Kapitola

Ověření znalostí

Projekt: B-SAFE
Číslo: 2018-1CZ01-KA204-048148

Funded by the
Erasmus+ Programme
of the European Union

1. 10 největších internetových hrozeb

V dnešní digitální době je velmi jednoduché získat přístup k internetu a prozkoumat všechna zákoutí virtuálního světa, ve kterém, na rozdíl od toho reálného, je vše snadno dostupné. Internet je prostor plný nových příležitostí a výhod, ale také rizik a hrozeb.

1. Nevhodný obsah

Na internetu se nachází velké množství obsahu, ne všechen je však společensky přijatelný nebo tříděný podle věku či oblasti. Určitý obsah může být nelegální, nevhodný, urážlivý nebo nehodící se pro určité věkové skupiny. Bez dohledu může na nevhodný, znepokojivý nebo explicitní obsah narazit kdokoliv včetně malých dětí.

Spousta webových stránek není zakázána a nikdo na jejich obsah nedohlíží a nespravuje ho. Příklady nevhodného obsahu jsou pornografie, násilný obsah, nebezpečné zboží (jako jsou zbraně), rasismus nebo nenávist, pro-ana stránky (stránky propagující anorexii) nebo jiné stránky s extremistickým obsahem.

2. Krádež dat

Jedná se o zcizení osobních nebo finančních údajů za pomoci počítačů, serverů nebo jiných elektronických zařízení za účelem získání nějakého užitku nebo poškození oběti. Kyberzločinci se mohou zaměřit na banky, společnosti nebo jednotlivce. Jedná se o nezákonné držení citlivých údajů jako jsou nešifrované informace o platebních kartách, údaje o bankovních účtech, hesla, podniková data, obchodní tajemství, duševní vlastnictví, zdrojové kódy, informace o zákaznících nebo záznamy o zaměstnancích.

Kyberzločinci používají k získání přístupu k počítači například spyware, což je program, který jim umožní získat informace o aktivitách na počítači.

3. Krádež identity

Krádež identity je krádež osobních identifikačních údajů za účelem spáchání trestných činů.
Prvním krokem pro pachatele je získání totožnosti cizího počítače. Toho nejčastěji dosáhne krádeží elektronických dat (hesel, přístupových dat atd.), obvykle pomocí neoprávněného kopírování (skimming), podvodným phishingem nebo hackováním.

Druhým krokem je zneužití ukradené identity. Hlavním cílem je většinou nabytí majetku, v některých případech jde zločincům pouze o ublížení či pošpinění jména oběti, například vydáváním se za oběť na sociálních sítích jako je Facebook, v jiných případech jednají za účelem spáchání trestných činů, jako například: zřízení úvěrové linky, pronájem domu, nákup zboží nebo služeb, aukce a mzdové podvody nebo vydírání.

4. Nežádoucí pozornost

Za takovýmto druhem pozornosti může být někdo, kdo je posedlý obětí (kyberstalking) nebo někdo, kdo chce oběti ublížit (kyberšikana).

Kyberstalking je chorobná posedlost osobou odehrávající se na internetu. Probíhá prostřednictvím online technologií jako jsou e-mail, sociální sítě, chatovací místnosti nebo za využití osobních údajů dostupných na internetu a čehokoliv dalšího, co lze na internetu o oběti dohledat a co může kyberstalker použít k zprostředkování kontaktu se svou obětí. Mezi typické chování kyberstalkerů patří sledování online aktivit oběti, chorobná snaha získat informace a osobní údaje oběti, sledování oběti prostřednictvím internetu bez jejího vědomí, nepřetržité telefonování a zasílání zpráv, manipulace a využití dalších prostředků, jak oběť nečekaně kontaktovat.

Kyberšikana je trestný čin páchaný prostřednictvím sociálních sítí a internetu za účelem zastrašovat, obtěžovat, vyhrožovat nebo shazovat druhé.

5. Triky a podvody

Jedním z typů podvodného chování na internetu je phishing. Jedná se o rozesílání podvodných zpráv, nejčastěji prostřednictvím e-mailu, které se zdají být od důvěryhodného zdroje.

Tyto zprávy mohou obsahovat malware (spyware, ransomware, počítačové viry nebo červy), buď v podobě odkazu nebo přílohy e-mailu, který po rozkliknutí nainstaluje do počítače škodlivý software.

6. Nežádoucí informace

Při brouzdání po internetu můžeme narazit na obsah a informace, které jsou falešné nebo které jsme ani najít nechtěli. **Na internetu se nachází velké množství falešných a zavádějících informací, se kterými se můžete setkat buď náhodou, nebo v souvislosti s něčím, co jste hledali.**

Nejrozšířenějším komunikačním prostředkem na internetu je e-mail. Většina lidí používá e-mail každý den, a proto je také jeden z nejoblíbenějších prostředků pro šíření spamu. Falešné e-maily jsou častým rizikem, k rozesílání lživých informací však může dojít i na sociálních sítích nebo na různých webových stránkách.

Falešné zprávy je možné najít kdekoliv ne pouze na e-mailu. Sociální sítě jsou běžným místem, kde se můžete setkat s falešnými zprávami nebo falešnými profily.

7. Snadné šíření a dlouhá životnost

Obsah v podobě zpráv nebo fotografií může sdílet kdokoliv, kdekoliv a kdykoliv. Je důležité si uvědomit, že když už se jednou rozhodnete něco přidat, zůstane tento obsah na internetu navždy. Proto je velmi důležité být opatrní a pečlivě promyslet, co se rozhodnete sdílet.

Obsah na internetu se šíří velmi rychle a může během krátké chvíle obletět celý svět.

8. Ničení nebo úprava dat

Důležitá data v zařízení mohou být předem smazána nebo upravena tak, aby uškodila budoucímu majiteli.

K tomu může dojít za pomoci počítačových virů, což jsou programy speciálně navržené k tomu, aby napadaly jiné programy, ničily důležitá systémová data a znefunkčnily sítě. Dalším takovým příkladem je třeba trojský kůň, což je program, který se dostane do systému nebo počítače přestrojený za běžný software a jehož cílem je způsobit škody na systémových procesech, datech na pevném disku atd.

9. Znefunkčnění zařízení

Operační systém zařízení může být také napaden trojským koněm. Trojský kůň se nejčastěji dostane do počítače prostřednictvím přílohy e-mailu a získá přístup k Vašemu počítači nebo systému.

10. Kyberterorismus

Kyberterorismus je závažnější druh trestné činnosti prováděné v kyberprostoru.

Jedná se o kybernetický útok, jehož cílem je vyvolat strach nebo zastrašit společnost nějakým ideologickým cílem. Zločinci využívají počítače nebo komunikační sítě k ničivým procesům a vyvolání rozruchu.

2. 10 nejdůležitějších pravidel bezpečného chování na internetu

1. Hesla

Většina internetových služeb je chráněna přístupovým kódem, který má zajistit ochranu soukromí informací uživatelů. Pokud je heslo jednoduché nebo velmi časté (hodně používané mezi uživateli), není problém jej uhádnout a získat neoprávněný přístup k cizímu účtu. Proto se doporučuje používat silná hesla, která mají minimálně 8 znaků, obsahují jak písmena (malá i velká), tak čísla a jiné speciální znaky. Vaše hesla by neměla obsahovat osobní údaje jako rodné číslo, jména rodinných příslušníků nebo známých a už vůbec ne jednoduché fráze nebo slova. Pro lepší zabezpečení je doporučeno pravidelně hesla měnit. Hesla byste nikdy neměli uchovávat v zápisnících nebo nešifrovaných souborech.

2. Bezpečnostní technologie

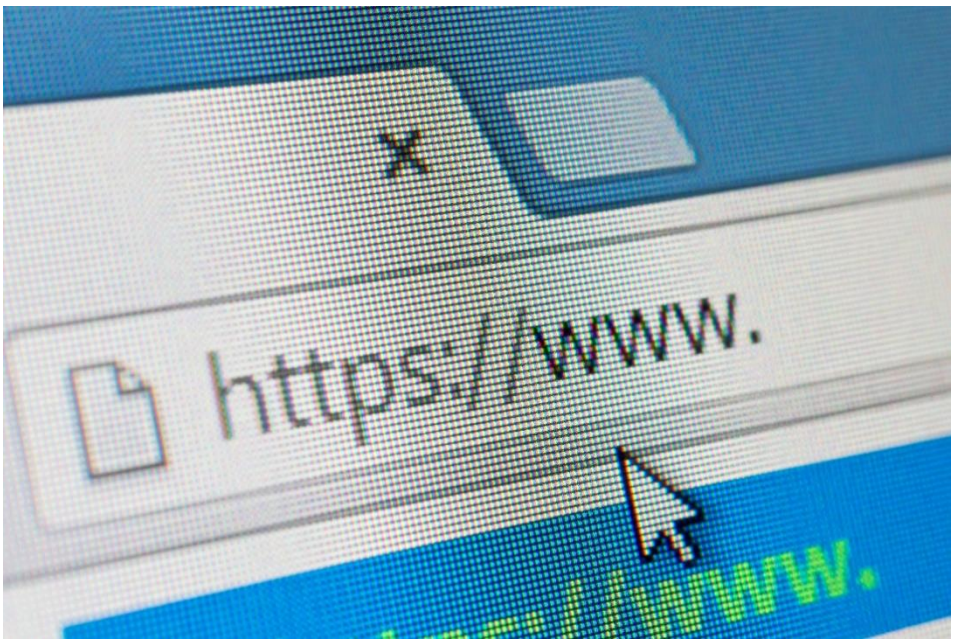
Vytvořte si několik záloh svých nejdůležitějších dat a neukládejte je všechny pouze na jedno místo. Vždy mějte staženou nejnovější aktualizaci softwaru. Nainstalujte si phishingový filtr či program na e-mail nebo webový prohlížeč.

Antivirový program, firewall a antispam jsou nejúčinnější způsoby, jak ochránit svůj počítač před všemožnými riziky, která se na internetu nacházejí. Používání těchto technologií podstatně snižuje riziko napadení a hrozeb. Provádějte pravidelně antivirové kontroly a ujistěte se, že Váš antivir a anti-spyware jsou kompatibilní.

3. Důvěryhodné webové stránky

Plno webových stránek používá k propagaci svých služeb techniky sociálního inženýrství, které využívají informace, jenž mají za úkol přilákat pozornost uživatelů, jako jsou slevy na nákup zboží (nebo dokonce nabídky zboží zdarma), žhavé novinky nebo exkluzivní zprávy a multimediální materiál atd. Abyste mohli bezpečně surfovat po internetu, je potřeba o těchto taktikách vědět a vyvarovat se návštěvě stránek s podobných obsahem.

Ověřte si SSL protokol webové stránky a **nikdy nezadávejte své osobní údaje** na stránce, která nemá platný SSL certifikát. Pro ověření klikněte na visací zámek vedle vyhledávacího řádku.



Pomocí Black Hat SEO technik pachatelé často povýší svou webovou stránku na první místa mezi výsledky vyhledávání, obzvlášť pokud obsahují široce užívaná klíčová slova, jako jsou aktuální aféry, výstřední zprávy a oblíbená témata (jako jsou sport nebo sex). Uživatel si při vyhledávání musí dávat pozor, na co kliká a ověřit si bezpečnost webových stránek.

Pokud si nepřejete na internetu zanechat svoji stopu, nejlépe tak učiníte využitím VPN (virtuální privátní síť) nebo proxy serveru, který funguje jako komunikační prostředník mezi Vámi a webem, který chcete navštívit.

4. Sdílení informací

Všechny informace a fotografie, které se rozhodneme na internet přidat, za námi vytvářejí digitální stopu, která tvoří naši digitální identitu. Proto je důležité dávat si pozor na to, co přidáváme a zda souhlasíme s tím, aby tyto informace byly dostupné všem.

Nepovolujte aplikacím přístup k Vaší poloze, kameře nebo mikrofonu a vyvarujte se uveřejňování nepotřebných informací. Nepovolujte zobrazení polohy u Vašich příspěvků.

Při používání sociálních sítí a aplikací pro odesílání rychlých zpráv byste měli přijímat a komunikovat pouze s lidmi, které znáte. Tímto se vyhnete nevyžádaným zprávám od útočníků, jejichž cílem je rozesílání malwaru, phishing, kyberšikana a další.

5. Veřejné Wi-Fi sítě

Pokud používáte veřejnou Wi-Fi síť k návštěvě běžných stránek, riziko napadení je minimální. Je však důležité vyhnout se na veřejných sítích navštěvování stránek, které po Vás požadují zadávání osobních údajů, jako jsou hesla nebo přihlašovací jména. Veřejná síť by se mohla stát terčem útočníků a Vy byste tak mohli přijít o cenné údaje. Stejný pozor byste si měli dávat i při používání známých sítí.

6. Podezřelé odkazy

Jedny z nejpoužívanějších způsobů, jak nalákat oběti na škodlivé stránky, jsou hypertextové odkazy. Vyvarujte se otevírání podezřelých odkazů a vyhněte se tak riziku napadení. Tyto odkazy Vám mohou přijít prostřednictvím e-mailu, chatovacích místností nebo zpráv na sociálních sítích. Důležité je analyzovat, zda se k tomuto odkazu vztahuje nějaká podezřelá situace (např. pozvánka k rozkliknutí fotografie napsaná v cizím jazyce), zda přišel od neznámé osoby nebo zda odkazuje na nedůvěryhodnou stránku.

7. Stahování souborů

K narušení bezpečnosti nejčastěji dochází při stahování souborů. Pokud si nejste stoprocentně jisti nezávadností, soubor či program nestahujte nebo proveďte důkladný průzkum ohledně toho, zda je jeho stažení bezpečné. Spousta webových stránek nabízí známé programy, které jsou ve skutečnosti pozměněné, upravené nebo nahrazené verzí, která obsahuje malware, a stažením takového programu dojde k zamoření počítače uživatele. Proto se doporučuje vždy stahovat programy a aplikace pouze z ověřených oficiálních zdrojů.

K šíření malwaru většinou dochází prostřednictvím spustitelných souborů. Z toho důvodu je dobré nespouštět soubory, jejichž bezpečností si nejste jisti a které nepocházejí od spolehlivého zdroje (zda pochází z chatovací místnosti, e-mailu nebo webové stránky).

8. Aktualizace operačního systému a aplikací

Správná a pravidelná aktualizace operačního systému (Windows, Linux, iOS...) a aplikací je jeden z předních způsobů, jak zabránit útočníkům v získání přístupu k Vašemu zařízení a jeho následného zneužití. Počítačové aktualizace sice většinou zaberou spoustu času a někdy vyžadují restart zařízení, jsou však nezbytné pro opravu slabin v zabezpečení softwaru.

Nezapomeňte tato stejná preventivní opatření uplatnit kromě Vašeho počítače a notebooku také na Váš mobilní telefon. Pro útočníky je snazší dostat se přes zabezpečení operačního systému ve Vašem chytrém telefonu než v počítači.

9. Nezadávejte osobní údaje do pochybných formulářů

Pokud se na internetu setkáte s formulářem, který po Vás požaduje zadání Vašich osobních údajů (např. uživatelské jméno a heslo), měli byste si nejdřív ověřit poctivost stránky, na které se nachází. Nejlépe uděláte, pokud zkontrolujete doménu stránky a https protokol, které Vám zaručí zachování důvěrnosti Vašich údajů. Tímto způsobem lze předejít phishingovým útokům, které se zaměřují na získávání citlivých údajů vydáváním se za důvěryhodnou stránku.

10. Soubory cookie

Soubor cookie je soubor vytvořený konkrétní webovou stránkou, který obsahuje malé množství informací, které se pohybují mezi odesílatelem a příjemcem a mají za úkol zjistit preference uživatele a usnadnit jeho počínání na webu. Tyto sdílené informace se však mohou dostat do rukou třetí strany, a proto je vhodné zvážit povolení jejich přenosu. Pokud jste jejich přenos však měli povolen, ničeho se nebojte, soubory cookie můžete z prohlížeče kdykoliv vymazat.

Procvičte si znalosti

Počítačová kriminalita

1. Co je to počítačová kriminalita?

Úkol: Vyberte správné odpovědi: správných odpovědí může být více.

a) Počítačová kriminalita je prohlížení nevhodného obsahu na internetu.
b) Počítačová kriminalita je nezákonný čin, při kterém je počítač použit jako nástroj nebo terč, případně jako obojí.
c) Počítačová kriminalita je čin, při kterém zaměstnavatel sleduje e-maily svých zaměstnanců.
d) Počítačová kriminalita je získávání veřejných informací na internetu.

2. Ve které z následujících situací dochází k phishingu?

Úkol: Vyberte správné odpovědi: správných odpovědí může být více.

a) Obdrželi jste e-mail s oznámením, že jste vyhráli nový iPhone a abyste výhru dostali, musíte zaslat své osobní údaje.
b) Obdrželi jste e-mail s výhodnou nabídkou na nákup nějakého zboží.
c) Obdrželi jste e-mail, ve kterém Vás banka žádá o změnu hesla. V e-mailu se přímo nachází odkaz na stránku.
d) Obdrželi jste e-mail s informacemi o kulturní akci ve Vašem městě.

3. Ano či ne?

Hacking lze v některých případech považovat za přínosnou a užitečnou činnost.

A □ **N** □

4. K vynechaným místům v textu přiřaďte správné možnosti – správné odpovědi můžete do textu dosadit kliknutím a přetažením.

_____ je zcizení osobních identifikačních údajů za účelem spáchání trestných činů, jako například: zřízení úvěrové linky, pronájem domu, nákup zboží nebo služeb, aukce a mzdové podvody nebo vydírání.

_____ se vyznačuje neustálým kontaktem se zaměřenou osobou – jejím urážením a pomlouváním. Útočník například vytvoří na Facebooku skupinu s názvem "Nenávidím…" a pozve všechny své přátele, aby se připojili.

_____ jsou aktivity, které nečestně vytvářejí bohatství pro zapojené osoby. Jedná se o využívání důvěrných informací nebo podvodné nabývání majetku jiné osoby za účelem zajištění hmotného prospěchu. Patří sem například

_____ je posedlost vyznačující se snahou dozvědět se co nejvíc informací o určité osobě bez jejího vědomí. Útočník například zjistí, kde se oběť narodila, s kým je v manželském svazku atd.
Kyberšikana; Kyberstalking; Krádež identity; Finanční kriminalita

5. Na vynechaná místa v textu doplňte vhodné výrazy.

Kybernetický útok, při kterém je využíván nebo zneužíván počítač či komunikační síť za účelem zničení nebo narušení, které má vyvolat strach nebo zastrašit společnost v ideologický cíl, se nazývá (_____).

Ochrana před nevhodným obsahem

1. K vynechaným místům v textu přiřaďte správné možnosti – správné odpovědi můžete do textu dosadit kliknutím a přetažením.

_____ je charakterizována jako explicitní popis nebo vyobrazení, jehož účelem je podnítit sexuální pud.
_____ propagace a podněcování nenávisti vůči jednotlivcům nebo skupinám na základě jejich rasy, národnosti, náboženství, zdravotního postižení, věku, sexuální orientace, pohlaví, genderové identity a dalších.
_____ jsou stránky, které považují anorexii za životní styl, nikoliv za nemoc.

_____ se na první pohled zdají být neškodné a často lidem poskytují zajímavé informace např. o různých historických událostech. Zmíněná fakta však bývají zkreslená a odkazují na zdroje, ve kterých jsou informace ovlivněny zvráceným pohledem na svět.

Rasismus nebo nenávist; Pornografie; Pro-ana webové stránky; Stránky s extremistickým obsahem

2. Který typ ohodnocení se zaměřuje na stránky s nevhodným obsahem?
Úkol: Vyberte správné odpovědi: správných odpovědí může být více.
a) Filmový rating MPAA (např. PG)
b) LT Int. Scale (např. LT Corporate Family ratings)
c) National Scale (např. NSR)
d) Online PEGI hodnocení (např. PEGI 7)

3. Který z následujících nástrojů je vhodný jako rodičovská kontrola pro obsah na internetu?
Úkol: Vyberte správné odpovědi: správných odpovědí může být více.
a) Protection online app
b) iWebfilter
c) K10 Web Protection
d) Anti-game

4. Osvojení kterých dovedností je u dětí nezbytné pro snížení rizika setkání se s nevhodným obsahem na internetu?

Úkol: Vyberte správné odpovědi: správných odpovědí může být více.

a) IT dovednosti
b) Kritické myšlení a odolnost
c) Digitální dovednosti
d) Pozitivní přístup k užívání technologií

5. K vynechaným místům v textu přiřaďte správné možnosti.

Nástroje ochrany jako jsou různá zákonná opatření, rodičovská kontrola, softwary a podpůrné instituce jsou užitečnou prevencí, klíčová je však vzájemná _____ mezi Vámi a Vaším dítětem.

domluva; důvěra; diskuze; řeč; komunikace

Ochrana osobních údajů

1. K vynechaným místům v textu přiřaďte správné možnosti

_____, známá také jako ochrana informací, je aspektem bezpečnosti údajů, který se zabývá řádným nakládáním s _____. Jedná se především o ochranu osobních údajů jednotlivců před _____. _____ osobních údajů je v Evropě po léta _____ právem. V posledních letech se však v praxi stala ochrana dat ještě důležitější. _____ a _____ usnadňují sběr, zpracování, ukládání, šíření a analýzu dat. _____ je právně závazné nařízení o ochraně fyzických osob v souvislosti se zpracováním osobních údajů.

zneužitím; technický pokrok; GDPR; základním; ochrana osobních údajů; osobními údaji; ochrana; globální vytváření sítí

2. Ano či ne?

GDPR se vztahuje pouze na automatické zpracování dat.

A □ N □

Osobními údaji se myslí citlivé údaje o nějaké osobě.

A □ N □

Důležitost ochrany citlivých údajů neustále roste.

A □ N □

Mezi osobní údaje patří například jméno, datum narození, věk, adresa bydliště nebo číslo bankovního účtu.

A □ N □

Mezi citlivé údaje patří například číslo kreditní karty, náboženské vyznání, členství v odborech nebo etnický původ.

A □ N □

3. K vynechaným místům v textu přiřaďte správné možnosti.

GDPR definuje _____ klíčových principů, které musí být při _____ striktně dodržovány. Porušení těchto zásad pravděpodobně povede k _____. U _____ osobních údajů má GDPR k dispozici celkem _____ zákonných podkladů pro zpracování, protože zpracování _____ je obecně zakázáno, pokud nejsou splněny zvláštní podmínky. Na zpracování _____ se vztahují zvláštní požadavky. Zpracování dat je povoleno pouze v specifických _____.

zpracování dat; sedm; necitlivých; šest; maximálním pokutám; osobních údajů; citlivých údajů; výjimečných případech

4. Která tvrzení týkající se narušení dat jsou pravdivá?

Úkol: Vyberte správné odpovědi: správných odpovědí může být více.

a. Povinností správce dat je ihned nahlásit zpracovateli dat jakékoliv narušení.

b. Pokud dojde k narušení dat, správce dat musí splnit ohlašovací a oznamovací povinnost.
c. Pokud dojde k narušení dat, zpracovatel dat musí splnit ohlašovací a oznamovací povinnost.
d. Orgán pro ochranu údajů musí být o narušení informován do 24 hodin.
e. Orgán pro ochranu údajů musí být o narušení informován do 72 hodin.
f. Orgán pro ochranu údajů musí být o narušení obeznámen, pokud by představovalo riziko pro práva a svobody subjektu údajů.
g. Dodatečné oznámení subjektům údajů není vždy nezbytné, pokud existuje vysoké riziko ohrožení práv a svobod subjektů údajů.

5. K vynechaným místům v textu přiřaďte správné možnosti

V zájmu zajištění ochrany _____ hraje otázka _____ ústřední roli. Důležitými klíčovými slovy v této souvislosti jsou _____ a _____. Termínem _____ se rozumí ochrana údajů prostřednictvím _____. To znamená, že již při vývoji nových technologií musí být zajištěna vhodná řešení v souladu s ochranou údajů. _____ znamená ochrana údajů prostřednictvím příslušného _____. Odpovědná osoba musí pomocí vhodného výchozího nastavení zajistit, aby byly zpracovávány pouze ty _____, které jsou naprosto nezbytné.

osobních údajů; bezpečnosti údajů, osobní údaje; ”privacy by design” (tzv. záměrná ochrana osobních údajů); privacy by design; ”privacy by default” (“ochrana osobních údajů ve výchozím nastavení”); technologického návrhu; privacy by default; výchozího nastavení

Bezpečnost používání chytrých telefonů

1. Jaká preventivní opatření pro ochranu Vašeho chytrého telefonu byste měli zavést v případě, že dojde k jeho ztrátě či krádeži?

Úkol: Vyberte správné odpovědi: správných odpovědí může být více.

a. Používejte PIN kód a zámek obrazovky.
b. Pro PIN použijte běžnou číselnou kombinaci, abyste si ho jednodušeji zapamatovali.
c. Poznamenejte si sériové číslo Vašeho chytrého telefonu.
d. Neinstalujte si aplikace proti krádeži.

2. Jaká tvrzení týkající se IM (Instant Messaging) jsou pravdivá?

Úkol: Vyberte správné odpovědi: správných odpovědí může být více.

a. IM je služba pro offline chatování.
b. IM je služba pro online chatování prostřednictvím mobilních aplikací.
c. Přenos zpráv probíhá v rámci tzv. pull procedury.
d. IM slouží pouze pro přenos textových zpráv.
e. Mezi IM patří například WhatsApp, Skype nebo Facebook Messenger.

3. Většina IM aplikací je zdarma. Jaká rizika z této skutečnosti plynou?

Úkol: Vyberte správné odpovědi: správných odpovědí může být více.

a. Aplikace po Vás bude platbu požadovat později, což bude mít za následek vysoké náklady.
b. Vaše data se stanou produktem aplikace.
c. Komunikace je většinou šifrovaná.
d. V aplikaci se skrývají všemožné druhy malwaru.

4. Ano či ne?

Neomezená oprávnění aplikace nepředstavují žádný problém.

A □ N □

Vývojáři aplikací mají zájem o Vaše osobní údaje.

A □ N □

Veškerý přístup, který má aplikace k Vašim osobním údajům, je viditelný v nastavení oprávnění dané aplikace.

A □ N □

Důležitost ochrany osobních údajů v souvislosti s užíváním IM a jiných aplikací neustále roste.

A □ N □

Při používání IM existuje riziko phishingových útoků.

A □ N □

Nešifrovaná komunikace nepředstavuje žádné riziko.

A □ N □

5. K vynechaným místům v textu přiřaďte správné možnosti.

Vzhledem k možným _____ spojeným s používáním aplikací Vás pravděpodobně zajímá, jak můžete lépe chránit sebe a své soukromí. Zde je několik tipů, na co si při používání aplikací dávat pozor: vždy používejte _____ verzi aplikace, jako profilové obrázky _____ obrázky, které nevlastníte, před stažením aplikace si pozorně si přečtěte _____, zadejte pouze _____ údaje, použijte _____, která toho o Vás moc neprozradí a nebude Vás obtěžovat se spamy, zkontrolujte _____ práva aplikace a v případě potřeby je upravte, upravte _____ (např. to, kdo uvidí Váš profilový obrázek) a _____ si uživatele, které neznáte.

zablokujte; bezpečnostním rizikům; nepoužívejte; nejnovější; přístupová; zásady ochrany osobních údajů; nastavení soukromí aplikací; nenutnější; zvláštní e-mailovou adresu

Informační tok/Komunikace na internetu

1. Nejužívanějším prostředkem pro online komunikaci je:

Úkol: Vyberte správné odpovědi: správných odpovědí může být více.

a) Instant messaging
b) E-mail
c) Webové stránky

2. K vynechaným místům v textu přiřaďte správné možnosti.

_____ je nežádoucí e-mail, který má za cíl oklamat Vás podvodnými informacemi nebo navést k provedení nějakého nevhodného činu. Často jsou prostřednictvím _____ těchto e-mailů rozesílány škodlivé programy. Je tedy velmi důležité znát typické znaky škodlivých e-mailů. Předtím než otevřete přílohu, rozkliknete odkaz nebo odpovíte na e-mail, zeptejte se sami sebe: je nabídka _____ (příliš dobrá na to, aby byla opravdová, odpovídá obsah e-mailu údajnému _____, obsahuje e-mail určitá _____ slova (například "poslední výzva", "účet zablokován"), žádá Vás odesílatel o sdělení _____, přijde Vám na _____ něco zvláštního, nachází se v e-mailu plno pravopisných či gramatických _____, byl e-mail automaticky přesunut do _____, jste vyzváni k spuštění programu s podivným _____ (např. složeniny známých formátů jako "jpg.vbs" nebo "gif.exe").

chyb; příloh; složky spamu; falešný e-mail; popudlivá; nereálná, odesílateli; důvěrných informací; odesílateli; formátováním

3. Jak fóra, tak chatovací místnosti jsou známé a oblíbené způsoby online komunikace a výměny informací. Vyberte, která tvrzení o těchto platformách jsou pravdivá.

Úkol: Vyberte správné odpovědi: správných odpovědí může být více.

a) Fóra jsou vhodnější pro komunikaci v reálném čase.

b) Chatovací místnosti jsou vhodnější pro komunikaci v reálném čase.
c) Fóra jsou vhodnější pro diskuze, při kterých nemusí být všichni zúčastnění online ve stejnou dobu.
d) Chatovací místnosti jsou vhodnější pro diskuze, při kterých nemusí být všichni zúčastnění online ve stejnou dobu.
e) Fóra jsou lépe organizovaná.
f) Chatovací místnosti jsou lépe organizované.
g) Pouze při registraci do fóra je požadovaná platná e-mailová adresa.
h) Chatovací místnosti a fóra umožňují uživatelům výměnu textových zpráv a ve většině případů i výměnu fotografií, videí, odkazů nebo souborů.

4. Jaká rizika plynou z užívání fór a chatovacích místností?

Úkol: Vyberte správné odpovědi: správných odpovědí může být více.

a) Falešné identity
b) Malware
c) Vysoké poplatky
d) Odkazy na stránky obsahující phishing
e) Nešifrovaná komunikace
f) Šifrovaná komunikace

5. K vynechaným místům v textu přiřaďte správné možnosti

Navozený pocit anonymity při užívání sociálních sítí může vést k lehkomyslnému zacházení s _____ a _____. To má za následek větší zranitelnosti sociálních sítí a jejich uživatelů a oblibu _____ se na ně zaměřovat. Zvláště rizika jako oklamání _____ nebo vědomé či nevědomé šíření _____ jsou velmi častá. Proto byste měli při užívání _____ brát v úvahu tyto body: nikdy nerozebírejte _____ či _____ informace na veřejných místech na internetu, pomocí dostupných _____ upravte, kdo má přístup k Vašim informacím, buďte kritičtí při _____ žádostí o přátelství, vždy zkontrolujte nastavení _____ na sociálních sítích a dávejte si pozor na _____ informace.
Pokud se setkáte s nevhodným užíváním sociálních sítí nebo nevhodným chováním na nich, můžete a měli byste tento nález _____ poskytovateli služby nebo jiným příslušným _____.

nepravdivých informací; sociálních sítí; důvěrné; údaji; útočníků; zavádějící; nahlásit; falešnou identitou; informacemi; orgánům; ochrany soukromí; přijímání; osobní; filtrů

Rodičovská kontrola

1. Jakým následkům čelí oběť sextingu?

Úkol: Vyberte správné odpovědi: správných odpovědí může být více.

a) Ponížení a sociální lynčování.
b) Veřejné ponížení a urážky, což může mít vliv hlavně na mladší osoby, jejichž osobnost se stále formuje, a to, jak je vidí druzí, je pro ně v tomto věku velmi důležité.
c) Pocity bezmoci či viny, hlavně pokud se o skutečnosti dozví rodiče nebo učitelé.
d) Pro oběť žádné následky neplynou.

2. K vynechaným místům v textu přiřaďte správné možnosti.

Grooming je definován jako _____, kterou záměrně provádí _____ osoba za účelem navázání vztahu a získání emoční kontroly nad dítětem či mladistvým. Hlavním cílem predátora je _____. Ke groomingu může docházet i mezi dvěma nezletilými osobami, ve většině případů je mezi nimi větší věkový rozdíl a _____ je starší z dvojice. Hlavním cílem predátora je získat důvěru _____, přimět ji k pořízení a zaslání fotografií či videí se _____ obsahem nebo se s ní dokonce setkat.

dospělá; kyberšikana; sexuálním; sexuální zneužívání; nezletilé osoby; predátorem

3. K vynechaným místům v textu přiřaďte správné možnosti

Jedním z prvních kroků _____ je urážení či vyhrožování _____ útočníkem, který hrozí tím, že vyzradí informace, které by mohly _____ její _____. V tomto případě není až tak důležité, zda jsou informace pravdivé, útočník je ve snaze uškodit oběti tak či tak vypustí do světa. Pokud informace nejsou pravdivé, jedná se o _____.

reputaci; dezinformaci; kyberšikany; oběti; poškodit

4. K vynechaným místům v textu přiřaďte správné možnosti

Účinným způsobem, jak rozpoznat _____ na internetu, je analyzovat, kolik času _____ na _____ tráví, jak často je připojená a jaké jsou její _____ projevy a chování, pokud zrovna na internetu není. Jestli se zdá být nervózní, rozrušená, úzkostná nebo dokonce v depresích nebo jestli u ní dochází k častým výkyvům _____, může být na vině _____.

nezletilá osoba; emoční; nálad; internetu; netolismus; závislost

5. K vynechaným místům v textu přiřaďte správné možnosti

Existuje několik metod, pomocí kterých se útočníci bez Vašeho vědomí dostanou k Vašim _____ a následně je vypustí do světa. Často se tyto _____ skrývají pod běžnými požadavky různých služeb na internetu, např. reklamy, které Vás žádají o zadání informací, kvůli vizualizaci dat, nebo _____ služby, které Vás pro přístup žádají o zadání _____. Ve velkém množství případů však k úniku dat dochází kvůli lehkomyslnosti _____, kteří si možné nástrahy _____ světa neuvědomují.

hesla; internetové; mladistvých; datům; metody; online

Hardware a software

1. *K vynechaným místům v textu přiřaďte správné možnosti*

Pojem hardware označuje _____ části počítače. Mezi příklady počítačového hardwaru patří _____, _____ a _____. Software představuje _____ počítače. Jedná se o soubor pokynů, které říkají hardwaru, jakým způsobem vykonávat určité funkce. Software je za využití jednoho hardwaru schopný vykonávat velké množství _____.

monitor; klávesnice; fyzické; programy nebo aplikace; myš; úkolů

2. *Jaká opatření Vám pomohou se zabezpečením softwaru? (více možností – pouze jedna odpověď není správná)*

a) Pravidelné aktualizace softwaru
b) Vytvoření několika záloh
c) Neinstalování softwarových firewallů
d) Šifrování informací

3. *Jednou z možností zabezpečení hardwaru je vyhnout se kupování komponentů od pochybných zdrojů. (rozhodněte, zda je uvedené tvrzení pravdivé či nikoliv).*

a) Ano
b) Ne

4. *Jaká opatření je možno zavést pro lepší zabezpečení softwaru? (více možností – pouze jedna odpověď není správná)*

a) Nainstalovat antivirový program a pravidelně ho aktualizovat.
b) Udělat průzkum o nástrojích zabezpečení, které chcete stáhnout.
c) Jednou za čas aktualizovat operační systém.
d) Zakázat sdílení souborů a médií, pokud je nepotřebujete.

5. *Které útoky na hardware jsou nejčastější? (více možností – pouze jedna odpověď není správně)*

a) Fyzické nehody
b) Modding
c) Trojský kůň
d) Phishing

Osobní údaje na sociálních sítích

1. Na co byste si měli dávat pozor při používání sociálních sítí? (více možností – vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně)

a) Pokud Vás odkaz přesměruje na stránku, kterou si nejste jisti, zkontrolujte, zda se na ní nachází poštovní adresa a kontaktní údaje.
b) Ujistěte se, že je na stránce uveden reklamační řád a informace o dopravě.
c) Pokud Vás požádá o přátelství někdo, koho neznáte, ověřte si pravost profilu zpětným vyhledáváním profilového obrázku
d) Abyste se vyhnuli phishingovému útoku, zkontrolujte celou URL adresu odkazu

2. K vynechaným místům v textu přiřaďte správné odpovědi – správné odpovědi můžete do textu dosadit kliknutím a přetažením.

Většina webových stránek umožňuje upravit přístupnost informací z veřejných na soukromé pomocí funkce _____.

Za to, jakým způsobem jsou shromažďovány nebo prezentovány osobní údaje, zodpovídá _____ konkrétní sociální sítě.

_____ je nejčastějším způsobem, jak nalákat a poškodit uživatele sociálních sítí.
vlastník/poskytovatel; phishingový útok; nastavení soukromí

3. Která z těchto tvrzení se vztahují na sociální sítě? (více možností – pouze jedna odpověď není správná)

a) Interaktivní
b) Usnadňují sdílení informací, nápadů, kariérních zájmů a dalších způsobů osobního vyjádření.
c) Propojení mezi dvěma a více lidmi.
d) Více než 4 miliardy aktivních uživatelů.

4. Jaká jsou nejčastější rizika sociálních sítí? *(více možností – pouze jedna odpověď není správná)*

a) Software, který pomocí šifrování odepře uživateli přístup k jeho datům, jako jsou fotografie nebo dokumenty, dokud nedojde k zaplacení výkupného.
b) Druh škodlivého kódu nebo softwaru, který na první pohled vypadá věrohodně, ale dokáže převzít kontrolu nad Vaším počítačem.
c) Druh malwaru, který se dokáže kopírováním sám množit a šířit na další počítače.
d) Druh malwaru, který způsobuje fyzické škody na počítači.

5. Jaká opatření můžete zavést, abyste byli vždy jeden krok napřed před kyberzločinci? (více možností – pouze jedna odpověď není správná)

a) Neukládejte si své přihlašovací údaje v zařízeních/prohlížeči/aplikacích.
b) Vyvarujte se sdílení osobních informací na internetu.
c) Vždy mějte staženou nejnovější verzi Vašeho bezpečnostního programu.
d) Zkontrolujte si nastavení soukromí.

Kybernetická bezpečnost

1. *Co je to kybernetická bezpečnost? (více možností – pouze jedna odpověď není správná)*

a) Prevence a rozpoznání digitálních útoků, ochrana systémů, hardwaru a softwaru.
b) Ochrana počítačů, serverů, mobilních zařízení, elektronických systémů, sítí a dat před škodlivými útoky.
c) Pouze zabezpečení softwaru a hardwaru.
d) Metody ochrany počítačů, sítí, programů a dat před útoky nebo získáním neoprávněného přístupu, jejichž účelem je zneužití zařízení.

2. *Jaká opatření lze zavést za účelem zlepšení kybernetické bezpečnosti? (více možností – pouze jedna odpověď není správná)*

a) Užívání odlišných hesel pro různé účty a profily.
b) Hesla by měla být jednou za čas obměňována a měla by obsahovat velká i malá písmena, čísla a speciální znaky.
c) Uložení hesla v tabulkovém procesoru v počítači.
d) Užívání vícefaktorové autentizace (pokud je to možné) pro různé účty na internetu.

3. *Jaká preventivní opatření lze použít při nakupování na internetu? (více možností – pouze jedna odpověď není správná)*

a) Přečtěte si recenze a zjistěte, zda měli předchozí zákazníci positivní nebo negativní zážitek z nakupování na konkrétní stránce.
b) Vytvořte si virtuální kreditní karty.
c) Mějte svůj antivirový program, antispyware a firewall neustále aktualizovaný.

d) Je zbytečné číst všeobecné podmínky různých webových stránek, protože jsou si všechny velmi podobné.

4. *Vyberte správné možnosti týkající se definice a využití cloud computingu. (více možností – pouze jedna odpověď není správná)*

a) Využití sítě na vzdáleném serveru provozovaném na internetu namísto lokálního serveru nebo osobního počítače.
b) Poskytování různých služeb na internetu včetně serverů, úložišť, databází, sítí, softwarů nebo analytik.
c) Existuje pouze jeden druh cloud computingového řešení.
d) Cloud computing lze provozovat bez lidského přičinění.

5. *Pomocí jakých opatření lze cloud computing vylepšit? (více možností – pouze jedna odpověď není správná)*

a) Používejte vícefaktorovou autentizaci.
b) Nastavte různé stupně oprávnění přístupu k informacím podle toho, které informace potřebují konkrétní lidé znát.
c) Zajistěte školení týkající se ochrany dat a soukromých informací.
d) Jednou za čas proveďte zálohu dat a informací.

Internet věcí

1. Která z následujících tvrzení týkajících se IoT jsou pravdivá? (více možností – vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně)

a) Díky IoT bude v budoucnu možno vylepšit veřejnou dopravu.
b) IoT přetváří fyzické objekty v ekosystémy informací, které jsou sdíleny mezi nositelnými, přenosnými, a dokonce implantovatelnými zařízeními a které mají za úkol obohatit naše životy, technologie a data.
c) Existuje velké množství IoT obchodních aplikací.
d) Chytrá auta, nositelná fitness a sledovací zařízení, hlasoví asistenti jsou všechno příklady IoT technologií.

2. Vyberte správná tvrzení týkající se internetu věcí (více možností – pouze jedna odpověď není správná)

a) IoT technologie lze použít pouze na lidech, domácnostech a v automobilovém průmyslu.
b) Jedná se o systém vzájemně propojených zařízení a mechanických a digitálních strojů.
c) Jedná se o sbližování několika technologií, analytik v reálném čase, strojového učení, komoditních senzorů a vestavěných systémů.
d) Pojem IoT zahrnuje vše, co nějakým způsobem souvisí s internetem.

3. Jaké jsou nejběžnější způsoby využití internetu věcí? (více možností – vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně)

a) Nositelná zařízení, která monitorují glukózu v krvi.
b) Lednice, která automaticky vytvoří nákupní seznam.
c) Chytrá města a chytré domácnosti.
d) Maloobchod a chytré automobily.

4. Jaká opatření je možno zavést, abyste se ochránili před kybernetickými útoky ve všech vrstvách architektury IoT? (více možností – vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně)

a) Ověření zařízení
b) Instalace známých bezpečnostních softwarů do počítačů, tabletů a chytrých telefonů.

c) Používání VPN, protože pomáhá chránit data přenášená na Vaší domácí nebo na veřejné Wi-Fi síti.
d) Pravidelně kontrolujte web vývojáře Vašeho zařízení kvůli aktualizacím firmwaru.

5. Jak nejlépe předejít narušení kybernetické bezpečnosti? (více možností – vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně)

a) Rozpoznání hrozeb a zranitelných míst
b) Posouzení vystavení se riziku prostřednictvím různých druhů analýz
c) Vytvoření ochranných a pohotovostních plánů
d) Určete, kdy upozornit krizový tým, odborníky na kybernetickou bezpečnost, poskytovatele služeb a pojišťovnu.

Klíč správných odpovědí

Počítačová kriminalita

1b, 2ac, 3T
4: Krádež identity, Kyberšikana, Finanční kriminalita, Kyberstalking
5: Kyberterorismus

Ochrana před nevhodným obsahem

1: Pornografie, Rasismus nebo nenávist, Pro-ana webové stránky, Stránky s extremistickým obsahem

2ad, 3b, 4bd

5: Důvěra

Ochrana osobních údajů

1: ochrana osobních údajů, osobními údaji, zneužitím, ochrana, základním, technický pokrok, globální vytváření sítí, GDPR
2: aN, bN, cA, dA, eN
3: sedm, zpracování dat, maximálním pokutám, necitlivých, šest, osobních údajů, citlivých údajů, výjimečných případech
4: b e f
5: osobních údajů, bezpečnosti údajů, "privacy by design" (tzv. záměrná ochrana osobních údajů), "privacy by default" (tzv. ochrana osobních údajů ve výchozím nastavení), privacy by design, technologického návrhu, privacy by default, výchozího nastavení, osobní údaje

Bezpečnost používání chytrých telefonů

1ac 2be 3bd
4: aN, bA, cN, dA, eA, fN
5: bezpečnostním rizikům, nejnovější, nepoužívejte, zásady ochrany osobních údajů, nejnutnější, zvláštní e-mailovou adresu, přístupová, nastavení soukromí aplikací, zablokujte

Informační tok/Komunikace na internetu

1: b
2: falešný e-mail, příloh, nereálná, odesílateli, popudlivá, důvěrných informací, odesílateli, chyb, složky spamu, formátováním
3: b c e h
4: a b d e
5: údaji, informacemi, útočníků, falešnou identitou, nepravdivých informací, sociálních sítí, osobní, důvěrné, filtrů, přijímání, ochrany soukromí, zavádějící, nahlásit, orgánům

Rodičovská kontrola

1 a b c
2: kyberšikana, dospělá, sexuální zneužívání, predátorem, nezletilé osoby, sexuálním

3: kyberšikany, oběti, poškodit, reputaci, dezinformaci
4: závislost, nezletilá osoba, internetu, emoční, nálad, netolismus
5: datům, metody, internetové, hesla, mladistvých, online

Hardware a software

1: fyzické, monitor, myš, klávesnice, programy nebo aplikace, úkolů
2: g
3: Ano
4: g
5: g,h

Osobní údaje na sociálních sítích

1: a, b, c, d
2: nastavení soukromí, vlastník/provozovatel, phishingový útok
3: d
4: d
5: a

Kybernetická bezpečnost

1: c
2: c
3: d
4: c
5: d

Internet věcí

1: a, b, c, d
2: a
3: b
4: a, b, c, d
5: a, b, c, d