KyberGuru

brožura k podcastovému seriálu

2024

Kraje pro bezpečný internet

KyberGuru

brožura k podcastovému seriálu 2024

Kraje pro bezpečný internet s podporou Středočeského kraje
a Vzdělávacího institutu Středočeského kraje

Obsah

O PROJEKTU KPBI

Projekt Kraje pro bezpečný internet vzdělává v problematice bezpečného užívání internetu

- veřejnost (děti, rodiče, seniory),
- pedagogy a
- sociální pracovníky.

Od roku 2013, kdy projekt vznikl, zpracoval desítky e-learningů, podcastů, videí a pracovních listů, realizoval online i offline školení, zapojil tisíce studentů do každoročního soutěžního kvízu pro základní a střední školy.

Aktuální informace zveřejňuje také na svém Facebooku (KPBI) a Instagramu (o_klik_napred).

Září 2013: projekt byl schválen usnesením Rady Asociace krajů České republiky na 6. zasedání v Ústí nad Labem, tisk č. 44.

2014: vznikají první e-learningové lekce pro žáky a studenty.

2016: vznikají první vzdělávací videospoty (pro cílovou skupinu seniorů).

2019-2021: aktulizace a přidávání nových e-learningových lekcí pro rodiče, děti, učitele a sociální pracovníky.

2023: do projektu se zapojilo všech 14 krajů ČR.

KYBERGURU 2023

Ohlédnutí za první podcastovou sérií.

KYBERGURU 2023: PŘEHLED PODCASTŮ A JEJICH TÉMAT

TÉMA 1

Kyberkriminalita v ČR strmě stoupá. Co s tím?

Trendy v kyberkriminalitě nám pomohl odhalit **mjr. Richard Valiček**, vedoucí oddělení kybernetické kriminality Středočeského kraje.

Víte, jestli se dopouštíte trestného činu, když nelegálně stahujete filmy z internetu?

TÉMA 2

Jak danit příjmy z online aktivit?

Daňová specialistka a majitelka účetní kanceláře **Šárka Pelikánová** sama natáčí podcast Snídaně s Šárkou.

Zjistěte, jaké typy online příjmů byste měli uvést do daňového přiznání.

TÉMA 3

Vyhněte se finančním podvodům na internetu

Ivan Štefek je bezpečnostní expert se zkušenostmi z pojišťovny ING nebo investiční skupiny KKCG.

Prozradil, kdo krade údaje k platebním kartám a co s nimi pak dělá.

TÉMA 4

Vliv počítačových her (nejen) na děti

Michaela Slussareff napsala knihu *Hry, sítě, porno*. Spoluzaložila iniciativu Digitální zdraví dětí a přednáší na FF UK v Praze.

Je opravdu reálné, aby vášnivý hráč střílečekšel někoho zabít ve skutečném světě?

TÉMA 5

Rozhovor s hackerem

Etický hacker, výzkumník a spolumajitel společnosti Cyber Rangers **Daniel Hejda** patří mezi TOP IT osobnosti roku 2021.

Proč byste si po hackerském útoku neměli vypínat počítač?

Cekem 300 minut rozhovorů si poslechněte na Spotify nebo YouTube kanálu KPBI.

KYBERGURU 2024

Představení nových dílů
a testových otázek.

KYBERNETICKÉ PASTI: OD FALEŠNÝCH E-MAILŮ PO DIGITÁLNÍ VYDÍRÁNÍ

NÚKIB evidoval v roce 2023 celkem 262 kybernetických incidentů, což je dvojnásobný nárůst oproti roku 2022. Cílem útoku mohou být firmy, státní instituce, ale i obyčejní lidé.

Zákulisí kyber-podvodů odhalují **plukovník Ondřej Moravčík**, vedoucí tiskového oddělení Policie ČR, **a plukovník Jiří Nový** z Národní centrály proti terorismu, extremismu a kybernetické kriminalitě.

Ve dvou epizodách rozhovoru se dozvíte:

- jestli se máme bát ztráty osobních údajů při nakupování na čínských online tržištích jako Temu nebo Alibaba,
- o co šlo vyděračům při ransomwarových útocích na nemocnice v Brně, Benešově nebo Düsseldorfu,
- jak je složité dopadnout pachatele online útoků?

Naučíte se taky, jak:

- zajistit důkazy,
- rozpoznat vishing, smishing nebo fake kryptoměny,
- neúmyslně nepodporovat DDoS útoky.

OTESTUJTE SVÉ ZNALOSTI

Který z následujících typů útoků vám nejčastěji posílá falešné e-maily s odkazem na podvodnou stránku?

1. ransomware
2. phishing
3. DDoS útok

Jaký je hlavní rozdíl mezi spear-phishingem a běžným phishingem?

1. Spear-phishing se zaměřuje na konkrétní osobu nebo organizaci, zatímco běžný phishing se rozesílá hromadně.
2. Běžný phishing se provádí pouze přes e-mail, zatímco spear-phishing používá různé komunikační kanály.
3. Spear-phishing vyžaduje fyzický přístup k zařízení oběti.

Jakým způsobem se ransomware obvykle nešíří?

1. Infikovanými e-mailovými přílohami.
2. Přes napadené webové stránky.
3. Sociálním inženýrstvím bez využití technických prostředků.

Zkontrolujte si své odpovědi v podcastu **KyberGuru.**

DĚTI V SÍTI: JAK CHRÁNIT NAŠE NEJMENŠÍ PŘED ONLINE PREDÁTORY A KYBERŠIKANOU?

Podle studie společnosti O2 z roku 2023 se každé páté české dítě ve věku 8–15 let už někdy setkalo s kyberšikanou a 40 % školáků přiznalo, že má online kamaráda, kterého nikdy neviděli naživo.

O bezpečnosti dětí na internetu si povídáme s vedoucím projektu E-Bezpečí **Kamilem Kopeckým** a spoluzakladatelkou Replug.me – psycholožkou **Radkou Kůřilovou**.

Ve dvou epizodách rozhovoru se dozvíte:

- jaké nové hrozby čekají na děti v online prostředí,
- kam si dojít pro radu, když se dostaneme do nesnází,
- jestli to rodiče občas nepřehánějí se sledováním svých dětí přes různé aplikace.

Naučíte se taky, jak:

- pracovat s dětmi, který byly vystaveny online vydírání,
- zpracovat pocity viny, bezmocnosti a frustrace,
- (ne)omezovat své děti v používání internetu a nových technologií.

OTESTUJTE SVÉ ZNALOSTI

Jaký je nejčastější varovný signál, že dítě může být obětí kyberšikany?

1. Ztráta zájmu o online aktivity.
2. Zvýšení zájmu o online aktivity.
3. Tajnůstkaření ohledně online aktivit.

Jak by měli rodiče reagovat, pokud jejich dítě přizná, že se mu na internetu děje něco nehezkého?

1. Ignorovat to a nechat dítě, aby to zvládlo samo.
2. Podpořit dítě, zajistit jeho bezpečnost a nahlásit incident příslušným autoritám.
3. Zakázat dítěti používat internet.

Jaký krok je nejdůležitější při prevenci závislosti dětí na online hrách?

1. Instalace programů rodičovských kontrol na všech zařízeních.
2. Pravidelný rozhovor s dítětem o rizicích nadměrného hraní a nastavování pravidel používání počítače/mobilu.
3. Dohled nad každým okamžikem stráveným online.

Zkontrolujte si své odpovědi v podcastu KyberGuru.

SENIOŘI V DIGITÁLNÍM SVĚTĚ: ULEHČEME JIM CESTU K BEZPEČÍ NA INTERNETU

Český statistický úřad v lednu 2024 uvedl, že internet a moderní technologie využívá každý druhý Čech nad 65 let. Oproti roku 2013 jde o více než třetinový nárůst počtu uživatelů v důchodovém věku.

O své zkušenosti se seniory se s posluchači podělí **Aneta Mundok Nitchová,** která pracuje jako vedoucí Senior linky a Poradenského centra organizace Život 90.

Ve dvou epizodách rozhovoru se dozvíte:

- proč starší lidé často tají, že se stali obětí nějakého internetového podvodu,
- jaké typy kyberútoků jsou primárně mířené na seniory a
- jak by vypadal internet, kdyby byl primárně pro lidi důchodového věku?

Naučíte se taky, jak:

- se svými staršími rodiči mluvit o nástrahách internetu,
- trpělivě přistupovat k průběžnému opakování zásad,
- se vypořádat se zděděným kyber-kostlivcem ve skříni.

OTESTUJTE SVÉ ZNALOSTI

Internetoví podvodníci běžně nepoužívají tuto taktiku:

1. Vydávání se za zaměstnance známé firmy.
2. Požadování vzdáleného přístupu k počítači.
3. Posílání fyzických dopisů s žádostí o přístup k bankovnímu účtu.

Bezpečnost na internetu zajistíme seniorům tak, že:

1. Zakážeme jim přístup na všechny webové stránky s výjimkou několika důvěryhodných.
2. Pravidelně jim ukazujeme, jak používat webové služby.
3. Dáme jim seznam nezávadných webových stránek a aplikací, které mohou bezpečně používat.

Jak naučíte svého seniora rozpoznat podvodný e-mail?

1. Doporučím mu, aby ignoroval všechny e-maily od neznámých odesílatelů.
2. Ukážu mu příklady běžných znaků phishingových e-mailů, jako jsou překlepy, naléhavé výzvy k akci a neznámé odkazy.
3. Nainstaluju na jeho počítač blokovací software.

Zkontrolujte si své odpovědi v podcastu KyberGuru.

ZAMĚSTNANCI V PRVNÍ LINII: PREVENCE KYBER-ÚTOKŮ VE FIREMNÍM PROSTŘEDÍ

Až 90 % veškerých kyberútoků na firmy zaviní samotní zaměstnanci. Nejčastěji tak, že kliknou na podvržený odkaz a zpřístupní útočníkům přihlašovací údaje do firemních databází a k dalším citlivým zdrojům.

Vývojář, školitel a šéf bezpečnosti ve společnosti Shoptet **Michal Špaček** mluví bez obalu o tom, jaké chyby dělají firmy při vzdělávání svých zaměstnanců v kyberbezpečnosti.

Ve dvou epizodách rozhovoru se dozvíte:

- proč za většinu kyber-útoků mohou jen a pouze lidé,
- jaké jsou nejčastější chyby, které zaměstnanci dělají,
- jestli je reálné změřit efektivitu vzdělávání v oblasti kybernetické bezpečnosti ještě předtím, než dojde k samotnému útoku?

Naučíte se taky, jak:

- nahradit phishingové testy smysluplnějším přístupem,
- zohlednit různé úrovně znalostí a zkušeností zaměstnanců,
- školit své lidi tak, aby to nebylo „nutné zlo“.

OTESTUJTE SVÉ ZNALOSTI

Co by měl zaměstnanec udělat, pokud si všimne podezřelé aktivity na svém firemním účtu?

1. Ignorovat to a pokračovat v práci.
2. Ihned informovat IT oddělení nebo svého nadřízeného.
3. Pokusit se vyřešit problém sám.

Firemní servery a únik citlivých dat nejčastěji způsobí:

1. neaktualizovaný firewall a antivir
2. lidská chyba
3. slabá hesla

Má smysl testovat ostražitost svých zaměstnanců cvičnými útoky, například podvrženými e-maily se škodlivou přílohou?

1. ano
2. ne
3. jen u nových zaměstnanců

Zkontrolujte si své odpovědi v podcastu KyberGuru.

UMĚLÁ INTELIGENCE: OD SCI-FI K REALITĚ – JAK AI MĚNÍ NÁŠ KAŽDODENNÍ ŽIVOT?

Podle studie Generative AI Research z roku 2023 použilo 49 % dotázaných některý nástroj umělé inteligence aspoň jednou v životě. Třetina z nich dokonce využívá technologii AI denně a plánuje ji používat ještě více.

Přínosy i rizika umělé inteligence rozebírá programátor, bloger a lektor kurzu *Začněte využívat ChatGPT naplno* **David Grudl.**

Ve dvou epizodách rozhovoru se dozvíte:

- kdy se začaly vyvíjet první nástroje umělé inteligence,
- proč by se o AI měl zajímat každý z nás,
- v čem může umělá inteligence pomoci v každodenním životě a jaké má limity?

Naučíte se taky, jak:

- nepodléhat nafouknutým předpovědím o budoucnosti AI,
- vybrat vhodný nástroj umělé inteligence,
- souvisí AI se strojovým učením a automatizací.

OTESTUJTE SVÉ ZNALOSTI

Co je hlavní výhodou využívání umělé inteligence v každodenním životě?

1. zlepšení lidských dovedností
2. automatizace rutinních úkolů a zvýšení efektivity
3. snížení potřeby lidské práce

Jaký je rozdíl mezi strojovým učením a hlubokým učením?

1. Strojové učení využívá složitější algoritmy než hluboké.
2. Hluboké učení je podmnožinou strojového učení, která využívá vícevrstvé neuronové sítě.
3. Strojové učení se používá v průmyslových aplikacích, zatímco hluboké učení v akademických.

Jaké jsou hlavní hrozby spojené s používáním umělé inteligence?

1. ztráta soukromí a bezpečnosti dat
2. zvýšená spotřeba energie
3. neschopnost AI systémů adaptovat se na nové situace

Zkontrolujte si své odpovědi v podcastu KyberGuru.

DALŠÍ VZDĚLÁVACÍ MATERIÁLY KPBI

E-LEARNINGOVÉ KURZY

Doma nebo ve škole si můžete vyzkoušet jakýkoli e-learning zcela zdarma. Nejmenší děti ve věku 6–8 let si můžou vyzkoušet kurz *Surfuj bez nehod* a od podzimu 2024 i sedm nových lekcí o kyberbezpečnosti.

VZDĚLÁVACÍ VIDEOSPOTY

Na YouTube kanálu KPBI na vás čeká přes 60 videí pro seniory, rodiče, děti i širokou veřejnost. Načerpejte nové informace o kyberšikaně, phishingu, internetu věcí nebo o závislosti na mobilu.

PRACOVNÍ LISTY

Přehledné, tematické, barevné, volně ke stažení. Zapojte děti do řešení otázek a zkontrolujte si s nimi správné odpovědi v dolní části pracovního listu.

BLOGOVÉ ČLÁNKY

Na našem webu **www.kpbi.cz** připravujeme sekci s články o novinkách ze světa bezpečného internetu, o rodičovských kyber-patáliích nebo o nakupování kryptoměn.

SOUTĚŽNÍ KVÍZ

Žáci a studenti se mohou každý podzim a zimu zapojit do vzdělávacího online kvízu na téma internetové bezpečnosti. Přesné termíny soutěže uveřejňujeme s předstihem na našem facebookovém a instagramovém profilu KPBI.

KyberGuru

www.kpbi.cz