit riziko úniku informací a kybernetických útoků.
- Bezpečné pracovní návyky jsou investicí do vaší profesní integrity a klidu.

8. ONLINE NÁVYKY A DIGITÁLNÍ ZDRAVÍ

- Digitální rovnováha (screen time, FOMO, info-overload)
- Dopad digitálního světa na psychiku
- Detox od zařízení – kdy a proč si dát pauzu
- Doporučené aplikace pro digitální rovnováhu

Digitální technologie jsou nedílnou součástí našeho života. Umět si však nastavit zdravé hranice je klíčové, aby nám přinášely užitek, ne stres, únavu nebo závislost. Tato kapitola pomůže najít rovnováhu mezi online světem a osobní pohodou.

⚖️ 8.1 Digitální rovnováha (screen time, FOMO, info-overload)

Co to znamená?

- **Screen time** – celkový čas strávený před obrazovkou (mobil, PC, TV).
- **FOMO (Fear of Missing Out)** – strach, že něco důležitého nebo zábavného uniká.
- **Info-overload** – přetížení množstvím informací, které mozek nezvládá zpracovat.

Dopady přemíry digitálního času:

- Snížená koncentrace a produktivita.
- Zhoršení kvality spánku.
- Zvýšená úzkost a stres.
- Sociální izolace.

🚦 **Tip:** Uvědomte si, kolik času opravdu potřebujete online, a stanovte si denní limity.

🧠 8.2 Dopad digitálního světa na psychiku

Digitální prostředí může působit pozitivně i negativně:

- **Pozitivní vlivy:**
  - Rychlý přístup k informacím a vzdělání.
  - Udržování sociálních kontaktů.
  - Podpora zájmů a kreativity.
- **Negativní vlivy:**
  - Zvýšená míra stresu a vyhoření.
  - Závislost na sociálních sítích.
  - Kyberšikana a srovnávání s nereálnými ideály.
  - Ztráta soukromí, pocit neustálého sledování.

🚦 **Tip:** Sledujte své emoce a reakce při používání digitálních technologií. Pokud máte pocit únavy nebo podráždění, je čas na změnu.

⏸️ 8.3 Detox od zařízení – kdy a proč si dát pauzu

Proč je detox důležitý:

- Obnova soustředění a kreativity.
- Zlepšení spánku.

- Posílení mezilidských vztahů v reálném světě.
- Snížení stresu a úzkosti.

Kdy si dát pauzu:

- Když cítíte únavu očí nebo bolesti hlavy.
- Když vás digitální svět rozptyluje od práce či rodiny.
- Při potížích s usínáním nebo neklidným spánkem.
- Když si všimnete závislosti na sociálních médiích nebo hrách.

Jak na detox:

- Naplánujte si **den nebo víkend bez mobilu/PC**.
- Vypněte notifikace, alespoň na určitý čas.
- Věnujte se aktivitám mimo digitální svět (procházky, sport, čtení).
- Zaveďte pravidelné „digitální půsty“ (např. večer po 20. hodině).

🚦 **Tip:** Detox nemusí být dlouhý – i krátké pauzy během dne pomáhají.

📱 8.4 Doporučené aplikace pro digitální rovnováhu

Uživatelsky přívětivé nástroje:

- **Screen Time** (iOS) / **Digital Wellbeing** (Android) – měří čas u obrazovky a umožňuje nastavit limity.
- **Forest** – pomáhá s koncentrací tím, že motivuje odložit telefon.
- **Headspace / Calm** – aplikace na meditaci a zklidnění mysli.
- **Flipd** – blokuje rušivé aplikace a pomáhá držet digitální detox.
- **Freedom** – blokování webových stránek a aplikací na různých zařízeních.

🚦 **Tip:** Vyzkoušejte si, která aplikace vám nejlépe sedí, a přizpůsobte ji svým potřebám.

📌 Shrnutí kapitoly:

- Digitální zdraví není jen absence technických problémů, ale **i duševní pohoda při používání technologií**.
- Nastavení hranic a pravidelný detox pomáhají udržet zdravou rovnováhu mezi online a offline světem.
- Používání vhodných nástrojů může být skvělým pomocníkem v této snaze.

9. JAK BÝT DIGITÁLNĚ ODPOVĚDNÝ OBČAN

- Chovejte se online stejně slušně jako offline
- Pomáhejte ostatním s orientací ve světě technologií
- Ověřujte, nešiřte
- Zapojujte se do vzdělávání a osvěty (školy, komunity, rodina)

Digitální svět je společným prostorem, kde každý z nás hraje roli. Odpovědné chování není jen otázkou osobní bezpečnosti, ale i přispění k lepšímu a bezpečnějšímu prostředí pro všechny.

🤝 9.1 Chovejte se online stejně slušně jako offline

- Buďte zdvořilí a respektujte ostatní uživatele.
- Vyhněte se urážkám, pomluvám, šíření nenávisti a kyberšikaně.
- Pamatujte, že za každým profilem je skutečný člověk se city.
- Dodržujte zákony a pravidla platná i v online prostoru.
- Vždy si ověřujte fakta před sdílením.

🚦 **Tip:** Přemýšlejte, jaký dopad může mít vaše slovo na ostatní.

🌍 9.2 Pomáhejte ostatním s orientací ve světě technologií

- Podporujte seniory, rodiče a méně zkušené uživatele v bezpečném využívání digitálních nástrojů.
- Sdílejte osvědčené postupy a doporučení.
- Buďte trpěliví a vysvětlujte jednoduše, bez odborných termínů.
- Pomozte s nastavením ochrany soukromí a zabezpečení zařízení.

🚦 **Tip:** Vytvořte nebo sdílejte jednoduché návody či checklisty.

🔍 9.3 Ověřujte, nešiřte

- Před sdílením zpráv, fotek či videí si vždy ověřte jejich pravost.
- Používejte důvěryhodné zdroje a fact-checking služby.
- Nepodléhejte emocím vyvolaným senzací nebo dezinformací.
- Upozorňujte ostatní na nepravdivý či manipulativní obsah.

🚦 **Tip:** Nesdílejte informace, které neznáte nebo nepocházíte z ověřených zdrojů.

📚 9.4 Zapojujte se do vzdělávání a osvěty (školy, komunity, rodina)

- Účastněte se školení, workshopů a seminářů o digitální bezpečnosti a odpovědnosti.
- Organizujte nebo podporujte aktivity v komunitě zaměřené na digitální gramotnost.
- Ve školách pomáhejte šířit povědomí o kybernetické bezpečnosti.
- V rodině vedějte otevřené rozhovory o digitálních hrozbách a správném chování online.

🚦 **Tip:** Aktivní přístup posiluje nejen vás, ale i celou společnost.

📌 Shrnutí kapitoly:

- Digitální odpovědnost znamená být vzorem a podporou pro ostatní.
- Společně můžeme vytvořit bezpečnější, přátelštější a důvěryhodnější digitální svět.
- Každý krok k lepšímu online chování se počítá.

10. KRIZOVÉ SITUACE A CO DĚLAT, KDYŽ…

- Ztráta zařízení nebo hesla
- Podezření na podvod
- Nahlášení incidentu (kde a jak)
- Kontakty: NÚKIB, Policie ČR, CERT, Linka bezpečí

Každý z nás se může setkat s nepříjemnou situací v digitálním světě – od ztráty zařízení přes podvodné útoky až po kybernetické incidenty. Důležité je vědět, jak rychle a správně reagovat, aby se minimalizovala škoda a zajistila ochrana.

📱 10.1 Ztráta zařízení nebo hesla

Co dělat při ztrátě telefonu, tabletu nebo notebooku:

- Okamžitě **změňte hesla** k nejdůležitějším účtům (e-mail, bankovnictví, sociální sítě).
- Pokud používáte službu „Najít moje zařízení“ (Apple, Google), pokuste se zařízení lokalizovat nebo vzdáleně uzamknout/vymazat.
- Nahlaste ztrátu operátorovi (mobilní telefon) a zablokujte SIM kartu.
- Zvažte nahlášení ztráty policii, zejména pokud je zařízení firemní nebo obsahuje citlivá data.

Co dělat při ztrátě nebo zapomenutí hesla:

- Použijte funkci „Zapomenuté heslo“ a obnovte přístup přes ověřené kontakty.
- Nikdy nesdělujte hesla e-mailem nebo přes telefon cizím osobám.
- Po obnovení hesla aktivujte **dvoufaktorové ověření (2FA)**.

🚦 **Tip:** Mějte zálohu dat na bezpečném místě.

🕵️ 10.2 Podezření na podvod

Jak poznat, že jste cílem podvodu:

- Obdržíte neočekávaný e-mail, SMS nebo telefonát s žádostí o osobní údaje, hesla nebo platbu.
- Na účtu se objeví neznámé transakce.
- Zařízení se chová podezřele (zpomaluje, otevírá aplikace samo, objevují se neznámé zprávy).

Jak reagovat:

- Neodpovídejte a neklikejte na odkazy.
- Okamžitě změňte hesla a zkontrolujte bankovní účty.
- Uložte všechny podezřelé zprávy nebo hovory jako důkaz.
- Informujte příslušné instituce (banku, Policii ČR, CERT).

🚦 **Tip:** Používejte aktualizovaný antivirový program a firewall.

🚨 10.3 Nahlášení incidentu (kde a jak)

- **Policie ČR:**
  - Telefonní linka 158 (pro nouzové situace)
  - E-mail: kriminalistika@pcr.cz
  - Web: www.policie.cz
- **Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB):**
  - E-mail: cert@nukib.cz
  - Web: www.nukib.cz
- **CSIRT.CZ (Computer Security Incident Response Team):**
  - E-mail: incident@csirt.cz
  - Web: www.csirt.cz
- **Linka bezpečí (zejména pro děti a mladistvé):**
  - Telefon: 116 111 (bezplatná, anonymní linka)
  - Web: www.linkabezpeci.cz
- **CZ.NIC – hlášení závadného obsahu:**
  - Web: www.stoponline.cz

📞 10.4 Kontakty

Organizace	Telefon	E-mail	Web
Policie ČR	158 (linka 112)	kriminalistika@pcr.cz	www.policie.cz
NÚKIB	-	cert@nukib.cz	www.nukib.cz
CSIRT.CZ	-	incident@csirt.cz	www.csirt.cz
Linka bezpečí (pro děti)	116 111	-	www.linkabezpeci.cz
CZ.NIC (závadný obsah)	-	-	www.stoponline.cz

📌 Shrnutí kapitoly:

- Rychlá a správná reakce na krizové situace může minimalizovat škody a ochránit vaše data i bezpečí.
- Nezapomínejte na zálohování a bezpečné uchovávání přístupů.
- Využívejte dostupné oficiální kanály pro nahlášení incidentů.
- Pomozte i ostatním být připraveni na krizové situace sdílením těchto informací.

⬅ END ZÁVĚR

Digitální svět je součástí každodenního života. Buďme v něm stejně ohleduplní, opatrní a zodpovědní jako v tom fyzickém. Zdravá digitální hygiena je cestou k většímu bezpečí – pro vás, vaši rodinu i celou společnost.

📎 Přílohy

- Kontrolní seznam: Moje digitální hygiena v 10 bodech
- Doporučené zdroje, aplikace a nástroje
- Slovníček základních pojmů
- Odkazy na důvěryhodné instituce a portály (např. osveta.nukib.cz, cz.nic, E-bezpečí)

PŘÍLOHA Č. 1

1. Kontrolní seznam: Moje digitální hygiena v 10 bodech

1. Používám silná a unikátní hesla pro každý účet.
2. Aktivoval(a) jsem dvoufázové ověření (2FA) všude, kde je to možné.
3. Nepřipojuji se k veřejným Wi-Fi sítím bez zabezpečeného připojení (VPN).
4. Neposkytuji citlivé údaje přes e-mail nebo zprávy bez šifrování.
5. Pravidelně aktualizuji operační systém, aplikace i antivirový program.
6. Pečlivě ověřuji e-maily a odkazy před kliknutím (vyhýbám se phishingu).
7. Nastavil(a) jsem soukromí na sociálních sítích a omezil(a) sdílení osobních dat.
8. Dávám pozor na kyberšikanu a vím, kde hledat pomoc.
9. Nepoužívám veřejná zařízení k práci s citlivými informacemi.
10. Mám zálohovaná důležitá data a znám postup při ztrátě zařízení nebo hesla.

PŘÍLOHA Č. 2

2. Doporučené zdroje, aplikace a nástroje

Zdroje a weby:

- osveta.nukib.cz – vzdělávání a osvěta v kybernetické bezpečnosti
- cz.nic.cz – doménová autorita a bezpečnostní projekty
- e-bezpeci.cz – informační portál pro bezpečné užívání internetu
- manipulatori.cz – ověřování pravdivosti informací
- linkabezpeci.cz – pomoc dětem a mladistvým v krizových situacích

Aplikace a nástroje:

- **VPN:** NordVPN, ProtonVPN, Surfshark
- **Správci hesel:** 1Password, Bitwarden, Keeper
- **Antivirus:** Avast, ESET, Kaspersky
- **Digitální rovnováha:** Screen Time (iOS), Digital Wellbeing (Android), Forest, Headspace
- **Fact-checking:** Demagog.cz, Ověřovna ČT

PŘÍLOHA Č. 3

3. Slovníček základních pojmů

- **Antivirus:** Program, který chrání počítač před škodlivým softwarem (virem, malwarem).
- **Dvoufázové ověření (2FA):** Bezpečnostní metoda, kdy je k přihlášení potřeba něco, co znáte (heslo) a něco, co máte (telefon, token).
- **Firewall:** Bezpečnostní nástroj, který kontroluje příchozí a odchozí síťový provoz a blokuje neautorizované přístupy.
- **Phishing:** Podvodná technika, kdy útočník snaží získat citlivé informace (hesla, čísla karet) vydáváním se za důvěryhodnou osobu nebo instituci.
- **VPN (Virtual Private Network):** Technologie, která šifruje internetové připojení a chrání uživatele před odposlechem a sledováním.
- **Kyberšikana:** Útok nebo obtěžování prováděné pomocí digitálních technologií.
- **Malware:** Škodlivý software, který může poškodit zařízení nebo ukrást data.
- **Digitální detox:** Plánované odpojení od digitálních zařízení, aby si uživatel odpočinul a snížil stres.
- **Phishing:** Pokus o podvodnou komunikaci za účelem získání citlivých údajů.
- **Správce hesel:** Software, který pomáhá bezpečně uchovávat a spravovat hesla.

PŘÍLOHA Č. 4

4. Odkazy na důvěryhodné instituce a portály

Instituce / Portál	Popis	Web
NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost)	Národní autorita pro kybernetickou bezpečnost	nukib.cz
CZ.NIC	Správce české domény, bezpečnostní projekty	nic.cz
E-Bezpečí	Informační portál o bezpečném využívání internetu	e-bezpeci.cz
Linka bezpečí	Pomoc dětem a mladistvým v krizových situacích	linkabezpeci.cz
CSIRT.CZ	Český tým pro reakci na kybernetické incidenty	csirt.cz
Manipulátoři.cz	Projekt zaměřený na ověřování a odhalování fake news	manipulatori.cz
Policie ČR – kybernetická kriminalita	Kontakty a informace pro hlášení kybernetické kriminality	pcr.cz