Základy bezpečnosti ve virtuálním světě

Milan Kolarovský

Bezpečnost na osobním počítači

- Dětský účet, který je omezený
- Nastavení omezení na Android zařízení
- Antivirový program s rodičovskou kontrolou
- Vypnutá webkamera

Dětský účet

- Kontrola obsahu
  - Rodiče mohou omezit přístup k určitému obsahu (aplikace, hry, weby)
- Monitorování aktivit
  - Rodiče mohou monitorovat, co dítě tvořilo na počítači
- Omezení času stráveného u počítače
- Věková omezení
- QR kód odkazuje na nastavení dětského účtu

Nastavení omezení na Android zařízení „Google Family Link“

- Omezení různého obsahu, jako jsou webové stránky a aplikace.
- Správa času stráveného na obrazovce.
- Lokalizace telefonů pomocí GPS.
- Možnost stahování aplikací z Obchodu Play.
- Omezení spuštění předinstalovaných aplikací na zařízeních.
- QR kód odkazuje na nastavení Family Link

Antivirový program s rodičovskou kontrolou

- Ochrana před viry a škodlivými webovými stránkami
  - Chrání celkově počítač před viry a škodlivými webovými stránkami
- Blokování škodlivého nebo nevhodného obsahu
  - Díky rodičovské kontrole je možné blokovat nevhodný obsah pro děti
- Monitorování aktivit
  - Rodiče mohou monitorovat, co dítě tvořilo na počítači

Vypnutá webkamera

- Ochrana soukromí
  - Přes webkameru lze pořídit snímky, které mají závažné následky
- Vypnutí kamery
  - Rodičovská kontrola
  - Přelepení
  - Odinstalování ovladačů

Bezpečnost na internetu

- Zásady soukromí
- Sdílení dat
- Sexting

Zásady soukromí

- Hlídání si své indentity
  - Online identita je osobnost dětí v online prostoru a je třeba ji chránit
  - Nikdy nikomu nesdělovat osobní údaje (věk, jméno, adresa, telefonní číslo, fotografie)
  - Opatrnost (Nedůvěra) ke všemu, co na internetu nalezneme
- Navštěvování pouze bezpečných stránek

Sdílení dat

- Nikdy nikomu nesdělovat osobní údaje
- Seznámení se s podmínkami dané sítě (vše, co se vloží na sítě, je v jejich vlastnictví)
- Je potřeba komunikovat se svými dětmi a vysvětlit jim nebezpečí
  - Je nutné, aby děti pochopily, proč je důležité být opatrný
  - Vysvětlovat empaticky, aby děti neudělaly přesný opak (nic nezakazovat, pouze varovat a komunikovat)
  - Používejte přirovnání ke hmatatelným věcem

Sexting

- Sexting je dobrovolné sdílení intimních materiálů (fotografie, videa)
- Další podoba sextingu je textová
- Největší riziko je zneužití, vydírání
- Spousta případů skončilo velmi tragicky

Obrana proti sextingu

- Vysvětlete dětem, co je vhodné sdílet
- Sledování dítěte pomocí rodičovské kontroly
- Naučte děti říct NE věcem, které jim nejsou příjemné (nemyslím domácí práce)
- Získejte co nejvíce informací o sociálních sítích, které dítě využívá
- Promluvte si otevřeně s dětmi o sexualitě
- Pokud se dítě stalo obětí sextingu kontaktujte policii, která podnikne další důležité kroky

Email

- Spam
- Phishing

Spam

- Forma nevyžádané hromadné komunikace
- Jedná se převážně o reklamní nabídky
- Dále je zde Phishing, který slouží ke krádeži dat, nebo financí
- Ochrana
  - Naučte se je rozpoznat (obsahují nesmyslné částky, poupravené odkazy)
  - Zvyšte bezpečnost vašich online účtů (silnější hesla, dvoufaktorové ověření)
  - Používejte DNS filtrování (mnoho poskytovatelů ho již má v základu, například Seznam)
- Pokud jste se stali obětí a zadali platební informace okamžitě zavolejte na danou instituci a vše zablokujte

Phishing

- Slouží ke krádeži osobních dat, financí nebo instalaci škodlivého softwaru
- Emailový phishing
  - Odesílán skrz spamovou komunikaci
  - Slouží zejména k získání citlivých informací a přístupovým údajům
- Spear phishing
  - Cílený útok
  - Používá personalizované e-maily (například napodobenina emailu od banky)

Ochrana proti phishingu

- Používaní vícestupňového zabezpečení
- Pořádně si prohlídněte příchozí mail
  - Emailová adresa
  - Design emailu
  - Odkaz na webovou stránku
- Žádná společnost nikdy nebude chtít, aby jste jim poskytli přístupové údaje
- Pokud jste se stali obětí a zadali platební informace okamžitě zavolejte na danou instituci a vše zablokujte

Sociální sítě

- Při komunikaci na sociálních sítích je třeba se držet těch samých zásad jako na celém internetu tj.
  - Nesdílet osobní údaje
  - Nesdílet nevhodné fotografie
  - Seznámit se s podmínkami dané sociální sítě (co vložíte na sociální sítě, je jejich majetek)
  - Nekonat proti svému přesvědčení z nátlaku
- Pro nezletilé je vhodné nastavit rodičovskou kontrolu
- QR kód odkazuje na nastavení soukromí na Facebook

Rizika mob. telefonu

- Podvodné telefonáty
- Podvodné SMS

Podvodné telefonáty

- Nezvedejte telefonáty z jiné předvolby než +420 pokud nevíte, že v dané zemi, ze které je telefonát, nemáte blízkou osobu
- Nesdělujte nikomu své osobní údaje
  - Žádná instituce je po vás chtít nebude (pouze banka rodné číslo)
  - Za žádnou cenu nesdělujte informace platební karty nebo potvrzovacího SMS kódu
- Buďte nedůvěřivý
- Pokud máte pochybnosti, nebojte se telefonát zavěsit a zavolat přímo na danou instituci

Podvodné SMS

- Podvodníci se vydávají za instituce za účelem získání osobních údajů a bankovních přístupů
- Buďte nedůvěřivý
  - Pořádně si prohlédněte text dané zprávy
  - Zkontrolujte telefonní číslo
  - Pokud je vám neznámo proč SMS přišla, kontaktujte napřímo danou instituci
- Nikdy nesvěřujte osobní údaje

Kyberšikana

- Definice
- Příklady
- Důsledky
- Prevence
- Jak reagovat

Definice Kyberšikany

- Kyberšikana je šikana, která se odehrává na digitálních zařízeních
  - Mobilní telefony, počítače, tablety
- Zahrnuje odesílání negativního, škodlivého, falešného nebo zlomyslného obsahu o někom jiné s cílem mu ublížit a zesměšnit
- Může také obsahovat osobní a soukromé informace o někom jiném
- Některé formy překračují hranici trestného chování

Příklad Kyberšikany

- Jan a Tomáš jsou spolužáci na střední škole. Jednoho dne se Tomáš rozhodl udělat Janovi naschvály. Vytvořil falešný profil na sociální síti pod Janovým jménem a začal posílat urážlivé zprávy ostatním spolužákům. Také zveřejnil několik trapných fotografií Jana, které pořídil bez Janova vědomí a souhlasu.
- Tomáš také vytvořil falešnou e-mailovou adresu v Janově jméně a začal posílat e-maily učitelům s nevhodným obsahem. Jan se dozvěděl o těchto aktivitách, když ho spolužáci a učitelé začali konfrontovat s těmito zprávami a fotografiemi.
- Toto je příklad kyberšikany, protože Tomáš použil digitální platformy k šikanování a obtěžování Jana, což mělo negativní dopad na Janovu reputaci a emoční pohodu.

Důsledky Kyberšikany

- Emoční a psychické problémy
- Sebepoškozování a sebevražedné myšlenky
- Problémy ve škole
- Sociální izolace
- Zdravotní problémy

Prevence Kyberšikany

- Bezpečné používání internetu
- Blokování a hlášení kyberšikany
  - Zde je potřeba komunikace se svými dětmi, aby se nebáli vás o ní informovat
- Podpora a pomoc
  - Pokud jste svědkem je důležité pomoc oběti

Jak reagovat při setkání s Kyberšikanou

- Neopovídejte na provokace
- Vše je třeba zaznamenat
- Nejvíce důležitá je komunikace s postiženou osobou
- Přerušení kontaktů s agresory
- Kontaktování policie

Otázky a Odpovědi

- Bezpečnost na počítači
- Bezpečnost na internetu
- Email
- Sociální sítě
- Mobilní telefon
- Kyberšikana

Konec ☺

Díky za Vaší pozornost!