První mobil

Příručka pro rodiče

Úvod

Rodičovství v digitální době vyžaduje nové dovednosti.
Proto je důležité být dětem aktivním průvodcem při seznamování s moderními technologiemi. S dobrými radami, nastavením hranic a vzájemnou komunikací může nový telefon přinést radost a zábavu, aniž by ohrozil bezpečnost nejen těch nejmenších.

Než se dítěti rozhodnete dát první mobil, podívejte se na pár technických rad a doporučení.

Nastavení prvního telefonu

Nejčastější situací je, že váš potomek dostane starší telefon po někom z rodiny. Myslete na to, že nestačí jen vyměnit SIM kartu. Některá data v telefonu zůstávají. Než starší telefon dítěti dáte,

- **zazálohujte si veškeré údaje**
- **odhlaste se ze všech účtů**
- **vymažte historii**
- **nebo v nastavení telefonu vyhledejte „Obnovení továrních dat“ nebo „Obnovení továrního nastavení“**

Jak telefon zabezpečit

Mobilní telefon je vlastně malý kapesní počítač. Umí dost věcí a bývá také docela drahý, byla by škoda přijít o něj nebo o údaje v něm obsažené. Spousta z nás má v telefonu velké množství fotek, videí nebo dalších informací. Obsahuje také soukromou komunikaci, kterou by neměl vidět nikdo cizí. Věnujte proto prosím čas nastavení jeho zabezpečení.

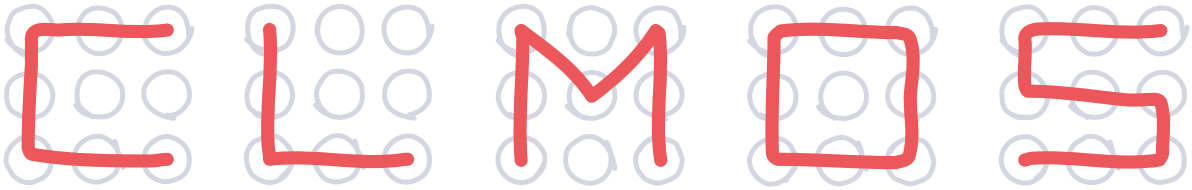
Pomocí PIN kódu

PIN je bezpečnostní číselný kód, který bývá většinou čtyřmístný. PIN je nám obvykle přidělen, ale je možné si ho změnit. Stejně jako u hesel bychom si měli nastavit takový PIN, který nebude možné jednoduše uhodnout.

Věděli jste, že ze čtyřmístného PINu lze vytvořit přibližně 10.000 různých kombinací, z nichž je ale téměř 300 lehce uhodnutelných? PIN by tedy neměla být čísla opakující se nebo jdoucí za sebou (1212, 1234, 4321, 1111 atd.)

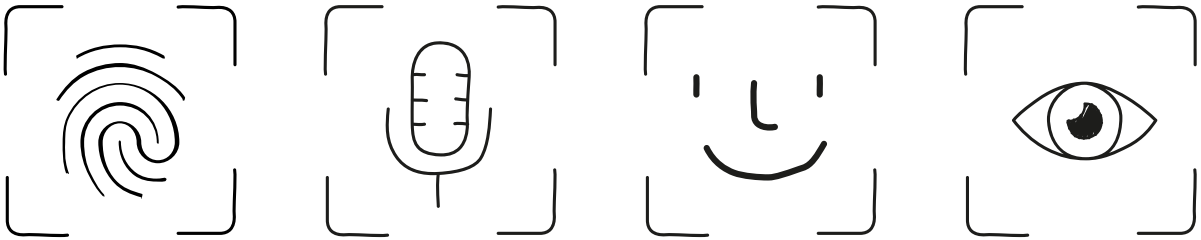
Pomocí gest

U dětí je hodně oblíbené zabezpečení pomocí gest. Telefon nebo tablet se odemkne, pokud správně vytvoříme na obrazovce symbol. Toto zabezpečení ale nepatří mezi nejsilnější. Stejně jako u PIN kódu existuje několik známých kombinací. Například gesto ve tvaru písmene, domečku nebo jiného známého tvaru. Použití podobného gesta je stejné, jako byste měli nastavené heslo „heslo“ nebo PIN 1234. Na internetu dokonce existují seznamy nejčastějších kombinací.



Pomocí biometrických údajů

Pokud to typ telefonu umožňuje, zabezpečte dítěti telefon touto metodou. Jedná se o jednu z nejbezpečnějších metod, jakou si zabezpečit vlastní účet nebo zařízení. Technologie se navíc velmi rychle vyvíjí a je velmi obtížné ji obejít nebo prolomit. Na rozdíl od jiných ochran účtu tyto mají jednu velkou výhodu. Nelze je zapomenout nebo ztratit.



Automatické zamknutí displeje

Chytré telefony mají funkci, která při jeho nepoužívání uzamkne displej. Když ho pak vezmete po nějaké době do ruky, musíte ho znovu odemknout. Dobu, než se telefon automaticky uzamkne, si můžete nastavit. Od pár vteřin po minuty (nebo vůbec). Je to důležitá ochrana proti tomu, aby se cizí návštěvníci dostali do telefonu.

Náhledy zpráv

Pokud na telefonu obdržíte zprávu, standardně to bývá tak, že se zobrazí její náhled. Někdy i v případech, pokud je obrazovka vypnutá. To se může jevit jako užitečná věc.

Pokud ale nejste u svého telefonu, může si zprávu přečíst kdokoliv. Nastavení náhledů zpráv lze upravit. V telefonu je tato volba umístěna většinou v položce „Oznámení“ nebo „Zprávy“.

Rady, které předejte svým dětem

Půjčování telefonu
Vysvětlete dětem, že by neměly telefon půjčovat cizím lidem. Kamarádům také ne. Když se i přesto tak rozhodnou, měly by být u toho a mít svůj telefon pod dozorem. Proč? V telefonu jsme většinou automaticky přihlášeni k mnoha službám a cizí lidé se k nim mohou jednoduše dostat.

Zálohujte!
Fotky, videa, komunikace nebo uložené herní pozice mohou nenávratně zmizet, pokud nebudete svoje zařízení zálohovat. Většina chytrých telefonů zálohuje automaticky na vzdálené úložiště (tzv. cloud).

Aktualizujte!
Můžete mít sice nejmodernější telefon, ale pokud nebudete pravidelně aktualizovat jeho systém nebo klíčové aplikace, stává se zranitelným. Kvůli chybám v aplikacích či systému se mohou útočníci dostat k SMS, stáhnout si fotografie, zapnout mikrofon nebo sledovat polohu.

Aplikace

Aplikace do telefonu instalujte jen z oficiálních míst výrobce. Mezi největší patří Google Play, App Store, Microsoft Store nebo Samsung Galaxy Store.

Jaké aplikace si stáhnout

Do dnešních mobilních telefonů si můžete i díky velké paměti nahrát stovky různých aplikací. Než stáhnete aplikaci z obchodu, podívejte se pozorně na několik věcí:

- Vývojáři si mohou zaplatit reklamu na své aplikace.
  Nespoléhejte na doporučení obchodu.

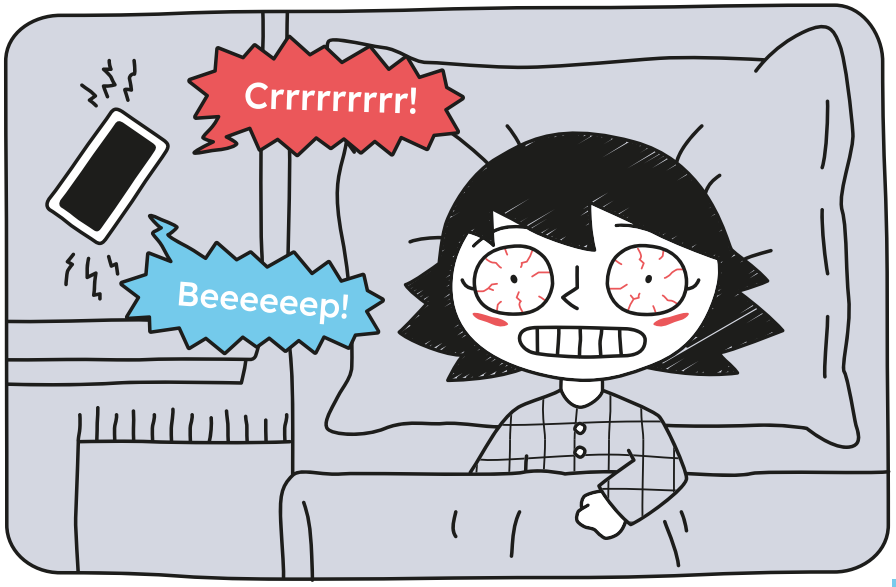
- Pročtěte si recenze. Nejen ty s pěti hvězdičkami, ale i ty nejhorší.
  Můžete zjistit, že aplikace není tak dobrá, jak se na první pohled jeví.

- Pozorně se podívejte na podmínky používání aplikace.
  Některé mohou sbírat více údajů, než je potřeba.

- Není Messenger jako Messenger. Některé aplikace se mohou jmenovat podobně nebo mít podobné logo. Zneužívají podobnost loga i názvu a mohou být i placené.

- Podívejte se, kdy byla aplikace v obchodě naposledy aktualizována. Pokud to bylo před delší dobou, nestahujte ji. Nemusí být již bezpečná.

Děti experimentují a budou si do telefonu instalovat desítky aplikací. Je dobré nastavit pravidla pro jejich stahování. Mluvte s nimi o tom, co je baví nebo jaké služby využívají.

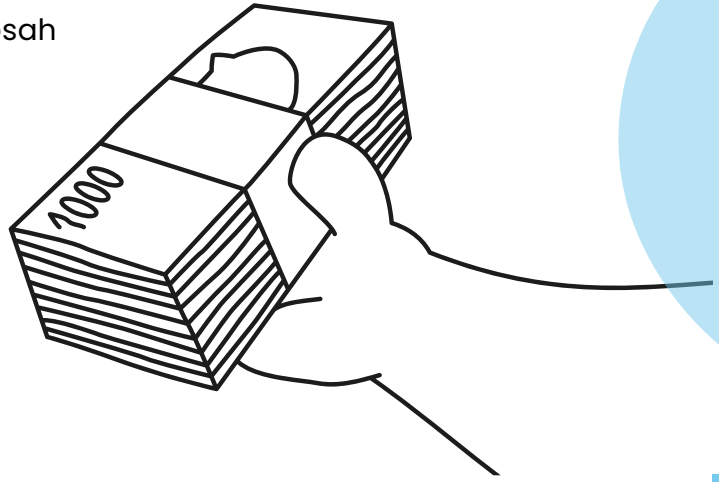


Placené aplikace

Velká část aplikací v obchodech je placená. Buď za ně zaplatíte jednorázově, nebo po nějaké době používání. Na to si dejte pozor. Pročtěte si pozorně podmínky o předplatném. Některé aplikace se tváří, že jsou zadarmo, a po několika týdnech odhalíte nepříjemné překvapení.
Najděte v telefonu položku Předplatné. Obvykle se v telefonu nachází v položce Nastavení. Zde můžete své platby za aplikace spravovat.

M platby – finanční transakce, herní aplikace

M platba je způsob, jak pomocí mobilního telefonu, resp. cestou telefonního čísla, které máte od operátora, zaplatit za nějakou službu. M platbou můžete zaplatit v podstatě cokoliv a účtovaná částka se vám přičte k vašemu účtu za telefonní služby. Že to neděláte? A co platba lístku v MHD nebo dárcovské DMS. To jsou M platby také… I dospělý se může zmýlit a využít této služby nechtěně. Třeba kliknutím na ANO pod obsahem, který chce zobrazit. Ta malá písmenka pod tímto ANO nás ale varovala, že obsah je placený.
A to nemluvíme o dětech.
Ty si velmi rády koupí placený obsah ve hře, kterou hrají na vašem mobilním telefonu. A rodiče se mnohdy nestačí divit, když jim přijde čtyřnásobně vyšší částka, než na kterou jsou zvyklí.



Wi-Fi, Bluetooth, Lokalizace

Chytré telefony nabízí celou škálu možností, díky kterým jsou plnohodnotným nástrojem při práci s internetem nebo obsahem. Vysvětlete dětem pár zásad při jejich používání.

Jak se připojit bezpečně na Wi-Fi síť

Pojmem Wi-Fi (Wireless Fidelity) se označuje bezdrátové propojení koncových zařízení (počítač, tablet, chytrý telefon) k počítačové síti, která je lokální nebo internetová. Nejedná se tedy o připojení k internetu, jde o funkci, která přenáší signál.

Než se připojíte na Wi-Fi, podívejte se na pár rad

- Do e-mailu, sociálních sítí nebo důležitých služeb se připojujte pouze přes aplikaci příslušné služby
- Používejte zašifrované stránky, které poznáte podle toho, že před začátkem webové adresy obsahují HTTPS
- U neznámých sítí si nenastavujte automatické připojení

- Věnujte pozornost varováním ze strany svého prohlížeče, antiviru nebo jiného bezpečnostního systému

- Při používání Wi-Fi používejte VPN, ta zašifruje přenos dat a nikdo cizí komunikaci nerozluští

- Dejte si pozor na sítě, které se tváří jako „free“ nebo „public“

Bluetooth

Je bezdrátová technologie pro výměnu dat mezi blízkými zařízeními. V závislosti na podmínkách má dosah zhruba deset až padesát metrů a jde o relativně bezpečnou technologii. Zařízení mění frekvenci až stokrát za vteřinu, aby se bránila hackerským útokům.

I když je technologie Bluetooth relativně bezpečná, dodržujte pár zásad:

- Při návštěvě přeplněných míst mějte Bluetooth vypnutý
- Aby byl proveden útok přes Bluetooth, musí být útočník poblíž. Hlídejte si proto své okolí
- Nastavte si na svém zařízení režim „Skryté“ místo režimu „Zjistitelné“
- Připojené zařízení by mělo být pravidelně aktualizováno

Lokalizace

Některé aplikace potřebují ke své funkčnosti zapnutí lokalizace. Může jít o navigaci, aplikace s mapami, počasím nebo třeba Pokémon GO. Bez zapnuté lokalizace bude nejspíš aplikace nepřesná nebo nefunkční. Zkuste dětem vysvětlit, že používáním lokalizačních služeb nebo označováním se na internetu, se vystavují určitému riziku.

Výhody používání lokalizačních služeb v telefonu:

- Najít, kde jsme, když se ztratíme v přírodě či neznámém městě
- Najít nejbližší zastávku, bankomat...
- Sdílet s přáteli místa, která jsme navštívili

Nevýhody používání lokalizačních služeb v telefonu:

Někteří lidé si mohou na základě sdílených informací dát dohromady, kde se nacházíte nebo jaká místa navštěvujete nejčastěji. Zjistit lze, do jaké školy děti chodí nebo kde bydlí. Pak už je jednoduché je dohledat.

Na internet dávejte fotografie nebo videa až s určitým časovým odstupem, když už se na příslušném místě nenacházíte. Omezte také sdílení fotek s označením polohy, na kterém se pravidelně nacházíte.

Rodičovská kontrola

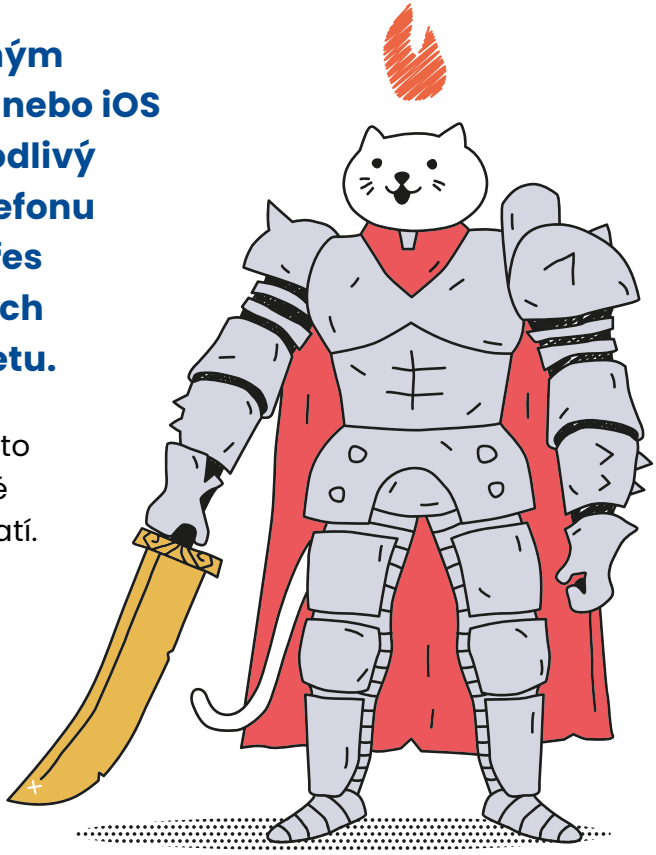
Sdílení polohy zařízení lze využít i pro rodičovskou kontrolu. Přesněji řečeno ke zjištění polohy telefonu vašeho dítěte. Tedy v případě, že ho má u sebe. Nejde samozřejmě o žádné šmírování, ale ujištění se, že například dorazilo v pořádku v obvyklý čas domů ze školy nebo na kroužek. K tomuto účelu slouží i aplikace, které mají více funkcí. Může to být kromě sledování polohy i omezení času stráveného na mobilním telefonu nebo na konkrétních aplikacích. A dále mohou pomáhat s filtrováním obsahu a aplikací vhodných pro děti.

Je potřeba mít antivir v telefonu?

Mobilní telefony s aktualizovaným operačním systémem Android nebo iOS jsou velmi dobře chráněny. Škodlivý software se může dostat do telefonu několika způsoby. Nejčastěji přes neznámé aplikace z neoficiálních obchodů a pohybem na internetu.

Antivirový program bychom ale i přesto měli mít. Některé jsou zdarma, některé placené. Investice do nich se ale vyplatí. Antivirových programů je celá řada, vyzkoušet můžete tyto:

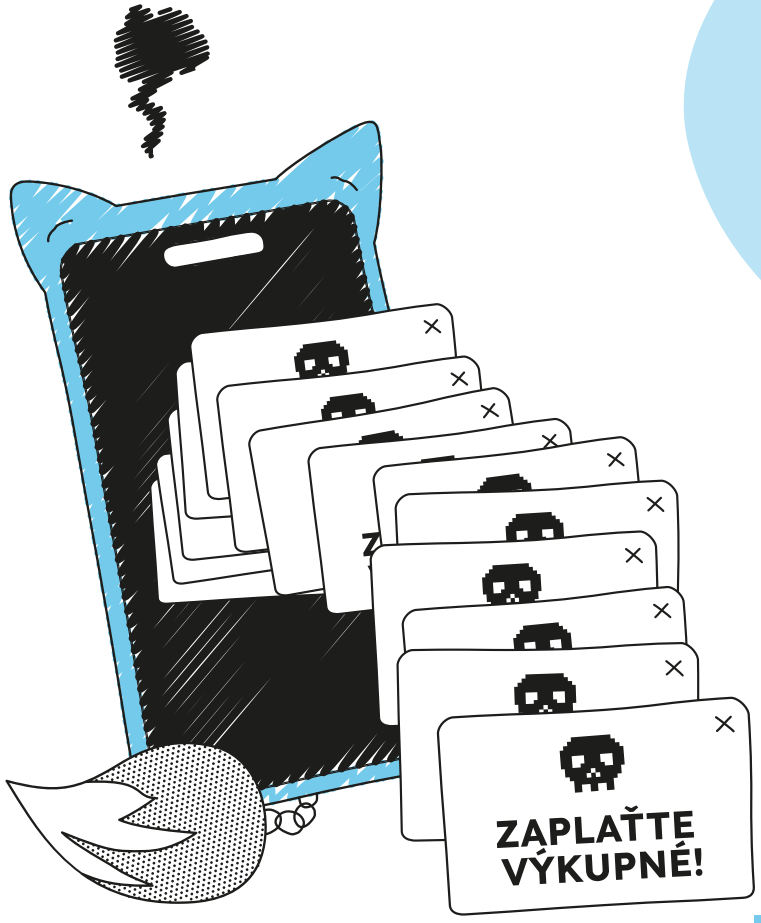
- **Norton Mobile Security**
- **ESET Mobile Security**
- **Avast Mobile Security**



Jak poznat, že je telefon zavirovaný

Pokud je telefon napaden škodlivým kódem, může se chovat zvláštně. Některé známky možného napadení telefonu:

- Baterie telefonu se rychle vyčerpává
- Objevují se aplikace, jejichž stažení si nevybavujete
- Vyskakují na vás reklamy
- Aplikace se stále zavírají
- Telefon se často restartuje, zamrzá nebo přehřívá
- Vaše data se velmi rychle vyčerpávají

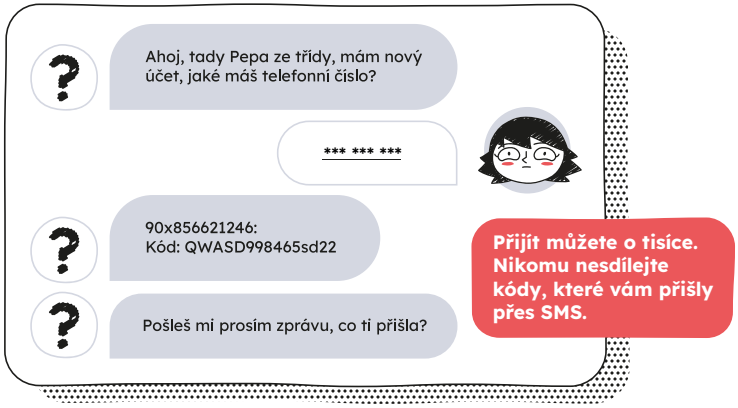


Nejčastější podvody

Vishing, smishing a spoofing jsou aktuálním trendem v nezákonných postupech podvodníků, jejichž cílem je získat neoprávněně cizí finanční prostředky nebo osobní data. Děti se nejčastěji mohou setkat se smishingem.

Smishing
Slovo smishing je kombinací slov SMS a phishing.

Jde o podvod, kterým se z vás útočník snaží dostat pomocí SMS zprávy údaje jako heslo, platební údaje ke kartě, PIN apod.



Jak poznat, že jde o podvodnou zprávu?

- SMS vás nabádá ke kliknutí na neznámý odkaz
- Odkaz bývá zkrácený
- Podvodníci se vydávají za známé společnosti (pošta, úřad nebo banka aj.)
- SMS obsahuje výzvu, vyvíjí časový nátlak nebo slibuje peníze
- Může občas obsahovat gramatické chyby

Co dělat v případě krádeže telefonu

Krádež telefonu není příjemná situace. I pokud byl telefon hodně levný nebo starší, měli bychom jeho krádež oznámit. Důležité jsou dva kroky:

1. **Obraťte se na svého operátora, který zablokuje SIM kartu**
2. **Obraťte se na Policii ČR, která zažádá operátory o zablokování telefonu podle jeho IMEI čísla**

Na Policii ČR musíte vlastnictví telefonu prokázat:
Účtenkou, fakturou, záručním listem nebo krabicí s výrobním číslem IMEI.

Co je IMEI a na co ho budu potřebovat

IMEI (International Mobile Equipment Identity) je unikátní patnáctimístné číslo mobilního telefonu, které mu přiděluje jeho výrobce. Toto číslo ukládá mobilní operátor do speciálního registru. Po nahlášení krádeže telefonu pak přístroj na základě tohoto čísla může operátor zablokovat.

Důležitá je rovnováha

Online prostor je v dnešním světě pro děti velmi důležitý. Abychom jim pomohli cítit se v něm dobře a předešli vzniku závislosti, je potřeba, abychom se v něm sami dokázali bezpečně a jistě pohybovat, snažili se porozumět světu svých potomků a respektovali ho.

Nakoukněte do světa svého dítěte – koho sleduje, co formuje jeho názory. Zkuste se chovat jako návštěva – nekritizujte, neshazujte to, co vidíte. Vymezte si doma offline zóny. Pro všechny – tedy i pro dospělé. Jděte dětem příkladem – rodič zabořený do mobilu odhánějící dítě od počítačové hry není zrovna přesvědčivý.

Slyšet pochvalu nebo potlesk je krásný pocit a je to zcela přirozené. Stejně tak i na internetu. Po získání lajku nebo jiném uznání vyplavuje náš mozek látku, která se nazývá dopamin. Náš mozek má tuto látku moc rád a chce tento pocit vzrušení nebo radost stále opakovat. Snaha zažít virtuální pochvalu nebo slávu může být návyková. Když lajky nebo ocenění ustanou, mohou děti cítit smutek, strach,

nejistotu nebo mít pocit selhání. Mít hodně lajků ale neznamená, že jsme slavní nebo že jsme lepší než někdo druhý.

Čas strávený dětmi online můžete ohlídat přes různé nástroje. Nezapomeňte, že je dobré vyvážit čas strávený online nějakou jinou aktivitou, třeba sportem nebo jinými koníčky.
Pravidlo 3N: NEzakazovat, NEzaostávat, NEzanedbávat.

Modré světlo - Omezte používání telefonu před spaním

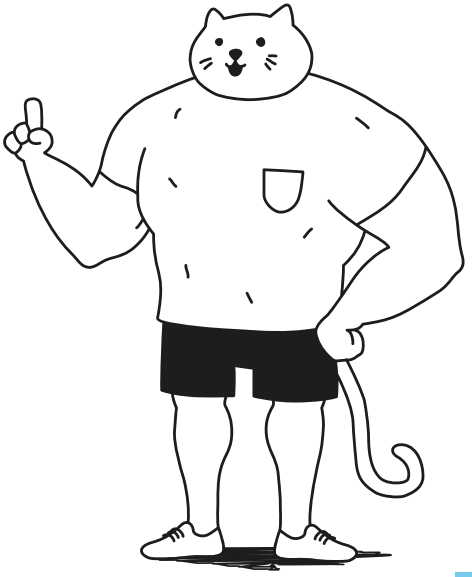
Vliv technologií na lidské zdraví je bohužel nenápadný a plíživý. Některé změny už ale vědci dokázali dobře popsat. Ať už jde o nárůst obezity mezi dětmi, větší počet nemocí očí nebo rozvoj cukrovky, onemocnění srdce a dalších chorob. Nadměrné používání informačních a komunikačních technologií ale způsobuje i spoustu nemocí, o kterých naši předkové nikdy neslyšeli. Zjednodušeně jim říkáme kybernemoci. Zasahují do fyzického i duševního zdraví člověka a setkává se s nimi skoro každý aktivní uživatel digitálních technologií.

Používáte mobil, tablet nebo počítač před spaním? A víte, co je to tzv. modré světlo? Modré světlo je všude okolo nás, jedná se o jednu ze složek slunečního světla. Díky němu dokáže náš organismus rozpoznat, jestli je den nebo noc. Pokud se vystavujete nepřirozenému modrému světlu v noci, naše tělo přestává produkovat hormon melatonin, což ovlivňuje kvalitu spánku, nebo se nám může hůře usínat.

Doporučené materiály

V České republice vzniká neuvěřitelné množství vzdělávacích materiálů k tématu kyberbezpečnosti. V příručce jsme se rizikovým jevům věnovali jen okrajově. O tématech jako je kyberšikana, sexting, podvody, ochrana soukromí, sociální sítě apod., se více dozvíte v uvedených zdrojích. Pokud si nebudete vědět rady, můžete se obrátit na specializované poradny. Třeba na Rodičovskou linku.

Pro ty nejmenší děti doporučujeme Kyberpohádky, které pomáhají rodičům i učitelům budovat zdravé návyky u předškolních dětí. Využít můžete také projekt ON-LINE ZOO, který nabízí knihu, audioknihu nebo omalovánky k daným tématům.



Zdroje:

www.o2chytraskola.cz
www.policie.cz
www.bezpecnyinternet.cz

Příručka vznikla za podpory:

Safer Internet Centrum | Česká republika

cz.nic

POLICIE ČESKÉ REPUBLIKY

vodafone

O2 | Chytrá škola

T-Mobile