UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
Kompetenčné centrum kybernetickej bezpečnosti na UPJŠ

2026

Stredoškolské bezpečnostné tímy - KyberTímy

(príručka)

Projekt Kompetenčné centrum kybernetickej bezpečnosti na UPJŠ (KCKB UPJŠ) financovaný Európskou úniou z prostriedkov Plánu obnovy a odolnosti Slovenskej republiky, kód projektu: 17R05-04-V01-00007.

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

OBSAH

ÚVOD

Táto príručka je primárne určená učiteľom stredných škôl a ich žiakom, ale inšpirácie na zostavenie kybernetického bezpečnostného tímu na škole v nej nájdu aj učitelia základných škôl. Príručka ponúka jednoduchý návod na zostavenie bezpečnostného tímu na škole a jeho fungovanie. Prevedie vás začiatkami fungovania tímu až po plánovanie bezpečnostných aktivít. Prináša niekoľko námetov na prednášky, workshopy a užitočné odkazy, na ktorých nielen učitelia, ale aj žiaci nájdu množstvo nápadov a odborného obsahu z oblasti kybernetickej a informačnej bezpečnosti.

Príručka vznikla po piatich rokoch úspešného fungovania Kybernetického bezpečnostného tímu na Gymnáziu sv. Košických mučeníkov v rámci projektu UPJŠ: Kompetenčné centrum kybernetickej bezpečnosti UPJŠ.

1 PREDSTAVENIE KC KB UPJŠ

Kompetenčné centrum kybernetickej bezpečnosti na Univerzite Pavla Jozefa Šafárika v Košiciach (KC KB UPJŠ) predstavuje kompetenčné centrum, v rámci ktorého sú realizované aktivity zamerané na vzdelávanie, výskum a expertnú činnosť v oblasti informačnej a kybernetickej bezpečnosti, ochrany dát, kyberkriminality a ochrany pred dezinformáciami. Súčasne KC KB UPJŠ realizuje medzinárodnú spoluprácu s akademickými partnermi zo zahraničia a poskytuje konzultácie pre možnosť prípravy a podania projektov v oblasti kybernetickej bezpečnosti.

Vytvorenie KC KB UPJŠ reflektuje viacero problémov, ktoré možno v súčasnosti identifikovať v oblasti informačnej a kybernetickej bezpečnosti (ďalej aj „KIB“):

- zvýšenie bezpečnostného povedomia relevantných subjektov zahŕňajúcich predovšetkým zamestnancov verejnej správy a študentov vysokoškolského a stredoškolského štúdia,
- vzdelávanie a výchova nových odborníkov pôsobiacich v tejto oblasti,
- výskum kybernetických hrozieb a identifikácia adekvátnych reakcií na tieto hrozby,
- zvýšenie operatívnej bezpečnosti v rámci verejnej správy poskytovaním expertných činností zo strany CSIRT tímu.

V rámci KC KB UPJŠ sa pripravoval študijný plán magisterského stupňa študijného programu aplikovaná informatika, ktorého jedna vetva sa zameriava na kybernetickú bezpečnosť. K tomuto študijnému plánu budú vytvorené, resp. modifikované viaceré predmety. Súčasne sa ako výstup kompetenčného centrá vytvára ponuka **vzdelávania** pre rôzne cieľové skupiny zamestnancov verejnej správy.

V kontexte projektu sa súčasne posilňuje **spolupráca so strednými školami**, najmä vo forme činnosti **KyberTímov**, ich vzdelávania a následného zapojenia do šírenia bezpečnostného povedomia medzi širokou verejnosťou.

V rámci vzdelávacích aktivít sa sumarizujú nové poznatky a skúsenosti z oblasti KIB, ale aj príbuzných oblastí. Tie sú aktuálne doplnené o rôzne formy zážitkového vzdelávania.

V rámci **výskumnej** činnosti dochádza v už existujúcich výskumných oblastiach k publikovaniu viacerých vedeckých výstupov a k vytvoreniu nových možných výskumných spoluprác na posilnenie výskumného a vývojového potenciálu KC KB UPJŠ.

Nemenej dôležitým výstupom projektu je doplnenie výbavy a vzdelávanie univerzitného CSIRT tímu a možnosť poskytovania **expertných činností** pre akreditované CSIRT tímy v SR za účelom rýchlejšej a adekvátnejšej reakcie na kybernetické bezpečnostné incidenty.

2 CIELE

Ciele, činnosti a zručnosti, ktoré sa rozvíjajú u žiakov, zapojených do Kybertímu:

- ✓ **vzdelávanie** žiakov v oblasti kybernetickej a informačnej bezpečnosti,
- ✓ **zvyšovanie bezpečnostného povedomia** medzi ľuďmi (prednášky, workshopy),
- ✓ **rozvoj žiakov** a ich **tímovej spolupráce**,
- ✓ rozvoj **soft-skills**, **komunikačných** a **prezentačných zručností**,
- ✓ **dobrovoľnícka** činnosť,
- ✓ rozvoj **sociálnych zručností**.

3 BENEFITY PROJEKTU KYBERTÍMY

V nasledujúce kapitole uvádzame niektoré významné benefity pre žiakov, učiteľov a školy, zapojené do projektu Kybertímy.

3.1 BENEFITY ZAPOJENIA SA STREDNEJ ŠKOLY DO PROJEKTU KYBERTÍMY

Najdôležitejšie benefity zapojenia sa strednej školy do projektu Kybertímy sú nasledovné:

- **vzdelávanie učiteľa**/učiteľov v aktuálnych trendoch v oblasti informačnej a kybernetickej bezpečnosti (online a prezenčné prednášky a workshopy, CSD)
- **vzdelávanie stredoškolákov** (informačná a kybernetická bezpečnosť, právne aspekty, zlepšovanie soft skills a prezentačných zručností ...)
- výstupy v rámci projektu – prednáška/workshop:

  povinné: na svojej škole, pre nejakú ZŠ,

  dobrovoľné: pre rodičov, seniorov, učiteľov a pod.
- **sieťovanie so základnými školami** (žiaci uskutočnia prednášku/workshop/CSD pre blízku/blízke ZŠ)
- **sieťovanie so strednými školami** – spolupráca a výmena skúseností (na CSD na UPJŠ alebo v rámci stretnutí Kybertímov).

3.2 BENEFITY ŽIAKOV STREDNEJ ŠKOLY V PROJEKTE KYBERTÍMY

Benefity žiakov strednej školy v projekte Kybertímy sú nasledovné:

- **vzdelávanie stredoškolákov** (informačná a kybernetická bezpečnosť, právne aspekty, ...)
- zážitkové učenie
- zlepšovanie **soft skills**: práca v tíme a práca s ľuďmi, komunikácia, zlepšovanie komunikačných zručností, flexibilita, riešenie problémov, kritické myslenie, time management, interpersonálne schopnosti
- zlepšovanie **prezentačných zručností**
- výstupy v rámci projektu – prednáška/workshop:

  povinné: na svojej škole, pre nejakú ZŠ,

  dobrovoľné: pre rodičov, seniorov, učiteľov a pod.

3.3 BENEFITY PRE ZÁKLADNÉ ŠKOLY

Benefity pre Základné školy sú najmä:

- **aktuálne informácie pre žiakov a učiteľov ZŠ** z informačnej a kybernetickej bezpečnosti – preventívne vzdelávacie aktivity (prednášky, workshopy, online prednášky/workshopy),

- **sieťovanie škôl** a **rozvoj spolupráce medzi školami.**

4 WORKSHOPY

Témy workshopov, ktoré môžu žiaci Kybertímu pripraviť a zrealizovať pre žiakov na základných školách, prípadne pre svojich rovesníkov alebo rodičov a seniorov:

- Bezpečne na internete
- Bezpečnosť na sociálnych sieťach
- Bezpečné heslo
- Podvodné správy / Phishing
- Bezpečnosť mobilných zariadení
- Bezpečnosť prehliadača
- Dezinformácie
- Malvér
- Online platby
- Kryptografia.

4.1 BEZPEČNE NA INTERNETE

Cieľová skupina: 5. – 9. ročník ZŠ, rodičia, seniori

Obsah workshopu:

- Krátka štatistika – internet, mobily, sociálne siete
- Digitálna stopa
- Digitálna stopa aktívna
- Digitálna stopa pasívna
- Hrozby na internete (stručne char. každú skupinu s ukážkou príkladov a tipmi ako sa chrániť alebo sa podrobnejšie zamerať na niektorú konkrétnu hrozbu):

  sociálne siete – ich využitie a zneužitie

  sociálne inžinierstvo – fyzicky aj na diaľku

  phishingové útoky

  e-shop

  heslá a ich autentifikácia

  verejné WiFi

  prenosné média (USB kľúč)

  mobilné zariadenia

  webový prehliadač

- Čo raz zverejníte na internete, ostane už navždy verejné – na záver zaradiť video:

Sharenting - Ella a jej odkaz rodičom:

https://www.youtube.com/watch?v=F4WZ_k0vUDM (originál)

https://www.linkedin.com/embed/feed/update/urn:li:activity:7089225446944321536?compact=true (Neoficiálna verzia, slovenské titulky)

4.2 BEZPEČNOSŤ NA SOCIÁLNYCH SIEŤACH

Cieľová skupina: 7. – 9. ročník ZŠ, seniori

Obsah workshopu:

- Video Veštec a čítanie myšlienok (https://www.youtube.com/watch?v=F7pYHN9iC9I) – ukážka, ako sa dajú informácie o ľuďoch vyhľadať na internete a sociálnych sieťach
- Podvodné správy na sociálnych sieťach – príklady
- Podvodné správy na sociálnych sieťach – ako rozpoznať podvodný odkaz (https://www.virustotal.com/gui/home/upload)
- Reklamy, veľmi výhodné ponuky
- Romantickí podvodníci
- Disinhibičný efekt
- Deepfake,
  video: (https://www.youtube.com/watch?v=1zg0_bRoj1U&ab_channel=O2Slovakia)
- Odporúčania ako sa vyhnúť podvodom na sociálnych sieťach
- Čo raz zverejníte na internete, ostane už navždy verejné – na záver zaradiť video:

Sharenting - Ella a jej odkaz rodičom:

https://www.youtube.com/watch?v=F4WZ_k0vUDM (originál)

https://www.linkedin.com/embed/feed/update/urn:li:activity:7089225446944321536?compact=true (Neoficiálna verzia, slovenské titulky)

4.3 BEZPEČNÉ HESLO

Cieľová skupina: 5. – 6. ročník ZŠ

Obsah workshopu:

- Tester hesiel – otestujte silu niektorých hesiel (https://csirt.upjs.sk/hesla/)
- Bezpečné heslo – ako vytvoriť bezpečné heslo?
- Čo by nemalo obsahovať heslo
- Správa hesiel
- Multifaktorová autentifikácia
- Úniky údajov – otestovať (https://haveibeenpwned.com/)
- Odporúčania – čo robiť, ak je email v zozname uniknutých emailov

4.4 PODVODNÉ SPRÁVY / PHISHING

Cieľová skupina: 7. – 9. ročník ZŠ, rodičia, seniori

Obsah workshopu:

- Čo podvodníkov zaujíma? (osobné údaje, používateľské meno a heslo, čísla kariet)
- Video – SCAM (https://www.youtube.com/watch?v=B1bM5aa4OqI)
- Čo je to phishing + aké formy phishingu existujú
- Smishing – podvodné SMS + príklady/ukážky – upozorniť na char. znaky
- Vishing – podvodné telefonáty + príklady/ukážky – upozorniť na char. znaky, video (https://www.youtube.com/watch?v=AzTNrtQ6v_o),

  overenie tel. čísla:

  https://www.vyhladavaniecisla.sk/

  https://www.neznamecislo.sk/

  https://www.ktomivolal.eu/

- Phishing – podvodné emaily + príklady/ukážky – upozorniť na char. znaky,

  overenie emailu odosielateľa:

  https://hunter.io/email-verifier

  https://seon.io/

  https://verifalia.com/validate-email

- Quishing – podvod cez QR kód + príklady/ukážky, video (https://www.linkedin.com/posts/ben-mckillop-0a07a5123_quishing-phishing-cyber-ugcPost-7251509680324120577-ddL_)
- Phishingový test

4.5 BEZPEČNOSŤ MOBILNÝCH ZARIADENÍ

Cieľová skupina: 7. – 9. ročník ZŠ, rodičia, seniori

Obsah workshopu:

- Aký bezpečný je môj mobil – senzory v mobile
- Čo najviac zneužívajú útočníci v mobilnom zariadení?
- Čo sú zraniteľnosti?
- Odporúčania
  Aktualizácie!
  Oficiálne úložiská aplikácií!
  Biometrické overenie!
  Neuchovávať cenné informácie!
  Antivírusová ochrana!
  Prehliadač – blokovanie reklám!
  Reštart telefónu – občas
- Zabezpečenie mobilného telefónu – OS Android:
  Aktualizácie

Upozornenia na zamknutej obrazovke
Povolenia (oprávnenia) aplikácií
Pozor na zjednodušené ovládanie
Účet google

- Zabezpečenie mobilného telefónu – iOS:
  Aktualizácie
  Súkromie a bezpečnosť
  Oprávnenia aplikácií
  Sledovanie
  Režim blokovania
  iCloud
  AdGuard pre Safari

4.6 BEZPEČNOSŤ PREHLIADAČA

Cieľová skupina: 7. – 9. ročník ZŠ, rodičia, seniori

Obsah workshopu:

- Blokovač reklám v prehliadačoch
- Prehliadač Chrome :

Ochrana súkromia a zabezpečenie

Odstrániť dáta prehliadania

Sprievodca ochranou súkromia

Súbory cookie tretích strán

Ochrana súkromia pri reklamách

Zabezpečenie

Nastavenia webov:

Povolenia
Ďalšie povolenia
Obsah
Ďalšie nastavenia obsahu

- Prehliadač Firefox:

História

Súkromie a bezpečnosť

- Prehliadač Edge:

História

Ochrana osobných údajov

Súbory cookie

4.7 DEZINFORMÁCIE

Cieľová skupina: 7. – 9. ročník ZŠ, rodičia, seniori

Obsah workshopu:

- Vysvetlenie, čo sú dezinformácie, misinformácie a malinformácie – rozdiely a príklady.
- Prečo sú dnes tak rozšírené: sociálne siete, rýchlosť šírenia, informačný pretlak.
- Dôsledky na spoločnosť, politiku, zdravotnícke rozhodnutia a medziľudské vzťahy
- Mechanizmy manipulácie
- Ekosystém šírenia dezinformácií
- Overovanie informácií
- Interaktívne aktivity
- Komunikácia s ovplyvnenými osobami
- Budovanie odolnosti

4.8 MALVÉR

Cieľová skupina: 7. - 9. ročník ZŠ

Obsah workshopu:

- Malvér - definícia
- Typy malvéru (vírusy, červy, trójske kone, ransomware, spyware, adware, rootkity…)
- Spôsoby šírenia a najčastejšie vektory útokov
- Životný cyklus útoku – od infekcie až po exfiltráciu dát
- (Praktické ukážky fungovania malvéru v bezpečnom prostredí)
- Detekcia a analýza malvéru (základné princípy, nástroje, sandboxing)
- Prevencia: bezpečnostné návyky, aktualizácie, zálohovanie, segmentácia siete
- Incident response: čo robiť po nákaze, kroky a odporúčané postupy
- Aktuálne hrozby

4.9 ONLINE PLATBY

Cieľová skupina: 9. ročník ZŠ, seniori

Obsah workshopu:

- Základné princípy online platieb a ich fungovanie
- Typy online platieb (karty, bankové prevody, platobné brány, e-peňaženky, mobilné platby)
- Bezpečnostné štandardy (3D Secure, tokenizácia, šifrovanie)
- Ako prebieha transakcia krok za krokom – zrozumiteľný technický prehľad
- Overovanie používateľov a autentifikačné metódy (MFA, biometria)
- Najčastejšie riziká a podvody pri online platbách a ako im predchádza
- Bezpečné nákupné návyky pre používateľov
- Právne a spotrebiteľské aspekty (reklamácie, chargeback, ochrana klienta)
- Trendy v digitálnych platbách (open banking, instant payments, kryptomeny – iba informačne)

4.10 KRYPTOGRAFIA

Cieľová skupina: 9. ročník ZŠ

Obsah workshopu:

- Kódovanie vs Šifrovanie
- Kódovanie – vysvetlenie a príklady
- Šifrovanie – vysvetlenie
- História šifrovania
- Kryptológia, kryptografia, kryptoanalýza, steganografia
- Symetrické šifrovanie, symetrické šifry substitučné, transpozičné – praktické úlohy
- Asymetrické šifrovanie

4.11 NÁPADY NA WORKSHOP – PRAKTICKÉ UKÁŽKY

V rámci aktivít na workshope môžu žiaci Kybertímu s účastníkmi prakticky realizovať rôzne aktivity, pri ktorých si precvičia nové vedomosti a nadobudnú nové zručnosti v oblasti kybernetickej a informačnej bezpečnosti. Na worskhopoch môžu použiť napríklad nasledujúce online nástroje:

Generátor hesiel: https://www.eset.com/sk/generator-hesiel/

Phishingový test:

- https://csirt.upjs.sk/phishing/
- https://istrosec.com/sk/e-learning/phishing-test/test/
- https://www.csirt.gov.sk/archiv/osvedcene-postupy/navody-a-odporucania/phishingovy-test-871.html
- https://safelab.sk/internetova-bezpecnost/phishingovy-online-test

Tester hesiel: https://hesla.csirt.upjs.sk/

https://www.itcity.sk/heslo/overenie/

Testovanie podvodných URL alebo súborov: https://www.virustotal.com/gui/home/upload

Testovanie podvodných URL: https://urlscan.io/

Úniky údajov: https://haveibeenpwned.com/

Bezpečnostné kvízy:

- Kvíz SLSP: https://www.slsp.sk/sk/ludia/bezpecnost
- Priamo kvíz SLSP: https://www.slsp.sk/sk/ludia/bezpecnost#/modalComponent/isOpen/true/url/%2Fsk%2Fconfiguration%2Fleads%2Fbezpecnost-test%2Fotazka1.modal
- Test digitálnej bezpečnosti TatraBanka: https://www.tatrabanka.sk/predigitalnubezpecnost/test-digitalnej-bezpecnosti/?utm_source=SilverpopMailing&utm_medium=email&utm_campaign=16687255&utm_content=spustit_test&mktid=874F4C0D08322FF2867D8C9FAA1D5FF0

4.12 NÁPADY NA WORKSHOP - VIDEÁ

Workshop môžu žiaci Kybertímu oživiť aj použitím videí, ktoré účastníkov zaujmú a často uľahčia a priblížia danú problematiku zaujímavým a netradičným spôsobom. Na bezpečnostných workshopoch možno použiť napríklad tieto videá:

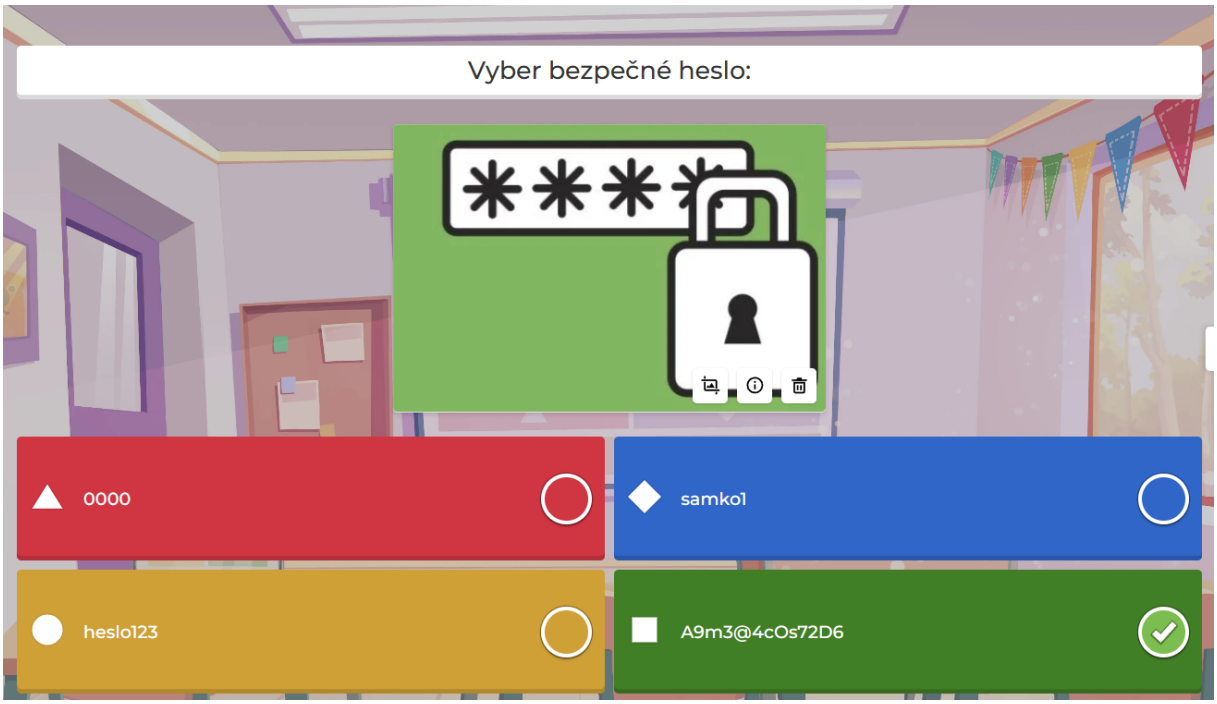
- Veštec – zdieľanie údajov na internete: https://www.youtube.com/watch?v=F7pYHN9iC9I
- PPPíter – vishing: https://www.youtube.com/watch?v=AzTNrtQ6v_o
- PPPíter – scam: https://www.youtube.com/watch?v=B1bM5aa4OqI
- PPPíter – phishing: https://www.youtube.com/watch?v=2ek-KeYRWdc
- Quishing: **:** https://www.linkedin.com/posts/ben-mckillop-0a07a5123_quishing-phishing-cyber-ugcPost-7251509680324120577-ddL_
- Sharenting - Ella a jej odkaz rodičom: https://www.youtube.com/watch?v=F4WZ_k0vUDM (originál)

  https://www.linkedin.com/embed/feed/update/urn:li:activity:7089225446944321536?compact=true (Neoficiálna verzia, slovenské titulky)

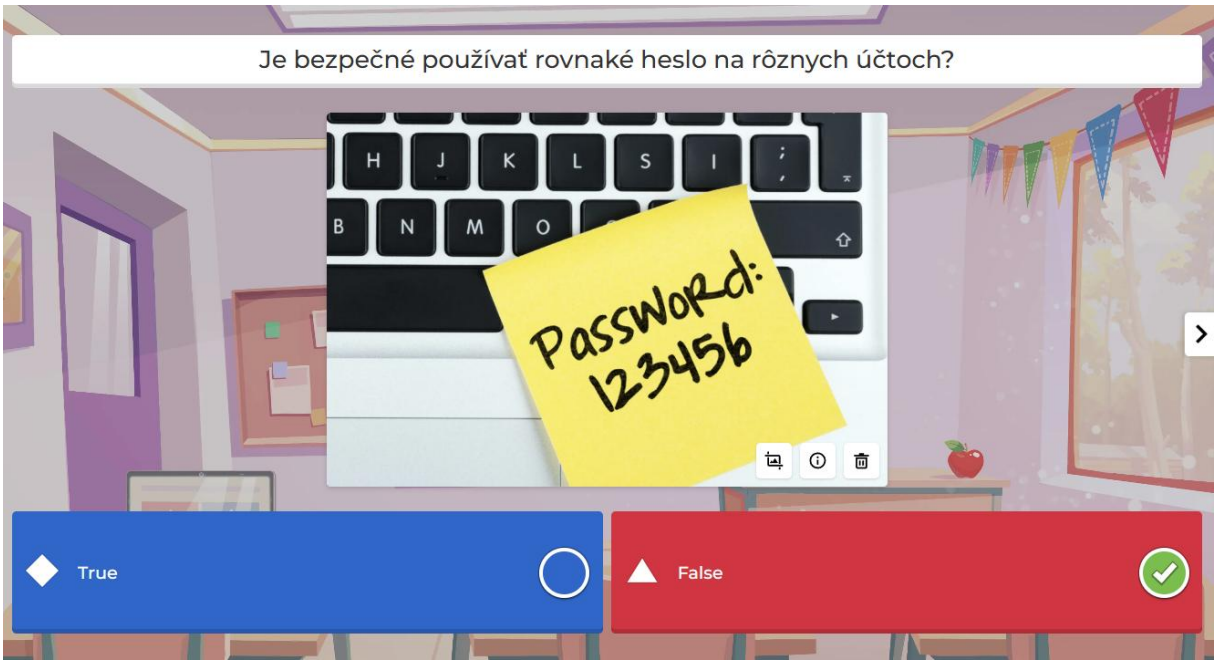
5 Kvízy

Bezpečnostné workshopy alebo iné aktivity môžu žiaci Kybertímu oživiť aj použitím rôznych kvízov. Uvádzame ukážku jednoduchého kvízu, ktorí bol pripravení pre žiakov základných škôl. Možno ho použiť na konci workshopu na zhrnutie informácií, ale aj na začiatku, ak chceme zistiť rozsah vedomostí, ktoré účastníci workshopu už z danej problematiky majú.

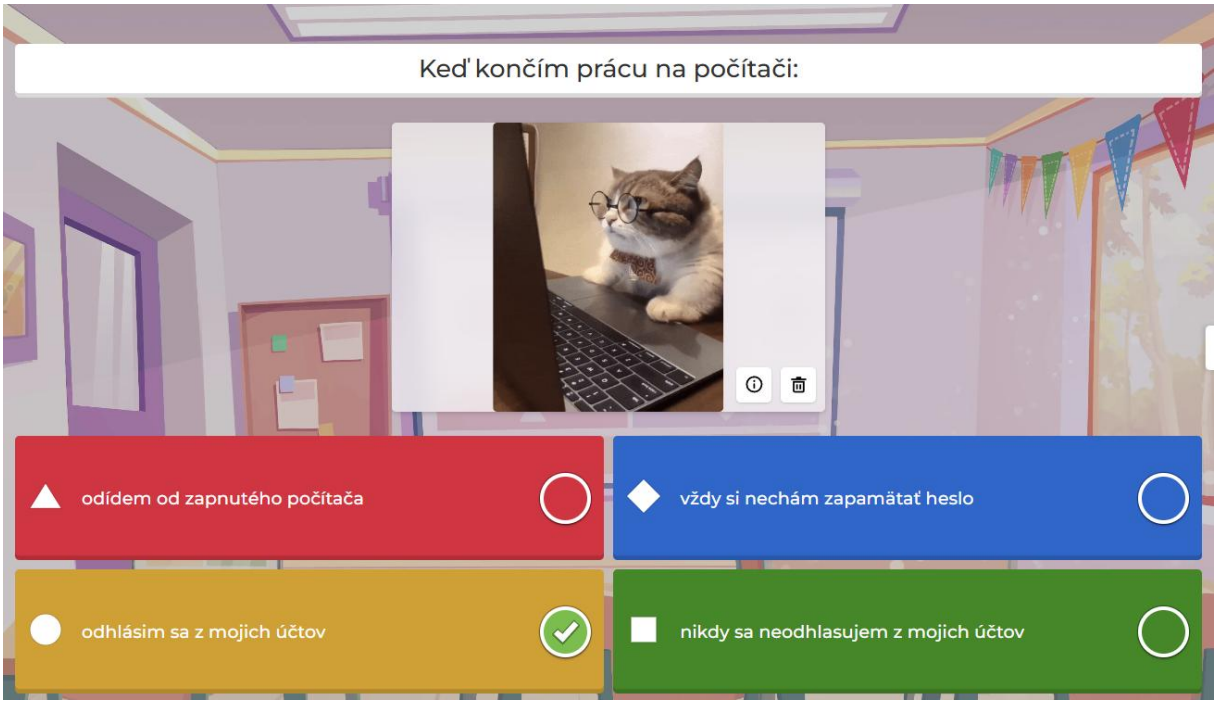
Kahoot pre žiakov základnej školy po absolvovaní bezpečnostného workshopu je dostupný na tejto linke: https://create.kahoot.it/share/kviz-bezpecnost/290db6cd-ac36-4475-81f8-a4f5c3511f8a a v texte nižšie uvádzame ukážku kvízu, používaného na workshopoch pre základné školy (Obrázok 1 - Obrázok 10.



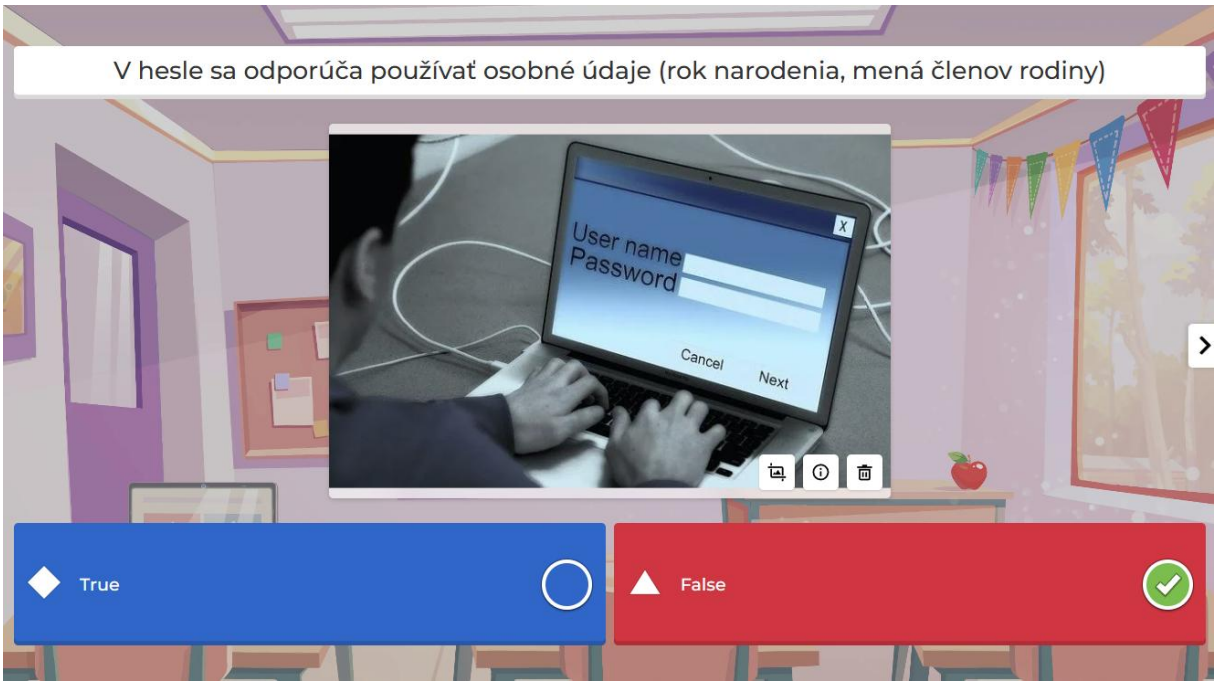
Obr. č. 1 – Bezpečnostný kvíz | 1.otázka



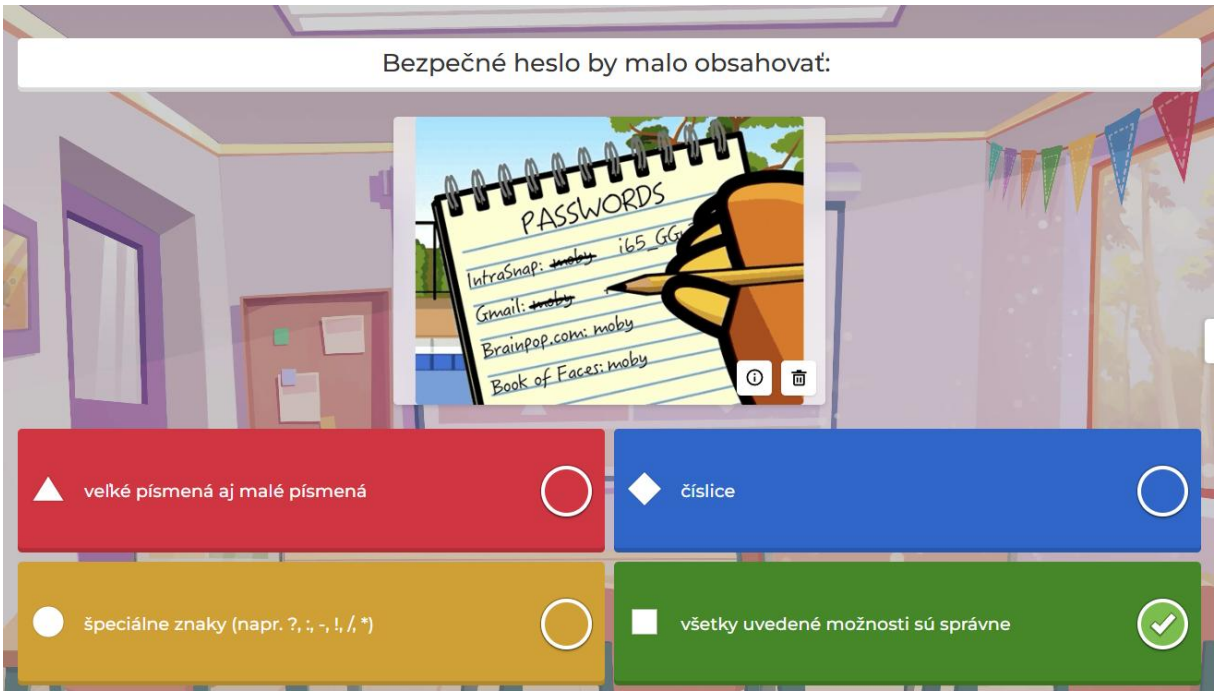
Obr. č. 2 – Bezpečnostný kvíz | 2. otázka



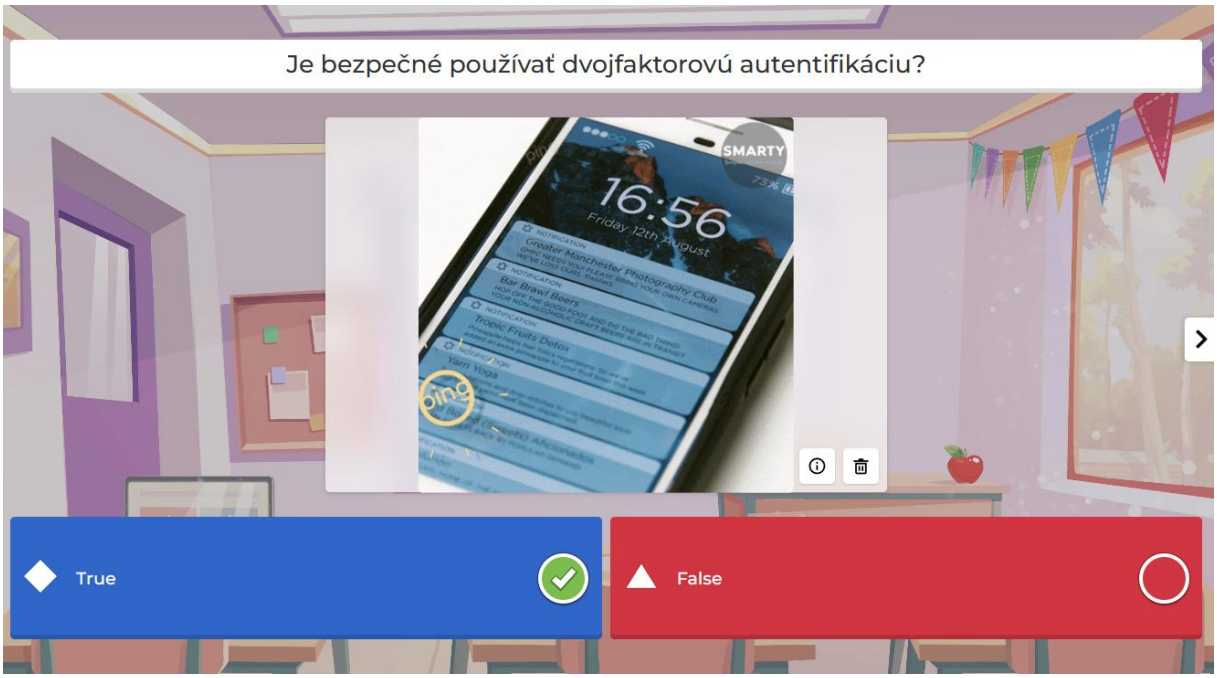
Obr. č. 3 – Bezpečnostný kvíz | 3. otázka



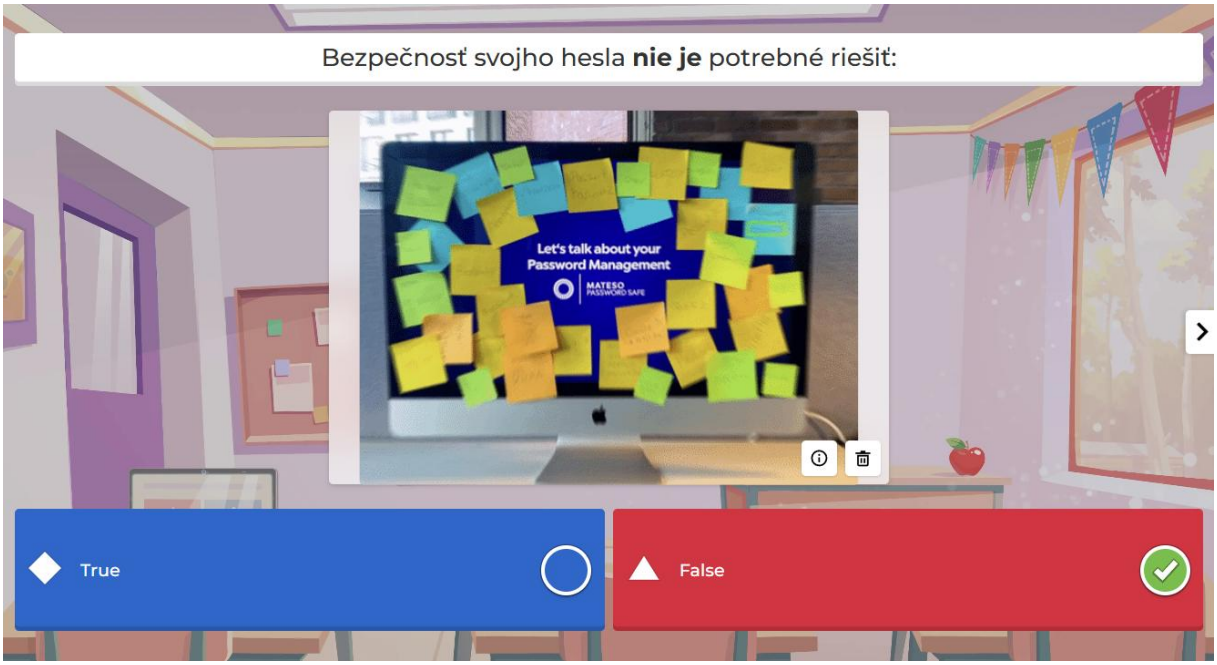
Obr. č. 4 – Bezpečnostný kvíz | 4. otázka



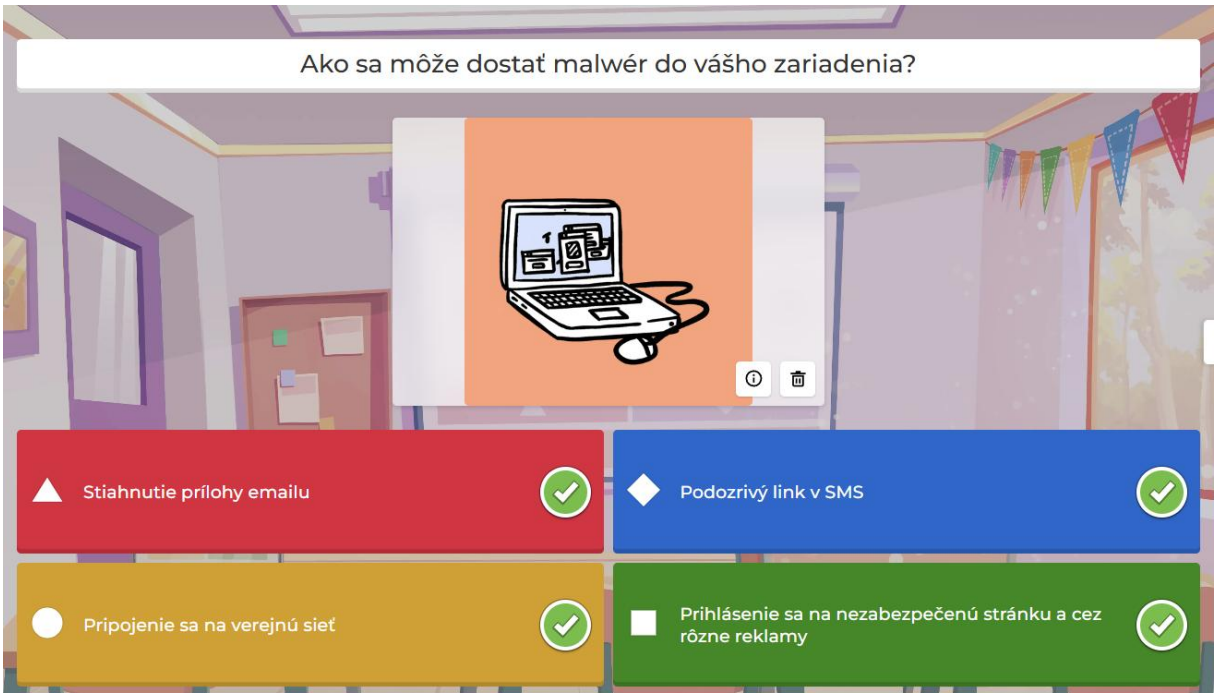
Obr. č. 5 – Bezpečnostný kvíz | 5. otázka



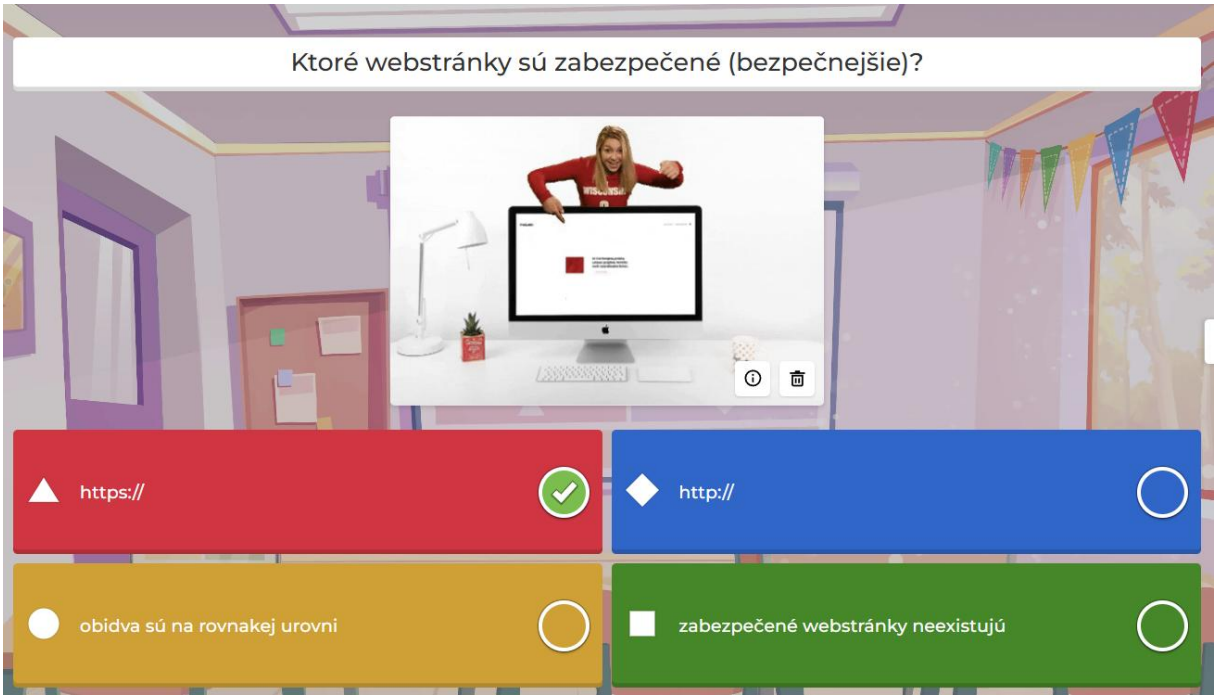
Obr. č. 6 – Bezpečnostný kvíz | 6. otázka



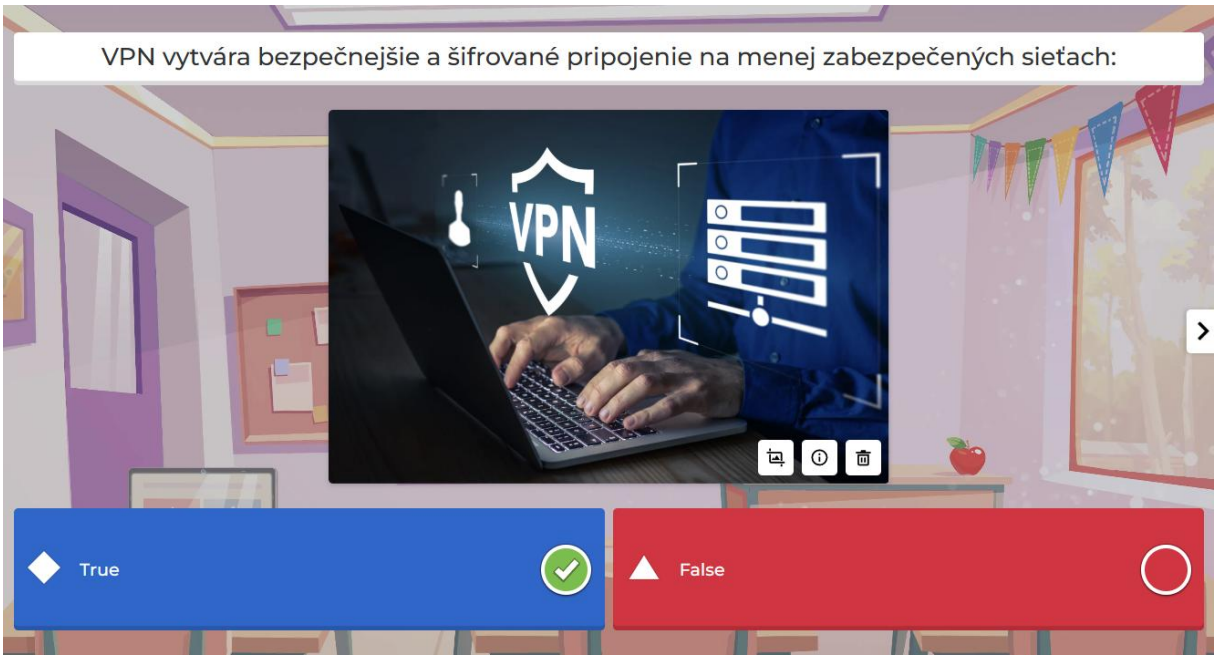
Obr. č. 7 – Bezpečnostný kvíz | 7. otázka



Obr. č. 8 – Bezpečnostný kvíz | 8. otázka



Obr. č. 9 – Bezpečnostný kvíz | 9. otázka



Obr. č. 10 – Bezpečnostný kvíz | 10. otázka

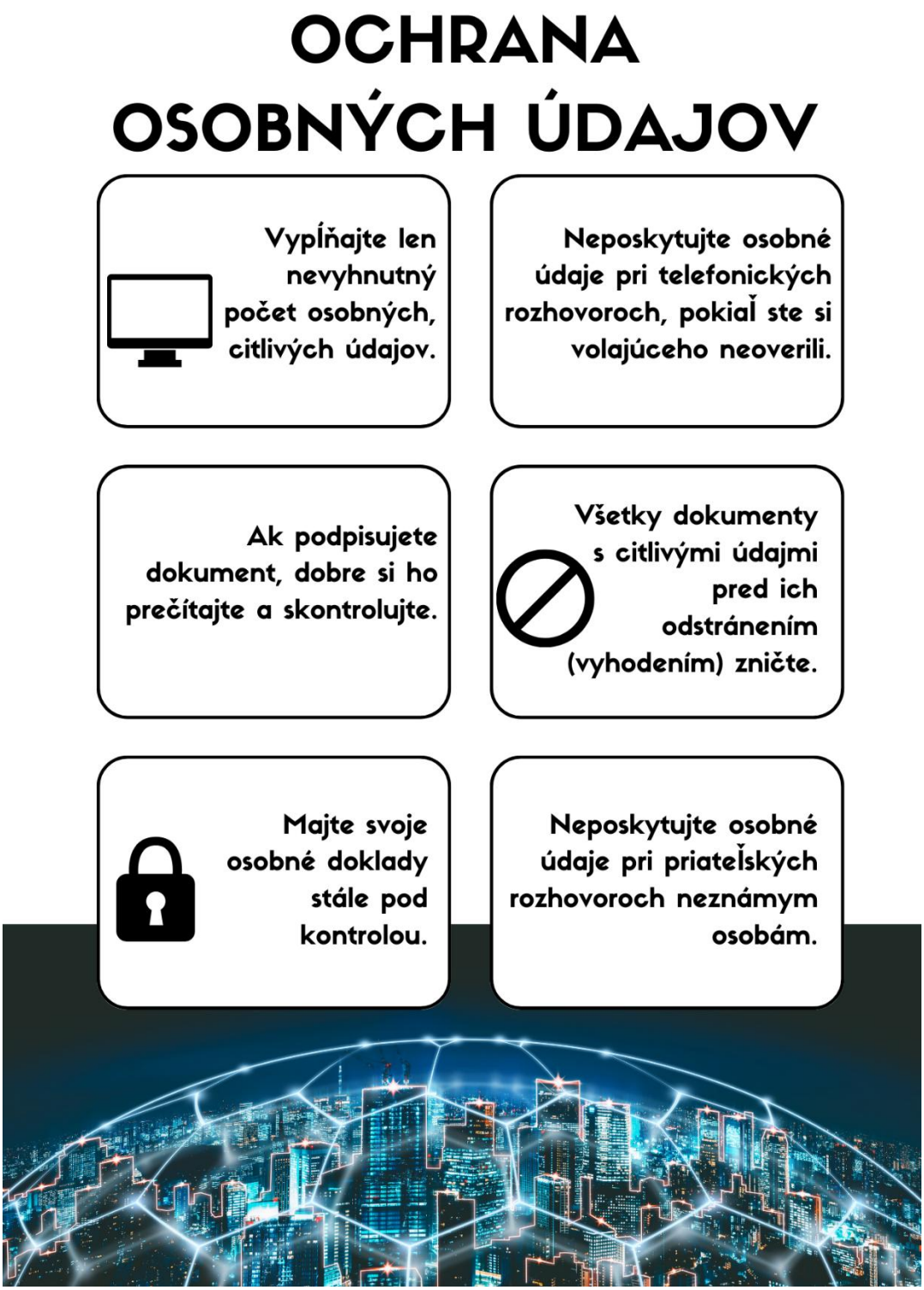
Zdroj obrázkov 1 - 10: Archív KyberTím GKM, https://kahoot.com/

6 INFOGRAFIKY

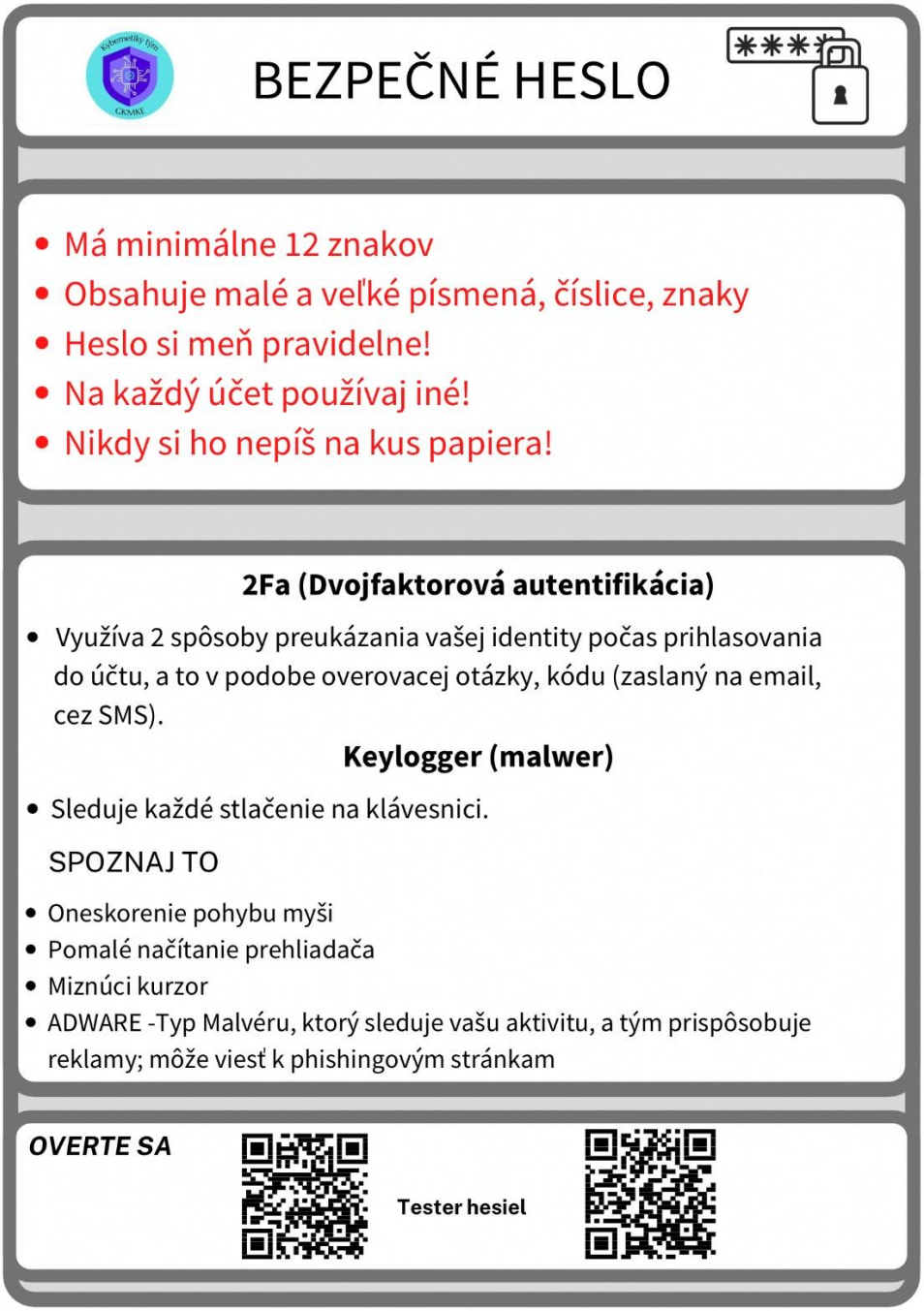
Webovú stránku môžu žiaci Kybertímu oživiť použitím rôznych plagátov. Plagáty možno umiestniť aj na nástenku v škole a v zmenšenej forme ich môžu rozdávať účastníkom workshopov. Nižšie uvádzame niekoľko ukážok plagátov a infografík, ktoré pripravili žiaci Kybertímu (Obrázok 11 – Obrázok 19).

Obr. č. 11 – Infografika Kybernetická bezpečnosť

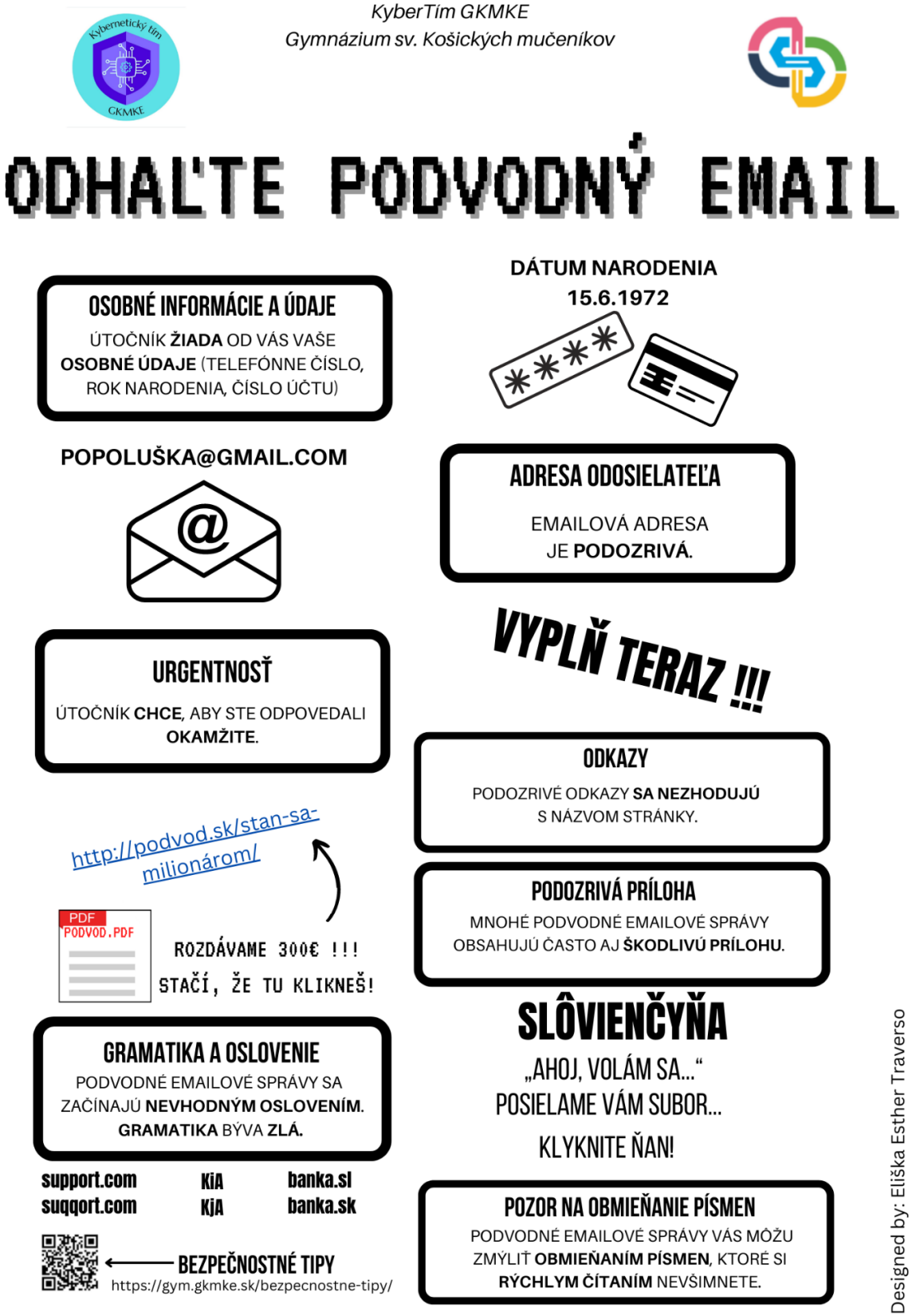
Obr. č. 12 – Infografika Ochrana osobných údajov – farebná verzia



Obr. č. 13 – Infografika Ochrana osobných údajov – verzia pre tlač na farebný papier

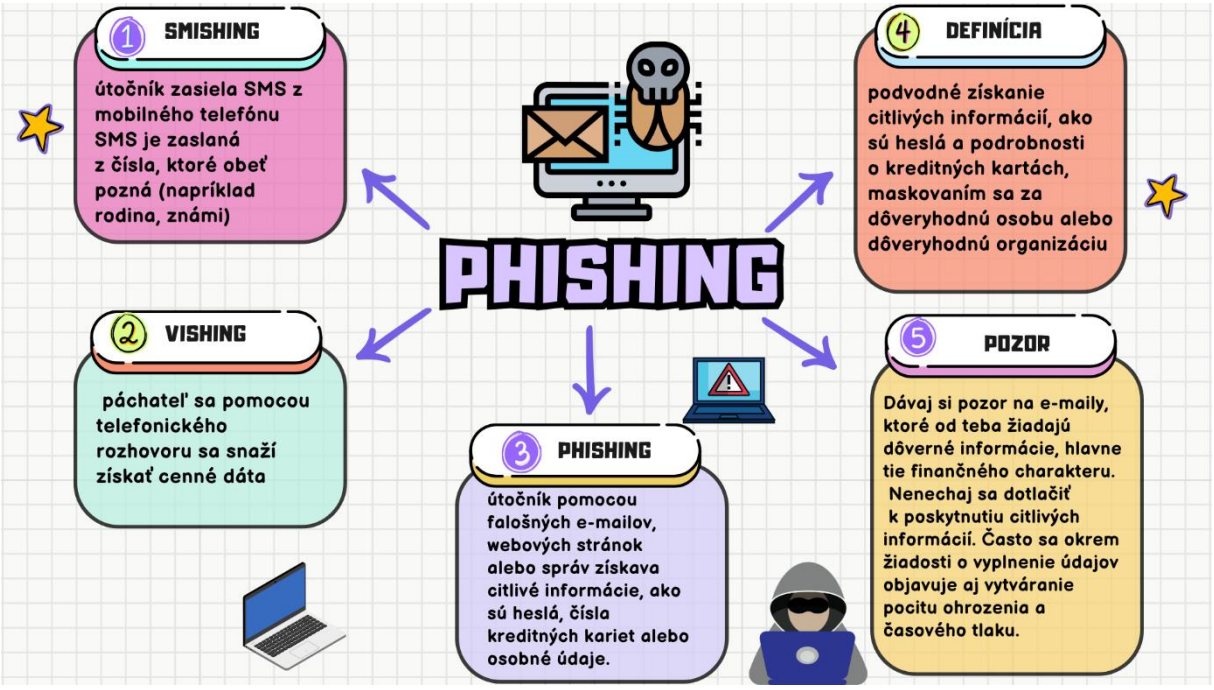


Obr. č. 13 – Infografika Bezpečné heslo



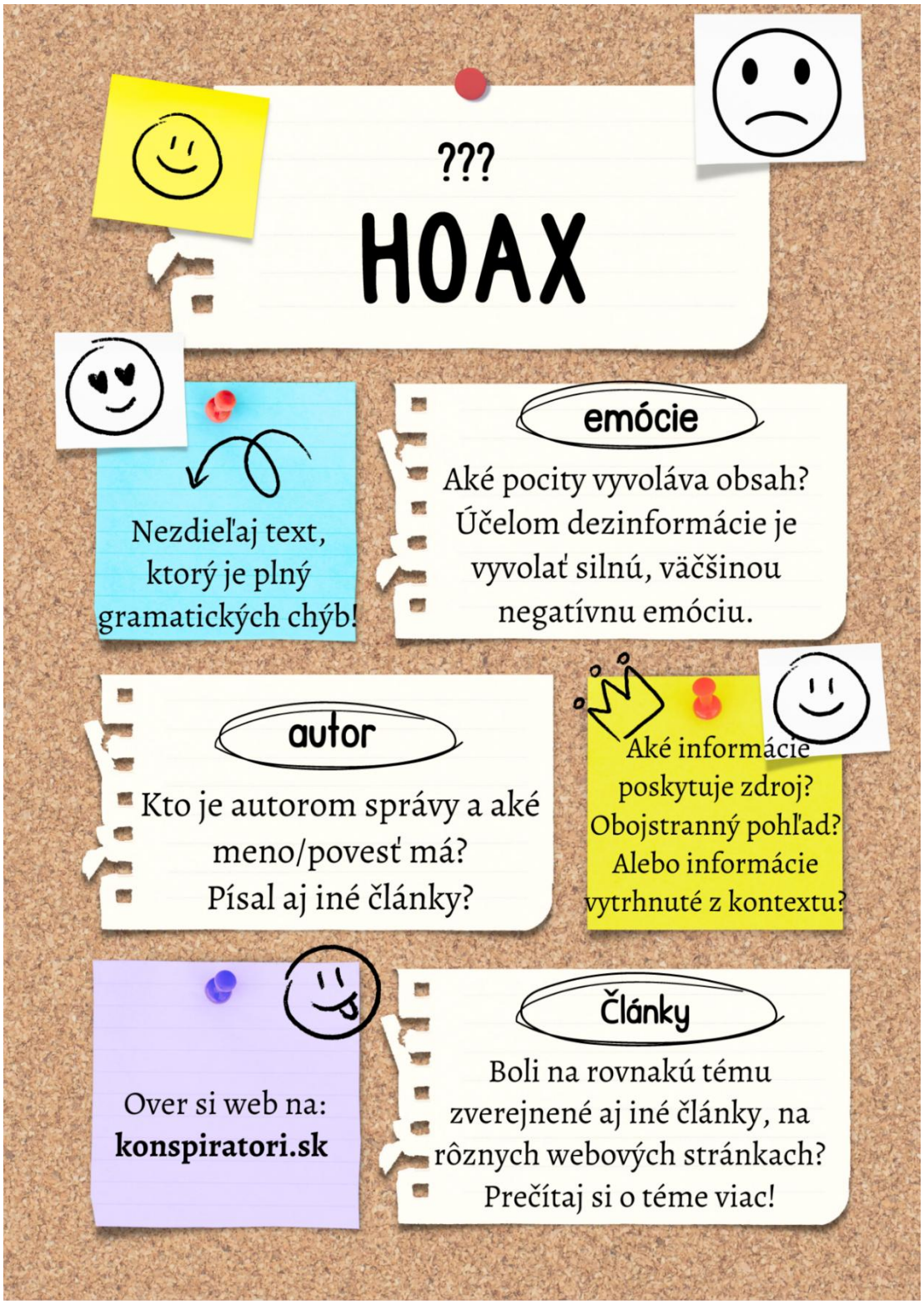
Obr. č. 14 – Infografika Odhaľte podvodný email

Obr. č. 15 – Infografika Ako odhaliť podvodný email



Obr. č. 16 – Infografika Phishing

Obr. č. 17 – Infografika Podvodné telefonáty (určené pre seniorov)



Obr. č. 18 – Infografika Hoax

Obr. č. 19 – Infografika Digitálna stopa

Zdroj obrázkov 11 - 19: Archív KyberTím GKM

7 WEBOVÁ STRÁNKA KYBERTÍMU

Kybertím, ktorý pôsobí na strednej škole, môže svoje aktivity a bezpečnostné tipy propagovať a zverejňovať na webovej stránke školy alebo si môže vytvoriť vlastnú webovú stránku. Uvádzame ukážku webovej stránky KyberTímu GKM, kde sú jednotlivé aktivity, podujatia a bezpečnostné tipy zverejnené takto:

- Prehľad aktivít: https://www.gkmke.sk/gym/it-aktivity/kyberneticka-bezpecnost/
- Bezpečnostné tipy: https://www.gkmke.sk/gym/bezpecnostne-tipy/
- CyberSecurityDay pre ZŠ: https://www.gkmke.sk/gym/cybersecurityday/

Ďalšie odkazy na webové stránky Kybertímov sú zverejnené napríklad na webovej stránke https://cyberawareness.sk/galeria-ziackych-prac-2024/.

8 WORKSHOPY PRE ŽIAKOV ZÁKLADNÝCH ŠKÔL

Workshopy pre žiakov ZŠ možno organizovať pre žiakov 2. stupňa ZŠ na ich základnej škole alebo na pôde vašej strednej školy. V prípade, že základná škola je príliš ďaleko, organizujte vzdelávanie online.

Workshopy, ktoré organizujeme na základnej škole, kde nás zavolajú, sú zvyčajne 4. Osvedčilo sa nám robiť workshopy pre triedy jednotlivo, nie pre všetky triedy naraz. Ak je to možné, je dobré uskutočniť workshop v počítačovej učebni, aby si žiaci mohli zároveň praktické veci vyskúšať a tak sa ich lepšie naučiť. Obvykle jeden workshop realizujú dvaja žiaci z Kybertímu. Takto je možné so 4 žiakmi Kybertímu uskutočniť na základnej škole 8 workshopov.

Vybranú tému z bezpečnosti žiaci spracujú formou prezentácie napr. v programe PowerPoint alebo Canva. Je dobré mať ju vo verzii nezávislej od pripojenia na internet, lebo pri prezentovaní môžu nastať technické komplikácie. Prednášku je dobré striedať s praktickými ukážkami, aby sme žiakov aktivizovali a viac zapojili do témy. Tiež si lepšie osvoja nové informácie, ak si ich priamo na mieste aj vyskúšajú. Na konci workshopu odporúčame urobiť krátky kvíz na zhrnutie. Na takýto kvíz sa osvedčila online platforma Kahoot. Nie sú nevyhnutne potrebné počítače, kvíz môžu žiaci robiť aj s použitím mobilného zariadenia alebo tabletu.

Pri žiakoch základnej školy je potrebné vhodne zvoliť terminológiu, aby sme ich nezahltili príliš veľkým množstvom pojmov, ktoré si nezapamätajú. V diskusii je dobré overiť, ktoré pojmy sú im známe, prípadne s ktorými podvodmi v online priestore sa už stretli v praxi, a postupne pridávame nové pojmy. Rozsah workshopu alebo prednášky volíme podľa veku žiakov, aby pojmy a aj množstvo nových informácií boli primerané ich veku aj psychickej zrelosti.

9 CyberSecurityDay pre ZŠ

CyberSecurity Day pre ZŠ (Obrázok 20 – logá organizátorov; Obrázok 21 – plagáty na podujatie) je poldňové podujatie určené pre žiakov 2. stupňa základnej školy (7. – 9. ročník) a ich učiteľov, ktorí sa zaujímajú o informačnú a kybernetickú bezpečnosť. Organizuje sa na pôde strednej školy. Obvykle pozostáva zo spoločnej prednášky, dvoch workshopov a po obede ukončuje podujatie bezpečnostný kvíz.

Na prednášku sú pozývaní odborníci na informačnú a kybernetickú bezpečnosť (napr. CSIRT-UPJŠ, ESET, eMsec, CSIRT.SK ...). Hosťujúca stredná školy zabezpečuje organizačnú stránku podujatia a členovia Kybertímu pripravujú dva rôzne workshopy pre žiakov ZŠ (Obrázok 20). Učitelia sa môžu zúčastniť na workshopoch spolu so žiakmi, alebo možno zorganizovať pre učiteľov samostatný workshop – v takomto prípade je potrebné zabezpečiť odborníka, ktorí povedie workshop pre učiteľov.

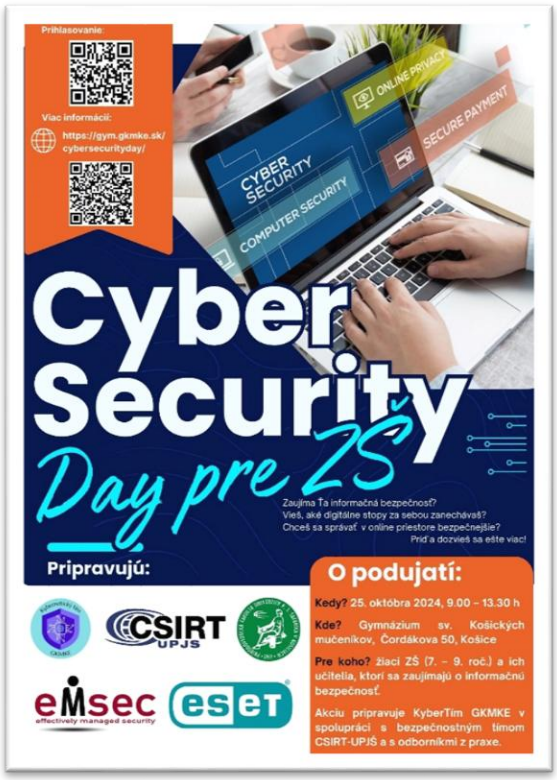
Na prednášku je potrebná väčšia prednášková miestnosť v závislosti od počtu účastníkov. Optimálny počet účastníkov na našej škole je 50. Pri väčšom počte bola už naša prednášková miestnosť aj priestory na prestávku mierne stiesnené. Tiež môže nastať problém s počtom počítačov, ktoré sú potrebné na workshopy.

Medzi jednotlivými aktivitami je potrebné urobiť prestávky na občerstvenie a presun, po workshopoch nasleduje obed. Po obede podujatie zakončuje bezpečnostný kvíz, ktorí tiež pripravujú žiaci Kybertímu. Odporúčame vytvoriť online kvíz, napr. použitím platformy Kahoot (https://kahoot.com/), Wooclap (https://www.wooclap.com/) alebo inej, kde sa výsledky vyhodnocujú bezprostredne po uskutočnení kvízu s ohľadom na počet účastníkov. Pri počte účastníkov do 40 je možné použiť platformu Kahoot v bezplatnej verzii. Pri počte 50 účastníkov a viac je lepšia platforma Wooclap, ktorá okrem štandardných otázok umožňuje importovať do kvízu aj prezentáciu, na záver je kvízu je preto možné zdieľať aj QR kód odkazujúci na krátky formulár so spätnou väzbou.

Obr. č. 20 – CyberSecurity Day pre ZŠ - logá organizátorov na CyberSecurityDay pre ZŠ


CyberSecurity
Day pre ZŠ
Zaujíma Ťa informačná bezpečnosť?
Si zvedavý, ako prebieha kybernetický bezpečnostný útok?
Čo všetko o Tebe vie internet?
Chceš vedieť, ako sa nestať obeťou podvodných správ?
Vieš, ako bezpečne používať svoje mobilné zariadenie?
Odpovede na tieto otázky nájdeš u nás!
Akciu pripravuje KyberTím GKMKE v spolupráci s bezpečnostným tímom CSIRT-UPJŠ a s odborníkmi z praxe.
Kedy? 24. februára 2023 v čase 9.00 – 13.00 h
Kde? Gymnázium sv. Košických mučeníkov, Čordákova 50, Košice
Pre koho? Akcia je určená žiakom ZŠ (7. – 9. roč.) a ich učiteľom, ktorí sa zaujímajú o Informačnú bezpečnosť.
Prihlasovací formulár:
https://forms.office.com/e/2etUG7x6tG
Viac informácií:
https://gym.gkmke.sk/cybersecurityday/
CSIRT UPJS
eset
FOND
EISI
NADÁCIA ZSE


CyberSecurity
Day pre ZŠ
Zaujíma Ťa informačná bezpečnosť?
Vieš, aké digitálne stopy za sebou zanechávaš?
Chceš sa naučiť odhaliť podvodné správy?
Odpovede na tieto a mnohé ďalšie otázky nájdeš u nás!
Akciu pripravuje KyberTím GKMKE v spolupráci s bezpečnostným tímom CSIRT-UPJŠ a s odborníkmi z praxe.
Kedy? 27. októbra 2023 v čase 9.00 – 13.00 h
Kde? Gymnázium sv. Košických mučeníkov, Čordákova 50, Košice
Pre koho? žiaci ZŠ (7. – 9. roč.) a ich učitelia, ktorí sa zaujímajú o informačnú bezpečnosť.
Prihlasovací formulár:
https://forms.office.com/e/dRJb5dFfbJ
Viac informácií:
https://gym.gkmke.sk/cybersecurityday/
CSIRT UPJS
eset


Prihlasovanie:
Viac informácií:
https://gym.gkmke.sk/cybersecurityday/
CYBER SECURITY
COMPUTER SECURITY
ONLINE PRIVACY
SECURE PAYMENT
Cyber Security Day pre ZŠ
Zaujíma Ťa informačná bezpečnosť?
Vieš, aké digitálne stopy za sebou zanechávaš?
Chceš sa správať v online priestore bezpečnejšie?
Príď a dozvieš sa ešte viac!
Pripravujú:
O podujatí:
Kedy? 25. októbra 2024, 9.00 – 13.30 h
Kde? Gymnázium sv. Košických mučeníkov, Čordákova 50, Košice
Pre koho? žiaci ZŠ (7. – 9. roč.) a ich učitelia, ktorí sa zaujímajú o informačnú bezpečnosť.
Akciu pripravuje KyberTím GKMKE v spolupráci s bezpečnostným tímom CSIRT-UPJŠ a s odborníkmi z praxe.
CSIRT UPJS
eMsec
eset


CyberSecurity Day pre ZŠ
Gymnázium
Zaujíma Ťa informačná bezpečnosť?
Vieš, aké digitálne stopy za sebou zanechávaš?
Vieš sa správať v online priestore bezpečne?
Príď a dozvieš sa ešte viac!
O podujatí:
Kedy? 6. februára 2025, 9.00 – 13.30 h
Kde? Gymnázium sv. Košických mučeníkov, Čordákova 50, Košice
Pre koho? žiaci ZŠ (7. – 9. roč.) a ich učitelia, ktorí sa zaujímajú o informačnú bezpečnosť.
Pripravujú:
Prihlasovanie:
Viac informácií:
https://gym.gkmke.sk/cybersecurityday/
CSIRT UPJS
eset
SECURITY DUNGEON

Obr. č. 21 – Plagáty na podujatie CyberSecurityDay pre ZŠ

Všetko potrebné na podujatie CyberSecurity Day:

1. **Plagát** o podujatí (6 týždňov dopredu vytvoriť) (Obrázok 21)
2. **Webstránka** o podujatí, článok na web, info na fb a instagram (1 mesiac dopredu)
3. **Prihlasovací formulár** online – cez forms
4. **List a plagát na školy, do KDK, KUI**, pre organizácie, kt. pracujú s mladými (1 mesiac dopredu)
5. **E-mail** = odpoveď na prihlásenie – **Potvrdenie registrácie** – posielať každému zaregistrovanému účastníkovi
6. **Menovky** Organizátor
7. **Občerstvenie** – objednať v jedálni koláče alebo kúpiť keksy, slané tyčinky a pod.
8. **Tekutiny**: 0,5 l vody pre každého účastníka a lektora
9. **Obedy** - objednať v jedálni
10. **Email** = **Pripomienka akcie** – 2 dni pred podujatím poslať každému zaregistrovanému účastníkovi
11. **Plagát** – rezervácia učebne – na farebný papier alebo farebne vytlačiť a nalepiť na učebne
12. **Harmonogram podujatia a obsah prednášky**/workshopu nalepiť na učebne
13. **Prezenčná listina** - účastníci podpíšu na vrátnici školy (2 + 2 žiačky - podpisy a odprevádzanie do prednáškovej miestnosti).
14. **Potvrdenie o účasti** – pečiatka a podpis pre účastníkov
15. **Informácia** o workshopoch na školách pre učiteľov na papier vytlačiť
16. **Heslá** na internet
17. **Papierová taška** – dať: pero, zápisník, keksík, propagačné materiály o škole, o UPJŠ, CSIRT, potvrdenie o účasti, heslo na internet, lístok na obed, info o KyberTíme pre učiteľov.

18. **Počítače** – poobede pred podujatím nastaviť do každého a prihlásiť HOST
19. **Prezentácia** - názov podujatia a logá organizátorov (Obrázok 20)
20. **Bannery** – gym, CSIRT-UPJS, ESET.. - bannery organizátorov vystaviť v prednáškovej miestnosti.
21. **Workshop** – 2 + 1 ľudia - 2 prednášajúci a jeden na pomoc pri práci s počítačom. Ak je práca s emailami, treba ich v každom počítači pootvárať a pripraviť už pred workshopom.
22. **Kvíz** - cez wooclap (väščie písmo nastaviť v prehliadači alebo použiť väčšie písmo už pri tvorbe prezentácie; zvukové ukážky púšťať cez mikrofón)
23. **Odmeny** do kvízu - pre 3 – 5 prvých miest pripraviť.
24. **Formulár** na spätnú väzbu alebo urobiť QR kód a hneď po kvíze dať vyplniť účastníkom
25. **Email s poďakovaním a linkou na spätnú väzbu** – po podujatí poslať emailom každému účastníkovi
26. **Článok** na web, FB, Instagram.

10 WORKSHOPY PRE SENIOROV

Workshopy pre seniorov môžu žiaci zorganizovať na svojej strednej škole alebo môžu navštíviť domov dôchodcov (Obrázok 22). Treba si pripraviť viaceré alternatívy workshopu. Niektorí seniori majú mobilné zariadenia, prípadne počítače, a používajú ich. Niektorí nie. Používajú mobil len na telefonovanie a posielanie SMS správ. Ale obe skupiny je potrebné upozorniť na rôzne možnosti podvodov, ktoré používanie týchto zariadení prináša.

Pri senioroch je potrebné vhodne zvoliť terminológiu, aby sme ich nezahltili príliš veľkým množstvom pojmov, ktoré si nezapamätajú alebo ktoré vôbec nepočuli a nepotrebujú ovládať. Skôr sa treba zamerať na rôzne spôsoby podvodov, s ktorými sa môžu stretnúť, a vysvetlenie založiť na skúsenosti a bežných pojmoch, ktorým rozumejú. Seniori nevyhnutne nemusia presne ovládať pojmy ako phishing, vishing, quishing a pod., ale potrebujú sa naučiť, že nemôžu veriť každému, kto im zatelefonuje, alebo pošle SMS správu. Potrebujú sa naučiť rozlišovať znaky podvodných správ a telefonátov a naučiť sa, akým spôsobom si volajúceho môžu overiť. Pre svoj každodenný život nepotrebujú presne pomenovať pojmy, ale mali by sa naučiť možnosti prevencie a ochrany pred podvodníkmi. Na to treba myslieť, keď žiaci pripravujú prezentáciu pre seniorov, či už na prednášku alebo praktický workshop.

Ďalším špecifikom práce so seniormi je čas, resp. trvanie prednášky/workshopu. Mali by sme pri plánovaní aktivít myslieť na to, že nie kvantita, ale kvalita je dôležitá. Informácie je potrebné vhodne a zrozumiteľne vysvetliť a praktické veci ukázať a pomôcť zrealizovať. Pri realizácii takýchto workshopov je dobré, ak prezentuje jeden alebo dvaja a žiaci a niekoľko žiakov je k dispozícii, aby pomohli seniorom s praktickými aktivitami. Závisí to od veľkosti vzdelávanej skupiny. Vysvetlime žiakom, že nie je dôležité prezentovať naraz príliš veľa informácií, ale radšej menej a zrozumiteľne, aby si ich ľudia zapamätali a vedeli použiť.

Praktické aktivity a prednášku je potrebné striedať, aby neklesala pozornosť a tak isto treba naplánovať a dodržať aj prestávky, aby sme poslucháčov príliš nezahltili informáciami a neunavili. Na záver aktivity pre seniorov môžeme tiež zaradiť kvíz z osvojených vedomostí.

Obr. č. 22 – Plagát na podujatie pre seniorov

ZÁVER

Práca so žiakmi na projekte takéhoto rozmeru si vyžaduje veľa trpezlivosti. Zo začiatku sa môžete stretnúť s ich veľkým nadšením, ktoré postupne s pribúdajúcimi aktivitami a inými povinnosťami môže opadnúť. Preto je potrebné ich neustále motivovať a povzbudzovať. Plánujte rôznorodé aktivity, aby sa žiaci pri nich nielen vzdelávali, ale aj zabavili, aby sa rozvíjali a postupne nadobudnuté vedomosti vedeli podať ďalej.

Po piatich rokoch dobrovoľníckej činnosti a stretávania sa vo voľnom čase plánujeme v budúcom školskom roku ponúknuť žiakom voliteľný predmet Informačná a kybernetická bezpečnosť. Pre lepšiu koordináciu činností a prípravu aktivít tímu sa ukazuje táto možnosť ako najlepšia. Stabilný čas na spoločné stretnutia je predpokladom na aktívnejšiu prácu žiakov a určite poskytne priestor pre realizáciu nových nápadov z oblasti informačnej bezpečnosti.

Práca žiakov v kybernetickom bezpečnostnom tíme na škole a realizácia rôznych bezpečnostných aktivít pre žiakov, učiteľov, rodičov i seniorov je veľkým prínosom. Nielen pre žiakov, ktorí sa v budúcnosti plánujú zaoberať informačnou a kybernetickou bezpečnosťou, ale pre všetkých žiakov. Zlepšujú svoje prezentačné zručnosti, učia sa pracovať v tíme a plánovať si čas a mnoho ďalších zručností, ktoré v budúcnosti určite využijú.

Veríme, že táto krátka príručka bude inšpiráciou pre iné stredné školy, pre učiteľov aj pre žiakov, aby nabrali odvahu a skúsili urobiť niečo nielen pre seba, ale aj pre svoje okolie. Aby sa vzdelávali v oblasti informačnej bezpečnosti, ktorá je v dnešnej digitálnej dobe už nevyhnutnosťou a aby nadobudnuté poznatky dokázali posúvať aj ďalej, svojmu okoliu a ľuďom, ktorí nemajú taký prístup k informáciám a takto spoločne zvyšovali bezpečnostné povedomie.

POUŽITÉ ZDROJE

[1] ESET. Generátor hesiel. Dostupné na: https://www.eset.com/sk/generator-hesiel/

[2] CSIRT-UPJS. Phishingový test. Dostupné na: https://csirt.upjs.sk/phishing/

[3] IstroSec. Phishing test. Dostupné na: https://istrosec.com/sk/e-learning/phishing-test/test/

[4] CSIRT.SK. Phishingový test – návody a odporúčania. Dostupné na: https://www.csirt.gov.sk/archiv/osvedcene-postupy/navody-a-odporucania/phishingovy-test-871.html

[5] Safelab. Phishingový online test. Dostupné na: https://safelab.sk/internetova-bezpecnost/phishingovy-online-test

[6] CSIRT-UPJS. Tester hesiel. Dostupné na: https://hesla.csirt.upjs.sk/

[7] ITcity. Overenie hesla. Dostupné na: https://www.itcity.sk/heslo/overenie/

[8] VirusTotal. Analyze suspicious files and URLs. Dostupné na: https://www.virustotal.com/gui/home/upload

[9] urlscan.io. URL and website scanner. Dostupné na: https://urlscan.io/

[10] Hunt, T. Have I Been Pwned. Dostupné na: https://haveibeenpwned.com/

[11] Slovenská sporiteľňa. Bezpečnosť – kvíz. Dostupné na: https://www.slsp.sk/sk/ludia/bezpecnost

[12] Slovenská sporiteľňa. Bezpečnostný test. Dostupné na: https://www.slsp.sk/sk/ludia/bezpecnost#/modalComponent/isOpen/true/url/%2Fsk%2Fconfiguration%2Fleads%2Fbezpecnost-test%2Fotazka1.modal

[13] Tatra banka. Test digitálnej bezpečnosti. Dostupné na: https://www.tatrabanka.sk/predigitalnubezpecnost/test-digitalnej-bezpecnosti/

[14] YouTube. Veštec – zdieľanie údajov na internete [Video]. Dostupné na: https://www.youtube.com/watch?v=F7pYHN9iC9I

[15] PPPíter. Vishing [Video]. Dostupné na: https://www.youtube.com/watch?v=AzTNrtQ6v_o

[16] PPPíter. Scam [Video]. Dostupné na: https://www.youtube.com/watch?v=B1bM5aa4OqI

[17] PPPíter. Phishing [Video]. Dostupné na: https://www.youtube.com/watch?v=2ek-KeYRWdc

[18] McKillop, B. Quishing phishing cyber [LinkedIn post]. Dostupné na: https://www.linkedin.com/posts/ben-mckillop-0a07a5123_quishing-phishing-cyber-ugcPost-7251509680324120577-ddL_

[19] YouTube. Ella a jej odkaz rodičom [Video]. Dostupné na: https://www.youtube.com/watch?v=F4WZ_k0vUDM

[20] LinkedIn. Sharenting – slovenská verzia [Video]. Dostupné na: https://www.linkedin.com/embed/feed/update/urn:li:activity:7089225446944321536