
UNIVERZITA KONŠTANTÍNA FILOZOFA
V NITRE

Bezpečnosť na internete

Jan Francisti

2023

Bezpečnosť na internete

Edícia Prírodovedec č. 838

Autor:
Mgr. Jan Francisti, PhD.

Recenzent:
RNDr. Ján Skalka, PhD.

Publikácia bola vytvorená v rámci projektu 001UKF-2-1-2022 Zvyšovanie kvality prípravy budúcich učiteľov matematiky, fyziky, chémie, informatiky, anglického jazyka, slovenského jazyka a techniky formou doplňujúceho pedagogického štúdia a rozširujúceho štúdia. Rukopis neprešiel jazykovou úpravou.

ISBN 978-80-558-2114-6

Obsah

ÚVOD

V súčasnej dobe, kedy internet prenikol do každej oblasti nášho života, kybernetická bezpečnosť sa stala kľúčovou záležitosťou pre každého, kto používa internet. Vzhľadom na to, že internet sa stal nedeliteľnou súčasťou našej komunikácie, zdieľanie informácií je nevyhnutné, aby sme si uvedomili všetky riziká a nebezpečenstvá, ktoré sú s ním spojené.

Jednou z najväčších výziev, ktorým musíme čeliť, sú sociálne siete a dezinformácie, ktoré na nich kolujú. V posledných rokoch sa stalo bežným, že na sociálnych sieťach sa šíria hoaxy, falošné správy a neoverené informácie. Tieto dezinformácie môžu mať škodlivé následky a môžu ovplyvniť verejnú mienku a politické rozhodnutia. Preto je dôležité, aby sme si uvedomili, že každý, kto používa internet, má zodpovednosť overiť si pravdivosť informácií, ktoré zdieľa.

Súkromie a bezpečnosť osobných údajov je ďalšou veľkou výzvou. S každým kliknutím na internete zanechávame digitálne stopy, ktoré môžu byť použité proti nám. Firmy často zhromažďujú a predávajú osobné údaje, ktoré sme zanechali na internete, čo môže viesť k zneužitiu našich údajov a identity. Preto je dôležité chrániť svoje súkromie a uvedomiť si, kto môže mať prístup k našim osobným údajom.

Hackovanie je ďalším veľkým problémom v kybernetickej bezpečnosti. Hackeri môžu získať prístup k našim zariadeniam a účtom a ukradnúť naše osobné údaje, financie a dokonca aj identitu. Preto je dôležité mať silné heslá a zabezpečiť svoje zariadenia proti útokom.

Kyberšikana a online šikanovanie sú ďalšími rizikami, ktorým môžu byť vystavení používatelia internetu. Online šikana môže mať veľký vplyv na psychiku a duševné zdravie ľudí, ktorí sú jej obeťou. Preto je dôležité, aby sme si uvedomili, že takéto správanie nie je akceptovateľné a že by sme mali podporovať bezpečné a rešpektujúce správanie na internete.

Kritické myslenie je ďalšou dôležitou zručnosťou, ktorú by sme mali mať pri používaní internetu. V dnešnej dobe, kedy sú informácie tak ľahko dostupné, môže byť ťažké rozlíšiť medzi pravdivými a falošnými informáciami. Preto by sme mali byť schopní analyzovať a hodnotiť informácie, ktoré vidíme na internete, a zistiť, či sú pravdivé alebo nie.

Gaming je ďalšou oblasťou, ktorá sa stáva súčasťou nášho online sveta. Pri hraní hier online sa môžeme stretávať s rôznymi nebezpečenstvami, ako sú podvody, phishing, útoky hackerov a ďalšie. Preto by sme mali mať na pamäti, že aj v hernom svete platia rovnaké pravidlá bezpečnosti ako v reálnom svete.

1 POCHOPENIE KYBERNETICKEJ BEZPEČNOSTI

V nasledujúcej podkapitole sa dozviete bližšie o samotnej kybernetickej bezpečnosti, ale aj o pojme kybernetika či bezpečnosť.

Kybernetická bezpečnosť je čoraz viac dôležitejšou oblasťou, ktorá si v poslednom čase získala značnú pozornosť kvôli rastúcej závislosti na informačných technológiách a ich využívaniu v osobnom aj profesionálnom prostredí. Kybernetické hrozby môžu mať rôzne formy, ako napríklad malvér, ransomvér, phishingové útoky (pojmy, o ktorých si povieme v pokračovaní kurzu) či iné činnosti, ktoré môžu ohroziť citlivé údaje a poškodiť fungovanie systémov.

V slovníku cudzích slov je pod pojmom kybernetika označená všeobecná veda o riadení, prenose a spracúvaní informácií v živých organizmoch, v technických a sociálnych systémoch a o vzájomných vzťahoch medzi týmito systémami.

Pre potreby knihy, kybernetiku však budeme považovať vedeckú štúdiu ktorá sa zaoberá komunikáciou a riadením systémov ktoré využívajú technológiu.

Všeobecne sa dá tvrdiť, že bezpečnosť je ochrana aktív pred hrozbami, pričom za aktíva považujeme všetko čo má pre danú organizáciu či jednotlivca hodnotu. Môže ísť o hmotné veci, rovnako môže ísť aj o nehmotné veci ako informácie, údaje, dobré meno či poznatky. Hrozby sú akékoľvek udalosti, skutočnosti či osoby ktoré môžu dostať aktíva do neželaného stavu.

Medzinárodný štandard ISO definuje informačnú bezpečnosť ako zachovanie dôvernosti, integrity a dostupnosti informácií. Dôvernosť, integrita a dostupnosť sú základné piliere na ktorých informačná bezpečnosť stojí.

Požiadavka na dôvernosť zaisťuje že je informácia chránená pred prezradením neoprávnenej osobe.

Požiadavka na integritu zasa chráni údaje pred úmyselnou alebo náhodnou zmenou ktorá môže mať vplyv na platnosť údajov.

Dostupnosť nám zasa zabezpečuje to aby bola daná informácia či údaj k dispozícii kedykoľvek a kdekoľvek keď o to používateľ žiada.

Hlavnou úlohou kybernetickej bezpečnosti je ochrana fyzickej časti počítača (hardvéru), ochrana programového vybavenia počítača (softvéru) a v neposlednom rade ochrana dát pred kybernetickými útokmi.

1.1 Pojmy v kybernetickej bezpečnosti

Pri kybernetickej bezpečnosti sa nachádza veľké množstvo pojmov, ktoré úzko súvisia a do kybernetickej bezpečnosti patria. V pokračovaní podkapitole sú detailnejšie popísané základné pojmy a technológie, ktoré využívajú kybernetickí zločinci pri realizácii rôznych útokoch a preto je dôležité ich poznať a ovládať. Na druhej strane sú popísané aj nástroje

alebo technológie, ktoré napomôžu používateľovi zabezpečiť využívané nástroje, operačný systém ale aj samotné zariadenie, za účelom aby sa nestál obeťou kybernetického útoku.

Antivírusový nástroj je počítačový softvér, ktorý sa používa na prevenciu, zisťovanie a odstraňovanie škodlivého softvéru. Antivírus chráni počítač pred veľkým množstvom hrozieb, ako je napríklad ransomvér, rootkity, trójske kone a spyware, phishingové útoky alebo botnety.

Exploit je časť softvéru, časť údajov alebo súbor príkazov, ktorý využíva chybu, poruchu alebo zraniteľnosť operačného systému alebo softvéru na škodlivé účely. Exploit môže spôsobiť narušenie správanie sa počítačového softvéru, hardvéru alebo iných zariadení.

Kybernetický útok je klasifikovaný ako akýkoľvek typ útoku na počítač alebo iné zariadenie komunikujúce v sieti, ktorú používajú kybernetickí zločinci na nasadenie škodlivého kódu do zariadenia s cieľom ukradnúť, zmeniť, zničiť alebo získať akúkoľvek výhodu z tejto akcie.

Malvér je jedným z pojmov, s ktorým sa používateľ najčastejšie stretne, keď sa hovorí o kybernetických bezpečnostných hrozbách. Tento pojem definuje akýkoľvek softvér používaný kybernetickými útočníkmi na: narušiť počítačovej operácie, zhromažďovanie citlivých informácií alebo o nezákonnom získavaní prístupu k súkromným operačným systémom.

Malvérová reklama (Malvertising) je spôsob využívania online reklamy na šírenie škodlivého softvéru. Kybernetickí zločinci vkladajú do online reklamných sietí alebo legitímnych webových stránok škodlivý kód alebo kód so škodlivým softvérom, ktorý potom infikuje operačný systém kliknutím, presmerovaním alebo stiahnutím na disk.

Oprava (Patching) je proces aktualizácie softvéru na inú, novšiu verziu. Záplata je malá aktualizácia vydaná výrobcom softvéru na opravu chýb v existujúcich programoch. Oprava sa môže týkať funkcií a použiteľnosti, ale môže zahŕňať aj bezpečnostné funkcie.

Phishing je ďalšia metóda, ktorú kybernetickí zločinci používajú na získanie citlivých informácií, ako sú používateľské mená, heslá a údaje o kreditných kartách, a to tak, že sa v e-mailoch alebo iných prostriedkoch elektronickej komunikácie vydávajú za dôveryhodný subjekt.

Ransomvér je forma škodlivého softvéru, ktorý v podstate zadržiava operačný systém alebo nástroje "v zajatí" a požaduje výkupné.

Sociálne inžinierstvo je jedna z najčastejšie používaných metód kybernetického útoku, ktorá si vyžaduje len malé alebo žiadne technológie. Spolieha sa na psychologickú manipuláciu s cieľom presvedčiť obeť, aby vykonala určité činnosti alebo prezradila dôverné informácie.

Spam tvoria nevyžiadané e-maily, ktoré zahlcujú najčastejšie e-mailové schránky. Za posledné roky, sa spam rozšíril aj do aplikácií na zasielanie okamžitých správ, textových správ, blogy, fóra, vyhľadávače, zdieľanie súborov a sociálne siete.

Spyware je typ softvéru, ktorý sa snaží zhromažďovať osobné informácie bez súhlasu používateľa. Je schopný úplne ovládnuť počítač. Informácie, ktoré zhromažďuje, potom posiela tretej strane bez povolenie používateľa.

Vírus je typ škodlivého softvéru, ktorý sa dokáže replikovať a šíriť do iných počítačov a na iné údaje alebo súbory. Vírusy sa šíria do iných počítačov tak, že sa pripájajú k rôznym programom a spúšťajú kód, pokiaľ by ste spustili stiahnutí infikovaný nástroj. Vírusy sa taktiež dajú použiť na krádež informácií, poškodenie počítača, zaznamenávanie stlačených klávesov, rozosielanie spamu, krádež platobných kariet, zobrazovanie politických alebo humorných správ na obrazovke a podobne.

Vírus Zero-Day sa objavia, keď kybernetickí zločinci objavia chybu v softvéri. Využijú túto zraniteľnosť a spustia útok. Pokiaľ používatelia nevlastnia najaktuálnejšiu verziu cieľového softvéru, nemajú aktualizovaný antivírus alebo ho vôbec nemajú, proti tomuto typu útoku nie sú schopní sa brániť.

Technológia filtrovania URL (Uniform Resource Locator) alebo webového obsahu predstavuje softvér ktorého úlohou je zabrániť prístup na nevhodné webové lokality alebo obsah. Softvérový filter kontroluje pôvod alebo obsah webovej stránky na základe súboru pravidiel poskytnutých spoločnosťou alebo osobou, ktorá filter URL nainštalovala. Ak bola webová stránka zaradená na čiernu listinu alebo bola označená ako infikovaná, zámedzí prístup na webové miesto, čím dosiahne blokovanie potenciálnych kybernetických útokov.

Trojan (Trójsky kôň) je typ škodlivého softvéru, ktorý sa skrýva ako bežný súbor alebo program, ktorého účelom je oklamať a prinútil stiahnuť a nainštalovať škodlivý softvér.

Trojský kôň môže v operačnom systéme spôsobiť mnoho nebezpečných vecí, napríklad poskytnúť kybernetickým zločincom neoprávnený vzdialený prístup k infikovanému počítaču.

Zaznamenávanie klávesov (keylogging) je metóda, ktorú kybernetickí zločinci používajú na zaznamenávanie stlačených klávesov na klávesnici s cieľom získať o dôverné informácie ako napríklad rôzne prihlasovacie údaje (sociálne siete, e-mailový klient, internet bankovníctvo a podobne). Útočníkom (ktorým sa podarí spomínaní nástroj do zariadenia inštalovať) to robia skrytým spôsobom, aby sa používateľ nedozvedel, že je sledovaní pri písaní hesiel, adries a iných osobných údajov na klávesnici.

Zraniteľnosť (Vulnerability) je slabé miesto, ktoré umožňuje útočníkovi narušiť bezpečnosť údajov v systéme.

Zneužitie zraniteľnosti systému môžeme rozdeliť do niekoľkých fáz:

- náchylnosť alebo chyba systému,
- prístup útočníka k chybe,
- schopnosť útočníka zneužiť chybu.

1.2 Otestujte svoje znalosti z témy ohľadom kybernetickej bezpečnosti

V pokračovaní podkapitoly sa nachádzajú rôzne otázky ohľadom kybernetickej bezpečnosti. Skúste si otestovať znalosti z kybernetickej bezpečnosti a odpovedať správne na čim viac otázok.

Otázka 1: Čo je phishing?

a) Spôsob útokov na fyzické objekty prostredníctvom kybernetických zariadení.

b) Získavanie citlivých informácií, ako sú heslá a bankové údaje, pomocou podvodného e-mailu alebo webovej stránky.

c) Proces zvýšenia rýchlosti internetového pripojenia prostredníctvom špecializovaného softvéru.

d) Metóda skenovania siete na identifikáciu zraniteľností.

Otázka 2: Čo je dvojfaktorová autentifikácia?

a) Proces vytvárania dvoch identických kópií dôležitých súborov pre zabezpečenie redundancie.

b) Spôsob overovania identity používateľa pomocou dvoch rôznych faktorov, napríklad hesla a jednorazového kódu.

c) Technika šifrovania údajov, aby sa zabránilo ich neoprávnenej činnosti.

d) Aktualizácia softvéru na najnovšiu verziu na zlepšenie bezpečnosti.

Otázka 3: Čo je ransomvér?

a) Druh škodlivého softvéru, ktorý využíva zraniteľnosti operačného systému na získanie kontroly nad počítačom.

b) Technika odpočúvania a odchytávania komunikácie na sieti.

c) Typ útoku, pri ktorom útočník ukradne citlivé informácie a neskôr ich pošle obetiam.

d) Malvér, ktorý šifruje súbory na počítači obete a požaduje výkupné za ich dešifrovanie.

Otázka 4: Čo je firewall?

a) Fyzické zariadenie, ktoré monitoruje a kontroluje tok dát medzi sieťami

b) Počítačový program na vytváranie a upravovanie dokumentov

c) Metóda prenosu dát medzi počítačmi pomocou bezdrôtovej technológie

d) Proces zálohovania údajov na externé zariadenie na ochranu pred stratou dát

Otázka 5: Čo je sociálne inžinierstvo?

a) Výskum a vývoj nových sociálnych sietí a komunikačných platforiem

b) Metóda využívaná útočníkmi na manipuláciu a získavanie citlivých informácií od ľudí

c) Bezpečnostný postup na ochranu osobných údajov

d) Ochrana sieťovej infraštruktúry pred neoprávneným prístupom

Otázka 6: Čo je VPN?

a) Proces odstraňovania vírusov a malvéru z počítačového systému

b) Bezpečný spôsob pripojenia k sieti cez verejný internet, ktorý zabezpečuje súkromie a šifrovanie

c) Sieťová architektúra pre prenos dát medzi rôznymi počítačmi v organizácii

d) Metóda ochrany súborov pred neoprávneným prístupom pomocou hesiel a oprávnení

Otázka 7: Čo je malvér?

a) Bezpečnostný protokol na overovanie identity používateľa

b) Fyzický hardvér, ktorý zabraňuje neoprávnenému prístupu k počítaču

c) Počítačový program, ktorý je navrhnutý na spôsobenie škody alebo získavanie neoprávnených prístupových práv

d) Metóda zálohovania údajov na externý server

Otázka 8: Čo je bruteforce útok?

a) Spôsob útoku na sieť, pri ktorom sa útočník pokúša získať neoprávnený prístup prostredníctvom manipulácie s údajmi

b) Technika prelomenia ochrany heslom prostredníctvom systematického skúšania všetkých možných kombinácií

c) Proces vytvárania zálohových kópií údajov na viacerých fyzických zariadeniach

d) Metóda získavania citlivých informácií pomocou podvodného e-mailu alebo webovej stránky

Otázka 9: Čo je zero-day zraniteľnosť?

a) Metóda skenovania siete na identifikáciu nových bezpečnostných rizík

b) Zraniteľnosť systému, ktorá je známa až po tom, čo ju útočník zneužil

c) Špeciálny typ firewallu, ktorý zabraňuje útokom z vnútra siete

d) Proces aktualizácie softvéru na najnovšiu verziu na zlepšenie bezpečnosti

Otázka 10: Čo je SQL injection?

a) Typ útoku, pri ktorom útočník vkladá škodlivý kód do databázových dotazov na manipuláciu s údajmi

b) Technika odstraňovania škodlivého softvéru z počítačového systému

c) Metóda zálohovania údajov do cloudu

d) Proces vytvárania zálohových kópií dôležitých súborov pre obnovu po havárii

Pokiaľ ste na niektoré otázky nevedeli správne odpovedať, alebo ste si odpoveďou neboli istý, tento kurz je určený práve pre Vás. Práve kurz o kybernetickej bezpečnosti Vás prevedie a poukáže na všetky uvedené fakty a vyvráti rôzne mýty, ktoré kolujú na internete práve zamerané na bezpečnosť v kybernetickom priestore.

2 SOCIÁLNE SIETE

Stránky sociálnych sietí dramaticky zmenili spôsoby, akými sa ľudia navzájom spájajú. Mnohí ľudia vytvárajú a udržiavajú svoje sociálne vzťahy na webe. V nasledovnej kapitole si bližšie priblížime čo sú to sociálne siete, ako fungujú, aké nebezpečenstva môžu číhať na sociálnych sieťach a ako sa voči ním chrániť.

2.1 Ako fungujú a na čo slúžia sociálne siete

Sociálne siete definujeme ako webové služby, ktoré umožňujú používateľom vytvoriť si verejný alebo poloverejný profil v rámci ohraničeného systému, vytvoriť zoznam ostatných používateľov, s ktorými majú spoločné spojenie, a prezerať si a prechádzať svoj zoznam spojení a spojenia vytvorené ostatnými v rámci systému.

Jedinečnosť stránok sociálnych sietí nespočíva v tom, že umožňujú používateľom stretávať sa s cudzími ľuďmi, ale skôr v tom, že umožňujú používateľom vyjadriť a zviditeľniť svoje sociálne siete. To môže viesť k spojeniam medzi používateľmi, ktoré by sa inak nenadviazali, ale často to nie je cieľom, a tieto stretnutia sú často medzi "latentnými väzbami", ktoré majú nejaké spoločné offline spojenie.

Na mnohých sociálnych médiách používatelia nevyhnutne nehľadajú nových ľudí, ale komunikujú predovšetkým s ľuďmi, ktorí už sú súčasťou ich rozšírenej sociálnej siete.

Základom sociálnych sietí sú viditeľné profily, ktoré zobrazujú zoznam priateľov, ktorí sú zároveň používateľmi systému. Po vstupe na sociálnu sieť sa od nového používateľa požaduje, aby vyplnil formuláre obsahujúce sériu otázok, pomocou ktorých sa vytvorí profil. Profil zvyčajne obsahuje deskriptory ako vek, miesto pobytu, záujmy, časť "o mne" a nahratie profilovej fotografie.

Verejné zobrazovanie spojení je kľúčovou súčasťou sociálnych sietí. Zoznam priateľov obsahuje odkazy na profil každého priateľa, čo umožňuje ostatným používateľom prechádzať sieťovým grafom klikaním na zoznamy priateľov.

Väčšina sociálnych sietí poskytuje používateľom aj mechanizmus na zanechávanie správ na profiloch svojich priateľov. Táto funkcia zvyčajne zahŕňa zanechávanie "komentárov". Okrem toho majú sociálne siete často funkciu súkromných správ podobnú webovej pošte.

Keďže sme zistili, čo sú to sociálne siete a ako fungujú, môžeme si predstaviť nebezpečenstvá, ktorým môžeme na sociálnych sieťach čeliť.

2.2 Základné pravidla, ktorými sa treba riadiť na sociálnych sieťach

2.2.1 Nevyprovokujte sa internetovými trollmi

Internetoví trollovia sú provokatéri, ktorí sa zapájajú do diskusií, aby podráždili ostatných používateľov pre určitý druh "zábavy". Trollov môžete nájsť všade: na fórach, chatoch a

iných platformách pre online komunikáciu. Oblasti komentárov v spravodajských médiách sú známe vysokou účasťou trollov. Určite ich sú húfy aj na sociálnych sieťach.

Príklad: V dôsledku kyberšikany, ktorá zahŕňala swatting a iné zásahy do offline sveta, prišiel jeden americký pár o čas, peniaze, prácu a nakoniec aj o manželstvo [1] .

Mnohí ľudia sa chytia na návnadu a začnú horúce debaty, v ktorých sa snažia vysvetliť svoj názor a márne strávia veľa času a úsilia. Na internete sa vždy niekto mýli - nestrácajte čas a energiu na trollov. Najlepšia reakcia je ignorovanie.

2.2.2 Nezverejňujte nič nezákonné

V mnohých krajinách ako napríklad Spojené Arabské Emiráty alebo Nový Zéland platia zákony, ktoré prísne trestajú trollovanie a kyberšikanovanie, pričom tresty sa pohybujú vo vysokých číslach.

Napriek tomu môžete vo väčšine krajín dostať pokutu alebo čeliť ešte vážnejším dôsledkom za príspevky, reposty a iné činnosti na sociálnych sieťach.

Príklad: Dvaja muži boli odsúdení na štyri roky väzenia po tom, čo vytvorili udalosť na Facebooku, ktorá nabádala k výtržnostiam. Muž v Bangladéši bol odsúdený na trest odňatia slobody za to, že žartoval o tom, že si želá smrť premiéra [2].

Preto by ste mali poznať zákony vo svojej krajine a pamätať si ich, keď niečo zverejňujete na sociálnu sieť.

2.2.3 Nezdieľajte podvodné informácie (scamy)

Podvodníci často klamú obete šokujúcimi príbehmi o umierajúcich deťoch, topiacich sa šteniatkach alebo veteránoch v ťažkej situácii. Takéto príspevky putujú po sociálnych sieťach zamaskované ako výzvy o pomoc. V skutočnosti sa používajú na finančné krádeže, phishing a šírenie škodlivého softvéru (hrozby, o ktorých si detailne povieme v časti o hackeroch).

Príklad: Chovateľ psov sľubuje, že pošle psy, ak majiteľ zvierat prevedie peniaze na pokrytie nákladov na leteckú dopravu. Niekoľko dní po odoslaní peňazí kupujúceho opäť kontaktuje podvodník, ktorý tvrdí, že potrebuje ďalšie peniaze na náklady, ako je očkovanie a cestovné poistenie [3].

Preto je lepšie byť ostražitý a každý príspevok skontrolovať skôr, ako kliknete na jeho tlačidlo "To sa mi páči" alebo "Zdieľať". Pokiaľ si neiste istý či je príspevok pravdivý, potom naň neklikajte vôbec - neriskujte, že zo seba a svojich priateľov urobíte obete podvodu.

2.2.4 Nezverejňujte svoje súkromné údaje

Mnohé sociálne siete ponúkajú "zaškrtnutie" miesta, kde ste niečo odfotili alebo zverejnili, alebo zobrazenie miest, ktoré ste navštívili. Ak sa zaujímate o nejakú udalosť, sociálna sieť môže upozorniť vašich priateľov v prípade, že sa chcú pridať. Štandardne má k týmto

údajom prístup ktokoľvek a zločinci majú tisíc a jeden spôsob, ako ich využiť, od vlámania sa do vášho domu až po krádež vašej digitálnej identity.

Príklad: Údaje z roku 2017 hovoria, že 78 % zlodejov využíva sociálne médiá na to, aby sa zamerali na nehnuteľnosti [4].

Je to tiež dobrý dôvod, aby ste si bez rozdielu nepridávali do zoznamu priateľov: Ľudia, ktorí posielajú žiadosti o spojenie s vami, môžu byť boti, trollovia alebo dokonca zločinci.

2.3 Aké nebezpečenstvá sa môžu skrývať na sociálnych sieťach

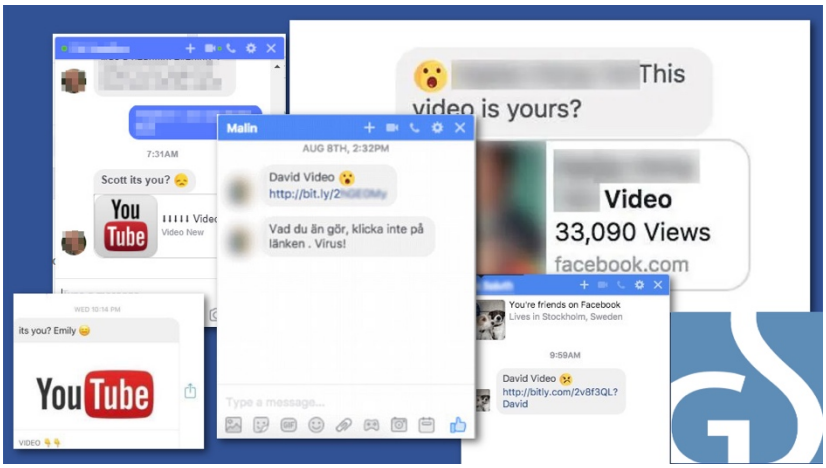
V dnešnej digitálnej ére sa sociálne siete stali neoddeliteľnou súčasťou nášho každodenného života. Poskytujú nám platformu na komunikáciu, zdieľanie zážitkov a udržiavanie kontaktov so známymi aj vzdialenými osobami. Napriek ich pozitívnym aspektom však nemožno prehliadať ani potenciálne nebezpečenstvá, ktoré sa na týchto platformách môžu skrývať. V tejto podkapitole sa budeme venovať preskúmaniu rôznych foriem rizík, ktorým sa môžu používatelia sociálnych sietí vystaviť.

2.3.1 Krádež identity

Keďže v súčasnosti používatelia na sociálnych sieťach zverejňujú rôzne informácie, práve tento druh údajov predstavuje pre útočníkov priame materiály pre krádež identity. Dátum narodenia, počet súrodencov škola, práca, ktorú používateľ navštevuje, predstavujú len malú skupinu informácií, ktoré môžu útočníci zneužiť. V minulosti útočníci, ktorým bolo cieľom ukradnúť identitu, museli venovať viac času a úsilia aby od danej obete získali nejaké informácie a v súčasnosti, ich majú takmer na jednom mieste.

2.3.2 Šírenie škodlivého softvéru

Okrem iných kanálov, útočníci šíria škodlivý softvér aj prostredníctvom sociálnych sietí, napr. cez správy, komentáre alebo príspevky, kde je jedinou úlohou útočníka aby obeť danú správu otvorila, resp. vykonala čo od nej vyžaduje (viac v časti phising). Pomocou krátkeho a pomerne jednoduchého kódu dokážu ukradnúť vašu identitu, zmocniť sa vášho zariadenia a údajov, ktoré sú v ňom uložené, či získať prístup k vášmu online bankovníctvu a iné. Najlepšou radou je neotvoriť odkaz pokiaľ nepoznáte jeho skutočný zdroj, prípadne



Obrázok 1 Falošné správy na sociálnych sieťach [5]

2.3.3 Špehovanie a získavanie súkromných informácií

Ako sme spomínali v pravidlách, na sociálnych sieťach sa často stretneme so zdieľaním osobných, dokonca aj dôverných informácií. Preto sa väčšina hrozieb na sociálnych sieťach spája so zneužitím osobných údajov. Ak raz informáciu nahráme verejne do online sveta, už sa z neho nikdy "nevymaže", rovnako už nikdy nebude dôverná, či tajná. Čím viac informácií poskytnete, tým ste zraniteľnejší. Ako v reálnom, tak aj vo virtuálnom svete.

2.3.4 Zlodeji reálneho sveta na sociálnych sieťach

Veľké množstvo ľudí si neuvedomuje aké nebezpečenstvo môže na nich číhať, pokiaľ zverejnia čo i len krátku informáciu, že sa napríklad chystajú na dovolenku. Fotografia destinácie a dátumu odletu a príspevok je v online priestore. Zlodej, ktorý takýto príspevok uvidí, Vám možno závidieť kam ideme na dovolenku nebude, ale určite bude vedieť, že sa doma zadržiavať nebudete a pokiaľ vie Vašu adresu, má dostatok času aby Vašu domácnosť navštívil a niečo odcudzil, či poškodil.

Spojitosti medzi virtuálnym a reálnym svetom je veľmi dôležité a treba mať na zreteli to, že čo nahráme do virtuálneho sveta, môže byť zneužite v reálnom svete.

2.3.5 Rovnocennosť informácií na sociálnych sieťach a v reálnom živote

Určite sme sa viackrát stretli so situáciou v reálnom svete, kde by vhodne prišla kombinácia tlačidiel, ktorá by vrátila krok dozadu. Podobne aj pri sociálnych sieťach je veľmi dôležité zamyslieť sa nad tým, čo chceme odoslať do internetu, lebo podobne ako pri reálnom svete ani na sociálnych sieťach neexistuje vrátiť krok dozadu (ako sme v predchádzajúcej časti spomenuli, príspevok odoslaný už nie je možné vymazať, lebo je niekde zachovaný). Prílišná sebadôvera na sociálnych sieťach môže niekedy ublížiť. Preto je veľmi dôležité sa pred odoslaním príspevku alebo napísaním komentáru zamyslieť či by sme danú myšlienku alebo informáciu povedali niekomu neznámemu len tak na ulici. Pokiaľ by sme tak neurobili,

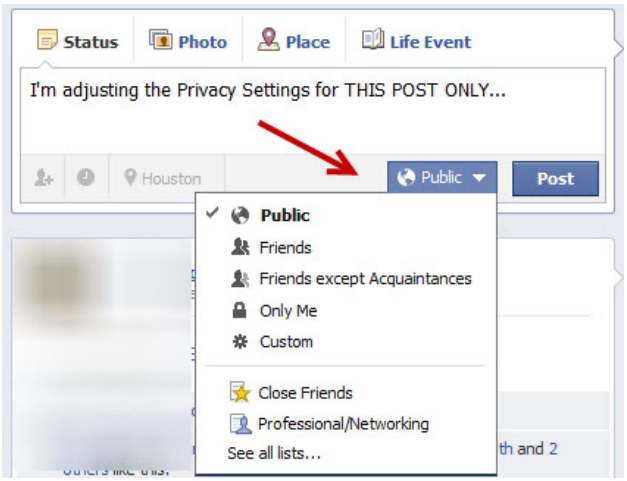
alebo nad podobnou myšlienkou zaváhali, tak ju určite netreba zdieľať ani na sociálnych sieťach, ani ak je napísaná z pohodlia domova alebo dovolenky.

2.4 Ochrana súkromia na sociálnych sieťach

Na sociálnych sieťach sa často stretneme s tým, že používatelia nezodpovedne zdieľajú svoje osobné údaje, vo väčšine prípadov dobrovoľne. Z predchádzajúcich podkapitol sme si bližšie povedali a zistili aké následky môžu nastáť, pokiaľ sa tieto údaje dostanú do nesprávnych rúk. V nasledujúcej podkapitole si detailnejšie popíšeme typy, ktorých cieľom je zvýšiť spôsob ochrany súkromia na sociálnych sieťach.

2.4.1 Bezpečnostné nastavenia v sociálnych sieťach

Je dôležité sa uistiť, že vaše fotky a príspevky na sociálnych sieťach sú viditeľné len pre tých ľudí, pre ktorých sú určené (rodina, kamaráti a podobne). Ostatní neznámi používatelia by nemali mať prístup k vašim osobným informáciám a najmä k fotkám vašich detí.



Obrázok 2 Nastavenie spôsobu zobrazovanie príspevkov na Facebooku [6]

2.4.2 Nezdieľanie lokality

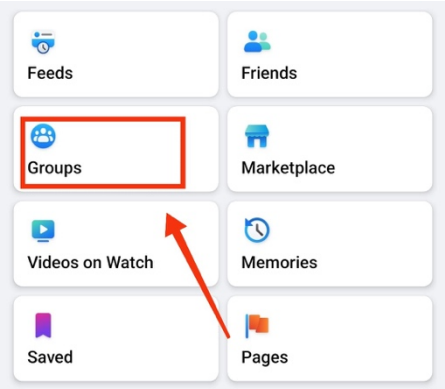
Funkcia automatického označovania geografického miesta na sociálnych sieťach môže mať svoje nevýhody, ako to dokázal prípad manželky jazdca Formuly 1 Jensona Buttona, ktorej zásnubný prsteň v hodnote 250-tisíc libier bol ukradnutý počas dovolenky vo Francúzsku a údajne bol možno identifikovaný práve vďaka tejto funkcii na sociálnej sieti [7].

Preto je dôležité byť opatrný pri používaní tejto funkcie a zvážiť, či chcete zdieľať svoju polohu a osobné informácie s ostatnými na internete.

2.4.3 Členstvo v skupinách

Je dôležité pravidelne prehodnotiť všetky online skupiny, do ktorých sme sa prihlásili, a zistiť, či sú stále relevantné a aktívne. Niektoré z týchto skupín môžu byť staré a ich

nastavenia zastarané, čo môže viesť k nežiadúcemu zdieľaniu osobných informácií. Ak sú skupiny verejné, ich obsah si môže prezrieť ktokoľvek na internete, a preto je dôležité zabezpečiť, aby boli nastavenia skupín aktualizované a aby sa zdieľali len tie informácie, ktoré sú určené pre konkrétnu skupinu ľudí.



Obrázok 3 Zoznam všetkých členstiev v skupinách na Facebooku [8]

2.4.4 Vyššia úroveň sebacenzúry

Je dobré si nastaviť vyššiu úroveň sebacenzúry na sociálnych sieťach. Predtým, ako napíšete nejaký komentár alebo zdieľate fotku na sociálnych sieťach, mali by ste si položiť otázku, ako by sa na to pozerala vaša stará mama alebo iná osoba, ktorú máte radi a ktorá má na vás vplyv. Ak by to bolo pre nich nepríjemné alebo by to mohlo poškodiť vašu reputáciu, mali by ste zvážiť, či by ste to mali naozaj zdieľať. Je dôležité si uvedomiť tak ako sme už spomínali, že internet si pamätá všetko, čo sa na ňom zverejní, a preto by sme mali byť opatrní a zodpovední pri zdieľaní informácií na internete.

2.4.5 Súkromné fotografie a videa

Je dôležité si dôkladne prezrieť akýkoľvek materiál, ktorý chystáte zverejniť na sociálnych sieťach, a zabezpečiť, aby v ňom neboli odhalené citlivé informácie, ako napríklad tajná skrýš náhradných kľúčov od domu alebo platobná karta. V prípade, že v materiáli sú uvedené tieto citlivé informácie, môžu sa stať terčom zlodejov a iných kriminálnikov, ktorí by mohli zneužiť tieto informácie na krádež alebo iné zločiny.

Nikdy by ste nemali zverejniť fotky svojho pasu, občianskeho preukazu alebo vodičského preukazu na sociálnych sieťach. Tieto dokumenty obsahujú osobné údaje, ktoré môžu byť zneužité pre podvodné účely, ako napríklad krádež identity alebo podvodné účty. Je dôležité chrániť svoje osobné údaje a zabezpečiť, aby neboli zverejňované na verejných miestach na internete.

2.4.6 Silné heslo a spôsob vyhľadávania

K podkapitole o heslách sa dostaneme v pokračovaní tejto knihe, kde si okrem iného povieme, že je dôležité mať rôzne heslá pre rôzne služby a nezdieľať ich s nikým.

Ak si na sociálnych sieťach chcete udržať svoju súkromnosť, uistite sa, že v nastaveniach máte vypnuté možnosti, ktoré umožňujú ľuďom hľadať vás pomocou vašej e-mailovej adresy alebo telefónneho čísla. Môžete si tiež zvoliť, kto vidí vaše príspevky a komentáre, a ak sa vám zdá, že vás niekto obťažuje alebo šíri nevhodný obsah, môžete ho zablokovať alebo nahlásiť administrátorom sociálnej siete.

2.5 Otestujte svoje znalosti z témy bezpečnosť na sociálnych sieťach

V predchádzajúcej kapitole sme sa detailnejšie pozreli na sociálne siete, ich fungovanie, problémy a útoky, ktorým môžeme čeliť a spôsoby a metódy ako byť na sociálnych sieťach chránení. V nasledujúcej časti sa nachádza rýchle otestovanie naštudovaných materiálov a overenie či ste danej problematike ohľadom sociálnych sietí správne pochopili.

Otázka 1: Ktorá z nasledujúcich možností je najvírusovejšou časťou internetu?

a) Stránky sociálnych sietí

b) Stránky tutoriálov

c) Stránky na chatovanie

d) Informačné stránky

Otázka 2: Ktoré z nasledujúcich opatrení nie je vhodné na zabezpečenie účtov na sociálnych sieťach?

a) Silné heslá

b) Prepojenie účtu s telefónnym číslom

c) Nikdy nikam nepísať svoje heslo

d) Vždy si v počítači uchovávajte kópiu všetkých svojich hesiel

Otázka 3: Ktorá z možností je správnym opatrením na zabezpečenie účtu na sociálnej sieti?

a) Uchovávajte si písomné záznamy o svojich heslách

b) Uchovávajte záznamy o svojich heslách v zvukovej podobe v osobnom mobilnom telefóne

c) Nikdy neuchovávajte heslo s príslušnými menami

d) Heslá sa uchovávajú v menšej veľkosti, aby si ich bolo možné zapamätať

Otázka 4: Ak hackeri získajú prístup k vašim účtom na sociálnych sieťach, môžu vykonať nejaký nezákonný alebo nehanebný čin, aby zhoršili vašu povesť.

a) Áno

b) Nie

Otázka 5: Snažte sa, aby vaše heslá nemali žiadny význam, aby bolo takmer nemožné úspešne vykonať útok _____

a) Sociálna inžinierstvo

b) Phishing

c) Bruteforce

d) Password guessing

Otázka 6: Zvýšte bezpečnosť svojho účtu na sociálnych sieťach tým, že vždy stlačíte tlačidlo _____, keď sa vzdialite od systému

a) Log out

b) Sign in

c) Sign up

d) Log in

Otázka 7: Kliknutie na lákavé reklamy môže spôsobiť problémy.

a) Nepravda

b) Pravda

Otázka 8: Čo znamená "Oznámiť príspevok" na sociálnej sieti?

a) Nahlasovať nevhodný alebo nebezpečný príspevok administrátorom

b) Zdieľať príspevok s priateľmi

c) Označiť príspevok ako obľúbený

d) Odstrániť príspevok zo sociálnej siete

Otázka 9: Čo je to "oversharing" na sociálnych sieťach?

a) Proces, kedy sa zdieľajú príspevky na viacerých sociálnych sieťach naraz

b) Spôsob, ako získať viac sledovateľov na sociálnej sieti

c) Proces, kedy používatelia zdieľajú príliš veľa informácií o sebe

d) Nastavenie súkromia, ktoré umožňuje prístup ku všetkým informáciám na sociálnej sieti

Otázka 10: Ako môžete znížiť riziko úniku informácií na sociálnej sieti?

a) Pravidelne meniť heslá

b) Zdieľať informácie iba s blízkymi priateľmi

c) Kontrolovať nastavenia súkromia

d) Všetky vyššie uvedené

3 DEZINFORMÁCIE A HOAXY

Dezinformácie a hoaxy sú veľkým problémom pre spoločnosť, pretože môžu narušiť verejnú diskusiu, ovplyvňovať politické rozhodnutia a podkopať dôveru verejnosti voči médiám a inštitúciám. Okrem toho majú vážne dôsledky pre jednotlivcov, pretože môžu ovplyvniť ich postoje, správanie a dokonca aj zdravie.

V nasledujúcej kapitole sa budeme zaoberať základnými vlastnosťami dezinformácií a hoaxov, ich spôsobom šírenia a technikami, ktoré sa používajú na manipuláciu s informáciami.

Dôležité je uvedomiť si, že boj proti dezinformáciám je zodpovednosťou každého jednotlivca. Je nevyhnutné rozvíjať svoje kritické myslenie, overovať zdroje informácií a byť dobre informovaný o technikách, ktoré sa využívajú na manipuláciu.

3.1 Pojem hoax

Hoax je termín používaný na označenie podvodnej správy, ktorá sa snaží presvedčiť ľudí o nepravdivých informáciách, udalostiach alebo faktoch. Tieto správy môžu byť vytvorené s rôznymi zámermi, napríklad s cieľom dosiahnuť zisk, šíriť politickú propagandu alebo sa jednoducho pobaviť na úkor iných.

Hoaxy sa môžu šíriť rôznymi spôsobmi, napríklad prostredníctvom sociálnych médií, e-mailových správ, webových stránok a dokonca aj tradičných médií. Správy môžu byť sprevádzané falošnými obrázkami, videami alebo citátmi a pre mnohých ľudí môžu byť úplne presvedčivé.

Hoaxy môžu mať škodlivé následky, napríklad môžu viesť k nesprávnym rozhodnutiam, dezinformácii verejnosti, nárastu nenávisti a dokonca aj k násiliu. Preto je dôležité byť opatrný a overiť si pravdivosť informácií predtým, ako ich zdieľate s ostatnými.

Proti hoaxom možno bojovať kritickým myslením, overovaním zdrojov a používaním dôveryhodných zdrojov informácií. Pri zdieľaní informácií by sme mali byť opatrní a nenechať sa unášať emóciami. Ak si nie sme istí pravdivosťou správy, mali by sme sa jej zdieľaniu vyhnúť a radšej si overiť zdroj a vecnú správnosť.

Ak vytvoríte podvod, môžete mať problémy so zákonom a trestným právom. V mnohých krajinách vrátane Slovenska je šírenie dezinformácií a lží trestným činom, najmä ak sa týkajú osôb, organizácií alebo štátu a majú za cieľ poškodiť ich povesť. Sankcie sa môžu pohybovať od pokút až po väzenie, najmä v prípadoch, keď má hoax vážne dôsledky pre jednotlivca alebo celú spoločnosť. Okrem toho vytvorenie hoaxu môže poškodiť vašu vlastnú dôveryhodnosť a povesť, a to v súkromnom aj pracovnom živote. Preto je dôležité vyhýbať sa šíreniu hoaxov a snažiť sa šíriť len overené a pravdivé informácie.

3.2 Dôvody vzniku hoaxov

Existuje mnoho dôvodov, prečo vznikajú dezinformácie. V nasledovnej podkapitole uvedieme niekoľko z nich:

- **Politická propaganda** - dezinformácie môžu vytvárať politické strany alebo vládne organizácie s cieľom ovplyvniť verejnú mienku a podporiť určitý politický program.
- **Finančný zisk** - mnohé dezinformácie sa vytvárajú s cieľom získať finančný zisk, napríklad vytváraním clickbaitových článkov, ktoré majú prilákať viac čitateľov a generovať väčšie príjmy z reklamy.
- **Konšpiračné teórie** - niektoré dezinformácie vznikajú preto, lebo ľudia veria rôznym konšpiračným teóriám, ktoré nie sú podložené faktami.
- **Rôzne ideologické presvedčenia** - dezinformácie môžu vytvárať rôzne skupiny, ktoré sa snažia šíriť svoje ideologické presvedčenie a presvedčiť ostatných ľudí o svojej pravde.
- **Náboženské presvedčenia** - niektoré dezinformácie vytvárajú ľudia, ktorí sa snažia šíriť svoje presvedčenie a presvedčiť ostatných ľudí, aby sa k nim pridali.
- **Nízka kvalita spravodajstva** - v niektorých prípadoch vznikajú dezinformácie z dôvodu nekvalitného spravodajstva, keď novinári neoverujú svoje zdroje a šíria nepravdivé informácie.
- **Zámerná manipulácia** - niektoré organizácie, napríklad lobistické skupiny, vytvárajú dezinformácie s cieľom manipulovať verejnosť a presadzovať svoje vlastné záujmy.
- **Senzacionalizmus** - dezinformácie sa často šíria kvôli senzacionalizmu ľudí, ktorých priťahujú kontroverzné alebo šokujúce správy.
- **Sociálne médiá** - sociálne médiá môžu byť miestom, kde sa dezinformácie šíria veľmi rýchlo a ľahko. Niektorí ľudia šíria dezinformácie bez toho, aby si overili ich pravdivosť.
- **Zámerné dezinformácie** - v niektorých prípadoch sa dezinformácie vytvárajú zámerne s cieľom poškodiť zvolený cieľ.

3.3 Hoaxi v reálnom živote

V skutočnosti sú hoaxy v našej spoločnosti veľmi rozšírené a môžu mať škodlivé dôsledky pre jednotlivcov a komunity. Uvedieme si niekoľko príkladov hoaxov, ktoré sa v minulosti uskutočnili:

V roku 1912 bola v anglickom Piltdowne objavená kostra prehistorického človeka. Neskôr sa zistilo, že kostra bola falošná a pozostávala z častí kostí človeka a orangutana [9].

Roswellský prípad UFO - V roku 1947 v Roswelli v Novom Mexiku údajne havarovalo UFO a vláda USA mala túto udalosť utajiť. Neskôr sa ukázalo, že išlo len o meteorologický balón [10].

Falošná štúdia o vakcínach a autizme - v roku 1998 bola uverejnená štúdia, ktorá tvrdila, že existuje súvislosť medzi vakcínami a autizmom. Táto štúdia bola neskôr odhalená ako podvod a jej autor bol vylúčený zo zoznamu advokátov [11].

Falošné video o Bigfootovi - V roku 1967 bolo zverejnené video, ktoré tvrdilo, že zobrazuje Bigfoota. Neskôr sa ukázalo, že išlo o podvod, keď tvorcovia filmu priznali, že Yetiho vytvorili len z kostýmu [12].

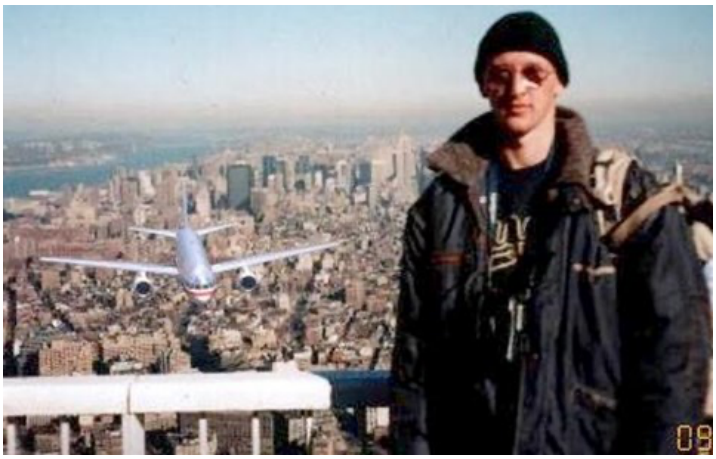
Falošné správy o pandémii COVID-19 - Počas pandémie COVID-19 sa na internete šírili rôzne hoaxy, napríklad že vírus je vynálezom vlád alebo farmaceutických spoločností, alebo že liečba bylinkami či určitými potravinami môže ochrániť pred infekciou [13].

Falošné správy o chemtrails - Mnohí ľudia veria teórii chemtrails, podľa ktorej lietadlá lietajúce vo veľkých výškach dokážu vypúšťať do ovzdušia nebezpečné chemikálie a látky. Táto teória však nie je podložená žiadnymi vedeckými dôkazmi a považuje sa za podvod [14].

3.4 Obrázkové hoaxy

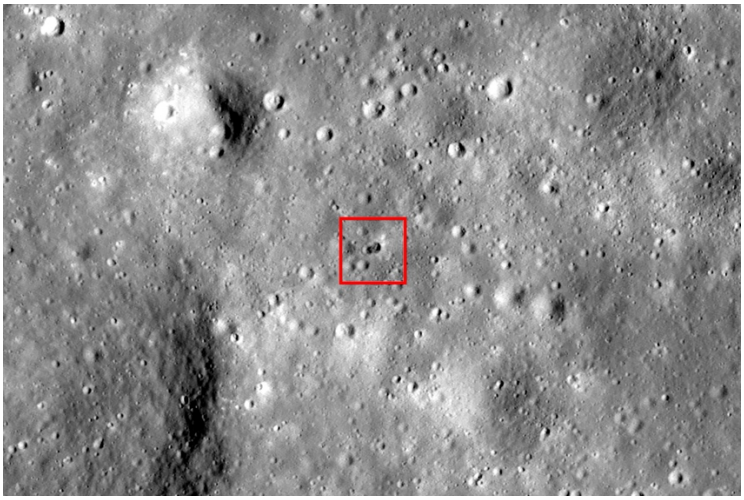
Obrazové hoaxy sú typom dezinformácie, pri ktorej sa na šírenie nepravdivých tvrdení využíva manipulácia s obrázkami alebo fotografiami. Tieto hoaxy sa často šíria prostredníctvom sociálnych médií a e-mailov a môžu byť veľmi účinné pri presviedčaní ľudí o nepravdivých tvrdeniach. Obrázkové hoaxy sa môžu používať na manipuláciu verejnej mienky, propagáciu nepravdivých informácií a šírenie paniky. Medzi príklady obrazových hoaxov patria zmanipulované fotografie, ktoré zobrazujú neexistujúce udalosti, falošné reklamy na lieky, ktoré sľubujú vyliečenie rôznych chorôb, a propagandistické obrázky, ktoré majú podporovať určitú politickú stranu alebo program.

Obrázok 4 Biely žralok plávajúci na ulici počas hurikánu Sandy [15]



Obrázok 5 Turista na WTC v New Yorku [16]

Obrázok 6 Drak vznášajúci sa nad pohorím [17]



Obrázok 7 UFO na mesiaci [18]

Obrázok 8 COVID protest vo Viedni [19]

3.5 Hoaxy na Slovensku

Slováci boli v minulosti postihnutí rôznymi hoaxami. Tu je niekoľko príkladov:

Falošná správa o útokoch na Slovensku: V roku 2017 sa na internete objavila falošná správa o sérii teroristických útokov na Slovensku. Ukázalo sa, že správa bola podvodom, ale mnohí ľudia boli vystrašení a znepokojení [20].

Falošné správy o zdravotných účinkoch: V posledných rokoch sa na Slovensku objavilo mnoho falošných správ o údajných zdravotných účinkoch rôznych potravín a liekov. Tieto správy môžu byť veľmi nebezpečné a môžu viesť k nevhodnému užívaniu liekov alebo nezdravým stravovacím návykom [21].

Na slovenských webových portáloch a sociálnych sieťach sa rýchlo šírila snímka veľkého medveďa, ktorý sa údajne objavil na sídlisku v Martine. Krátko po jej zverejnení začalo veľa jednotlivcov túto fotografiu rozširovať prostredníctvom zdieľania [22].

Hoax o 5G sieťach bol rozšírený na celom svete dokonca aj na Slovensku a mnohí ľudia si stále myslia, že tieto siete predstavujú značné riziko pre zdravie a životné prostredie. Tento hoax tvrdí, že 5G technológia spôsobuje rôzne zdravotné problémy vrátane rakoviny, a to prostredníctvom rádiovej frekvencie a elektromagnetického žiarenia [23].

Osoba šíriaca hoax zverejnila materiál pochádzajúci z Okresného úradu v Banskej Bystrici pod názvom "Základné záväzky v oblasti obrany štátu pre rok 2023," ktorý bol publikovaný na oficiálnej webovej stránke Ministerstva vnútra Slovenskej republiky. V tomto dokumente sa nachádza informácia o plánovaných komplexných cvičeniach s cieľom vykonávať úlohy po vyhlásení vojnového stavu a mobilizácii ozbrojených síl Slovenskej republiky, súčasne realizovaných v spolupráci so spravodajským rezortom vnútra a Ministerstvom obrany Slovenskej republiky [24].

3.6 Základné princípy mediálnej gramotnosti

Mediálna gramotnosť predstavuje súhrn vedomostí a schopností, ktoré nám umožňujú kriticky a premyslene uvažovať o informáciách, ktoré prijímame alebo produkujeme. Je dôležité mať na pamäti niekoľko základných princípov mediálnej gramotnosti, ktoré nám pomáhajú rozvíjať tieto schopnosti.

Prvým kľúčovým princípom je kritické myslenie. Ide o schopnosť hodnotiť a posudzovať informácie, ktoré sa k nám dostávajú, a vedieť rozpoznať, kedy sú tieto informácie pravdivé a kedy nie. Kritické myslenie zahŕňa schopnosť identifikovať zdroje informácií, analyzovať ich a porovnávať s inými zdrojmi. Tiež nám pomáha rozpoznať rôzne formy manipulácie a zaujatosti, ktoré môžu ovplyvniť naše chápanie a hodnotenie informácií.

Druhým princípom je schopnosť identifikovať a hodnotiť zdroje informácií. Je nevyhnutné vedieť, odkiaľ informácie pochádzajú a či sú tieto zdroje dôveryhodné. V dnešnej dobe, keď je prístup k informáciám taký rozmanitý a ľahko dostupný, je dôležité mať schopnosť správne rozpoznať kvalitné zdroje a kriticky posudzovať ich dôveryhodnosť.

Ďalším dôležitým prvkom je schopnosť analyzovať médiá. Toto zahŕňa schopnosť porozumieť rôznym formám médií, ako sú tlač, televízia, rozhlas a internet. Je potrebné vedieť rozpoznať, ako sú informácie prezentované, aký je ich zdroj a aký účel majú. Toto nám pomáha lepšie pochopiť, aký vplyv majú médiá na naše chápanie sveta okolo nás.

Okrem toho, mediálna gramotnosť zahŕňa aj schopnosť rozpoznávať a chápať rôzne spôsoby komunikácie, ako sú text, obraz, zvuk a video. Je dôležité byť schopný rozpoznať, ako sú informácie prezentované prostredníctvom týchto médií a aký je ich účel. Táto schopnosť nám umožňuje lepšie dekódovať a porozumieť informáciám, s ktorými sa stretávame.

Ďalším kľúčovým aspektom mediálnej gramotnosti je bezpečnosť na internete. V digitálnom veku je dôležité vedieť, ako chrániť svoje osobné údaje a vyhnúť sa nebezpečenstvám, ktoré môžu hroziť online. Je potrebné byť oboznámený s rizikami a vedieť, ako sa chrániť a zachovať si svoju súkromie v online prostredí.

Kreativita je tiež súčasťou mediálnej gramotnosti. Táto schopnosť nám umožňuje vytvárať vlastný obsah a komunikovať s ostatnými prostredníctvom rôznych médií. Kreativita nám dáva možnosť byť aktívnymi tvorcami a zdieľať naše myšlienky, názory a príbehy prostredníctvom médií.

V súhrne, tieto základné princípy mediálnej gramotnosti nám umožňujú vyvíjať kritické myslenie a lepšie chápať informácie, ktoré prijímame. Sú tiež základom pre aktívnu účasť v procese tvorby a zdieľania informácií s ostatnými.

3.7 Metódy ochrany voči hoaxom

Existuje niekoľko spôsobov, ako sa chrániť pred hoaxmi a dezinformáciami. Na základe predošlej podkapitole ohľadom mediálnej gramotnosti si popíšeme niektoré.

- Pokúste sa overiť informácie: skôr, ako sa s nimi podelíte, uistite sa, že sú pravdivé. Pokúste sa nájsť ďalšie zdroje, ktoré tvrdenie potvrdzujú.
- Buďte opatrní na sociálnych sieťach: Mnohé hoaxy sa šíria prostredníctvom sociálnych sietí. Buďte opatrní pri zdieľaní informácií, ktoré vidíte na sociálnych sieťach, a snažte sa overiť ich pravdivosť.
- Dôverujte overeným zdrojom: Dôverujte len dôveryhodným a overeným zdrojom. Snažte sa nájsť informácie na overených webových stránkach alebo v renomovaných médiách.
- Snažte sa byť kritickí: Ak vidíte nejakú informáciu, ktorá sa vám zdá podozrivá, skúste sa na ňu pozrieť kriticky a analyzovať ju. Pokúste sa nájsť ďalšie informácie, ktoré by mohli tvrdenie potvrdiť alebo vyvrátiť.
- Vyhnite sa klikaniu na podozrivé odkazy: Mnohé hoaxy sa šíria prostredníctvom odkazov na neoverených webových stránkach. Vyhnite sa klikaniu na podozrivé odkazy a ak je to možné, nainštalujte si do počítača antivírusový program.
- Zdieľajte len overené informácie: Snažte sa zdieľať len overené a pravdivé informácie. Ak si nie ste istí, či je nejaká informácia pravdivá, nezdieľajte ju.

Tieto metódy vám pomôžu chrániť sa pred hoaxmi a dezinformáciami a zachovať si dôveryhodnosť a dobré meno.

3.8 Otestujte svoje znalosti z témy o dezinformáciách a hoaxoch

Otázka 1: Čo je hoax?

a) Prírodná katastrofa
b) Podvodná správa
c) Technologická inovácia
d) Politická stratégia

Otázka 2: Aké sú dôsledky šírenia hoaxov?

a) Zvýšenie násilia
b) Dezinformovanie verejnosti
c) Strata majetku
d) Rozvoj demokracie

Otázka 3: Akým spôsobom sa hoaxy najčastejšie šíria?

a) Tradičné médiá
b) E-mailové správy
c) Sociálne médiá
d) Telefonické hovory

Otázka 4: Ako možno bojovať proti šíreniu hoaxov?

a) Kritickým myslením
b) Používaním dôveryhodných zdrojov
c) Overovaním zdrojov informácií
d) Všetko z uvedeného

Otázka 5: Aké sú ciele hoaxov?

a) Šírenie pravdivých informácií
b) Dosiahnuť zisk
c) Urýchliť vývoj technológií
d) Podporovať politickú stabilitu

Otázka 6: Čo môžu hoaxy obsahovať?

a) Falošné citáty
b) Falošné obrázky a videá
c) Falošné informácie
d) Všetko z uvedeného

Otázka 7: Ako možno overiť pravdivosť správy?

a) Overením zdroja informácií
b) Porovnaním informácie s viacerými zdrojmi
c) Použitím dôveryhodných zdrojov informácií
d) Všetko z uvedeného

Otázka 8: Ktoré z nasledujúcich tvrdení je hoax?

a) Slnko sa každý rok priblíži k Zemi
b) Všetky uvedené tvrdenia sú hoax
c) Chobotnica má 8 nôh
d) Voda v mikrovlnnej rúre exploduje

Otázka 9: Čo je clickbait?

a) Reklamný banner na internetovej stránke.
b) Tlačová správa s nízkou dôležitosťou.
c) Zaujímavý nadpis alebo obrázok, ktorý láka na kliknutie.
d) Reakcia na dezinformáciu prostredníctvom kliknutia na odkaz.

Otázka 10: Prečo je dôležité mať mediálnu gramotnosť?

a) Zlepšuje schopnosť robiť fotografie a videá.
b) Umožňuje rozpoznať a kriticky hodnotiť informácie.
c) Poskytuje prístup k exkluzívnym médiám.
d) Zvyšuje popularitu na sociálnych médiách.

4 OSOBNÉ ÚDAJE

Osobné údaje sú v súčasnosti jedným z najcennejších aktív, ktoré máme. Ich zhromažďovanie a spracovanie prebieha takmer v každej oblasti nášho života - od nakupovania cez zdravotníctvo až po online aktivity. Avšak s narastajúcim množstvom osobných údajov v digitálnom svete rastie aj potenciál pre ich zneužitie.

Výzvou pre kybernetickú bezpečnosť je chrániť tieto údaje pred útokmi hackerov, phishingom, malvérom a inými technikami, ktoré by mohli narušiť ich dôvernosť a integritu. V prípade, že sa dostanú do nesprávnych rúk, môžu byť využité na získanie neoprávnenej finančnej výhody alebo na manipuláciu s verejnou mienkou.

Kým existujú rôzne spôsoby, ako ochrániť osobné údaje, dôležité je si uvedomiť, že ich bezpečnosť začína u každého jednotlivca. Prvým krokom by mala byť starostlivá voľba silného hesla, ktoré je jedinečné pre každú službu a nezdieľa sa s nikým iným. Okrem toho by mali byť údaje zabezpečené dvojfaktorovou autentifikáciou, ktorá poskytuje dodatočnú úroveň ochrany.

Okrem toho by sme mali byť opatrní pri zdieľaní našich osobných údajov s tretími stranami a informovať sa o tom, ako budú naše údaje použité. Aj keď sú služby zadarmo, neznamená to, že sú bezplatné - naše údaje môžu byť predané reklamným spoločnostiam alebo využité na iné účely, ktoré by nás mohli ohroziť.

Napriek tomu, že kybernetická bezpečnosť nie je úplne zaručená, môžeme prispieť k jej zlepšeniu tým, že budeme opatrní a zodpovední pri nakladaní s našimi osobnými údajmi. Osobné údaje sú našou digitálnou identitou a ich ochrana by mala byť našou prioritu.

4.1 Heslá

Heslo je tajný kód, ktorý slúži na overenie identity používateľa a umožňuje mu prístup k chráneným zdrojom. Heslá sa často používajú v digitálnom svete, napríklad pri prihlasovaní do online účtu alebo k odomykaniu zariadení.

Dôležitosť hesiel spočíva v tom, že poskytujú základnú úroveň ochrany pred neoprávneným prístupom k dôležitým informáciám. Bez hesla by každý mohol získať prístup k našim účtom a osobným údajom.

Preto je dôležité používať silné heslá, ktoré sú zložité na uhádnutie. Silné heslo by malo obsahovať kombináciu veľkých a malých písmen, čísel a špeciálnych znakov, ako sú napríklad výkričník alebo otáznik. Heslo by malo mať aspoň 8 znakov, ale čím dlhšie a zložitejšie, tým lepšie.

Je tiež dôležité, aby sme pre každý účet používali iné heslo a aby sme ich pravidelne menili. Ak použijeme rovnaké heslo pre viacero účtov a jedno z nich bude ohrozené, môže to ohroziť všetky ostatné účty.

Využívanie silných a jedinečných hesiel je preto kľúčové pre ochranu našich osobných údajov a digitálnej identity. Ak by sme nezabezpečovali naše účty a osobné údaje správne, mohli by sme sa stať obeťou kybernetických útokov, ktoré by mohli mať vážne následky.

4.2 Fakty a mýty o heslách

V tejto podkapitole sa zameriame na rozlíšenie faktov od mýtov v súvislosti s heslami. Rozhodli sme sa preskúmať niektoré bežné tvrdenia a zistiť, čo je pravda a čo iba fikcia. Pri pohľade na fakty a mýty o heslách je dôležité mať na pamäti, že kybernetické hrozby sa neustále vyvíjajú a technológie sa menia. Preto je nevyhnutné byť obozretný a používať osvedčené postupy na ochranu našich hesiel.

Fakty o heslách:

- Silné heslo je nevyhnutné pre ochranu vašich digitálnych účtov a osobných údajov.
- Heslá by mali byť aspoň 8 znakov dlhé a mali by obsahovať kombináciu veľkých a malých písmen, čísel a špeciálnych znakov.
- Jedinečné heslá pre každý účet sú kľúčové. Nikdy nepoužívajte rovnaké heslo pre viacero účtov.
- Pravidelné menenie hesiel je dôležité. Odporúča sa meniť heslá aspoň raz za tri mesiace.
- Používanie hesiel v prehliadačoch a zapisovanie hesiel do súborov alebo na papier môže byť nebezpečné.

Mýty o heslách:

- Heslo musí byť komplikované a ťažko zapamätateľné. Toto nie je pravda. Ak heslo obsahuje kombináciu slov a čísel, ktoré majú pre vás nejaký význam, bude pre vás ľahšie si ho zapamätať.
- Dostatočná ochrana vašich digitálnych účtov závisí iba od silného hesla. Silné heslo je síce dôležité, ale existujú aj iné faktory, ktoré ovplyvňujú bezpečnosť vášho účtu, ako napríklad aktivácia dvojfaktorovej autentifikácie.
- Najlepšie heslá sú generované náhodne pomocou softvéru. Toto nemusí byť vždy pravda, pretože takéto heslá sú pre používateľov často ťažko zapamätateľné.
- Zapisovanie hesiel do súborov alebo na papier môže byť bezpečné. To nie je pravda, pretože takéto záznamy môžu byť ľahko ukradnuté alebo stratene, a tým ohroziť bezpečnosť vašich účtov.
- Menenie hesiel nie je dôležité. Je dôležité meniť heslá aspoň raz za tri mesiace, pretože staré heslá môžu byť skompromitované a použité na neoprávnený prístup k vašim účtom.

4.3 Spôsoby, na základe ktorých môžu byť odhalené heslá

- Heslá môžu byť uhádnuté: Niektorí útočníci môžu skúšať rôzne kombinácie hesiel, ktoré by mohli byť správne. Tento útok sa nazýva útok hrubou silou.

- Heslá môžu byť odhalené cez phishing: Útočníci môžu vytvoriť falošnú stránku prihlasovania a požiadať používateľov o zadanie svojich prihlasovacích údajov. Potom môžu použiť tieto informácie na získanie prístupu k účtom.
- Heslá môžu byť ukradnuté pri útoku na databázy: Útočníci sa môžu pokúsiť získať prístup k databáze s heslami. Ak sa im to podarí, môžu mať prístup k množstvu hesiel a použiť ich na neoprávnený prístup k účtom.
- Heslá môžu byť odhalené prostredníctvom malvéru: Malvér môže obsahovať keylogger, ktorý môže sledovať všetky kroky používateľa a zaznamenávať všetky údaje, ktoré zadáva, vrátane hesiel.
- Heslá môžu byť odhalené cez verejne dostupné informácie: Používatelia často používajú osobné údaje, ako sú mená svojich domácich zvierat alebo dátumy narodenia, ako súčasť svojho hesla. Tieto informácie môžu byť ľahko získané z verejne dostupných zdrojov a použité na odhalenie hesla.

Je dôležité, aby používatelia používali silné a unikátne heslá a aby boli opatrní pri zadávaní svojich prihlasovacích údajov na internete. Je tiež dôležité chrániť svoje zariadenia pred malvérom a pravidelne meniť heslá na svojich účtoch.

4.4 Spôsoby ako vytvoriť silné heslo

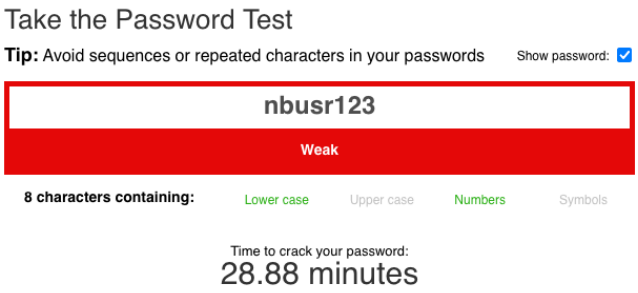
Existuje niekoľko krokov, ktoré môžete urobiť, aby ste si vytvorili silné a bezpečné heslo:

- Dĺžka hesla: Heslo by malo byť dostatočne dlhé, minimálne 12 znakov. Čím je heslo dlhšie, tým ťažšie ho bude útočník uhádnuť.
- Používanie rôznych znakov: Heslo by malo obsahovať rôzne druhy znakov, ako sú veľké a malé písmená, čísla a špeciálne znaky. Používanie rôznych druhov znakov zvyšuje množstvo možností, ktoré útočník musí skúsiť, aby uhádol vaše heslo.
- Unikátnosť hesla: Heslo by malo byť unikátne a nemalo by sa používať na viacerých účtoch. Ak útočník získa vaše heslo na jednom účte, môže sa pokúsiť použiť ho na iných účtoch.
- Náhodnosť hesla: Heslo by malo byť náhodne vygenerované. Vyvarujte sa používaniu zreťazených slov alebo fráz, ktoré by mohli byť uhádnuté.
- Použitie hesla správne: Aj keď máte silné heslo, musíte ho stále používať správne. Nezdieľajte ho s nikým, neukladajte ho v nezabezpečených súboroch a nemeníte ho pravidelne.
- Použitie hesla manažéra: Ak máte veľa hesiel na pamätanie, môžete použiť heslo manažéra. Heslo manažér vám umožní uložiť všetky vaše heslá na jednom mieste a chrániť ich jediným silným heslom.

Používanie silného a unikátneho hesla je dôležité pre kybernetickú bezpečnosť. Uistite sa, že používate heslá, ktoré sú ťažké na uhádnutie a zabezpečujú vaše osobné údaje.

Aby ste zistili, či vaše heslo je dostatočne bezpečné a spĺňa vyššie spomenuté kritéria, existujú stránky určené na otestovanie: *passwordmonster.com, www.security.org/how-secure-is-my-password, bitwarden.com/password-strength* a podobne.

Pokiaľ ste zistili, že vaše heslo je ľahké na odhalenie s nejakým spôsobom, ktoré sme uviedli, existujú webové služby a nástroje, ktoré napomôžu k vytvoreniu hesla, napr.: *lastpass.com/features/password-generator*, *delinea.com/resources/password-generator-it-tool*, *www.avast.com/random-password-generator*, *passwordsgenerator.net* a podobne.



Obrázok 9 Odhadovaný čas zistenia hesla [25]

4.5 Otestujte svoje znalosti z témy ohľadom hesiel a osobných údajov

Otázka 1: Aké sú základné princípy ochrany osobných údajov?

a) Prístup, správa, zdieľanie
b) Súkromie, transparentnosť, zodpovednosť
c) Dátové centrum, šifrovanie, aktualizácia
d) Analýza, identifikácia, vyhodnocovanie

Otázka 2: Čo znamená GDPR?

a) Generická databázová platforma pre reprezentáciu
b) Všeobecné nariadenie o ochrane údajov
c) Global Data Privacy Regulation
d) Grafické rozhranie pre databázy

Otázka 3: Akým spôsobom môžete chrániť svoje heslo?

a) Používať rovnaké heslo pre viacero účtov
b) Písať heslo na papier a nosiť ho so sebou
c) Používať silné a unikátne heslo pre každý účet
d) Zdieľať heslo s priateľmi

Otázka 4: Čo je viacfaktorová autentifikácia?

a) Autentifikácia pomocou viacerých hesiel
b) Autentifikácia na viacerých zariadeniach súčasne

c) Autentifikácia s využitím viacerých metód overovania
d) Autentifikácia iba na základe používateľského mena

Otázka 5: Aké informácie by ste nikdy nemali zdieľať online?

a) Vaše celé meno
b) Adresa bydliska
c) Rodné číslo
d) Všetky vyššie uvedené informácie by nemali byť zdieľané online

Otázka 6: Čo je to šifrovanie údajov?

a) Proces ukladania údajov v cloudovom úložisku
b) Metóda ochrany údajov pomocou matematických algoritmov
c) Pravidelné zálohovanie údajov na externý disk
d) Spôsob zdieľania údajov prostredníctvom sociálnych médií

Otázka 7: Aké je odporúčanie týkajúce sa aktualizácie softvéru?

a) Ignorovať aktualizácie, ak všetko funguje správne
b) Aktualizovať softvér pravidelne, aby ste mali najnovšie zabezpečenie
c) Aktualizovať softvér iba na starších počítačoch
d) Stiahnuť softvér iba z neoverených zdrojov

Otázka 8: Aký je najbezpečnejší spôsob uloženia hesiel?

a) Zapisovanie ich na papier a uchovávanie v bezpečnom mieste
b) Ukladanie do textového súboru na počítači
c) Používanie správcu hesiel alebo heslového manažéra
d) Zapamätávanie všetkých hesiel bez záloh

Otázka 9: Ktoré práva máte podľa GDPR v súvislosti s vašimi osobnými údajmi?

a) Právo na zabudnutie a právo na vymazanie údajov
b) Právo na rozšírenie dátového limitu
c) Právo na zdieľanie údajov so všetkými spoločnosťami
d) Právo na anonymizáciu údajov

Otázka 10: Aký je význam silnej heslovej frázy?

a) Jednoduché zapamätanie a písanie hesla
b) Zvýšená odolnosť voči útokom hrubou silou
c) Rýchle obnovenie zabudnutého hesla

d) Vylepšenie funkcionality používateľského účtu

5 HACKERI

Hackeri sú jednotlivci alebo skupiny ľudí, ktorí využívajú svoje technické zručnosti a znalosti počítačových systémov na neoprávnené preniknutie do cudzích počítačových systémov alebo sietí. Často to robia s cieľom neoprávnene získať prístup k informáciám, škodlivým útokom alebo zneužívať systémy. Existujú rôzne typy hackerov, napríklad čierny hackeri, ktorí sa zameriavajú na zlodejstvo údajov, škody alebo vydieranie, a bieli hackeri, ktorí sa zaoberajú testovaním bezpečnosti systémov a pomáhajú identifikovať slabé miesta, aby sa predišlo zneužívaniu.

5.1 Rozdelenie hackerov

Existuje niekoľko spôsobov, ako môžeme rozdeliť hackerov na základe ich motivácií a účinkov ich činnosti. V pokračovaní podkapitoly uvedieme kategórie hackerov a ich dôvody útokov:

- Čierny hacker (Black Hat Hacker): Čierni hackeri sú skupiny alebo jednotlivci, ktorí využívajú svoje schopnosti na nelegálne účely. Ich cieľom môže byť získanie finančného zisku, škodenie iným osobám alebo organizáciám, krádež citlivých údajov, sabotáž, vydieranie alebo podvody. Ich útoky sú zamerané na zneužívanie bezpečnostných slabín v systémoch.
- Biely hacker (White Hat Hacker): Bieli hackeri sú odborníci na bezpečnosť, ktorí sa zameriavajú na zlepšovanie kybernetickej bezpečnosti. Ich účelom je identifikovať bezpečnostné chyby a slabiny v systémoch a pomôcť ich vlastníkom tieto chyby opraviť. Bieli hackeri často pracujú pre organizácie, kde im je zverená úloha testovať bezpečnosť systémov a nájsť potenciálne zraniteľnosti pred tým, ako ich zneužijú čierni hackeri.
- Sivý hacker (Grey Hat Hacker): Siví hackeri sú niekde medzi čiernymi a bielymi hackermi. Sú to jednotlivci, ktorí neoprávnene prenikajú do systémov, ale ich motivácie sú zväčša nejednoznačné. Niektorí z nich sa snažia pomôcť identifikovať bezpečnostné chyby systémov a informovať ich majiteľov, zatiaľ čo iní môžu vyhľadávať výhody alebo uznanie tým, že odhalia chyby verejne.
- Hacktivist (Hacktivist Hacker): Hacktivisti sú hackeri, ktorí používajú svoje schopnosti na podporu politickej, sociálnej alebo environmentálnej agendy. Útočia na ciele, ktoré súvisia s ich presvedčením a snažia sa upozorniť na konkrétne problémy alebo vyvolať zmenu. Ich útoky môžu zahŕňať poškodzovanie webových stránok, distribúciu informácií, úniky údajov a podobne.
- Script Kiddie: Script Kiddie je jedinec, ktorý nemá vlastné technické schopnosti ani znalosti, ale využíva dostupné nástroje a skripty, ktoré mu umožňujú uskutočňovať útoky na ciele. Sú zvyčajne motivovaní túžbou po škárovaní, vyvolávaní nezrovnalostí alebo jednoducho pre zábavu. Ich útoky sú často nedbanlivé a nepresné.
- Štátny hacker (State-Sponsored Hacker): Štátni hackeri sú čierni hackeri, ktorí konajú v mene štátnej inštitúcie alebo vlády. Ich motivácia môže zahŕňať získanie

strategických informácií, špionáž, politický vplyv, sabotáž alebo kybernetické vojny. Majú vysokú úroveň technických schopností a finančné zdroje na podporu svojich operácií.

- Hacker záujmových skupín (Hacktivist Group): Tieto skupiny hackerov majú politické, sociálne alebo ideologické motivácie. Ich cieľom je presadzovať ich presvedčenie prostredníctvom kybernetických útokov. Môžu sa zameriavať na webové stránky, organizácie alebo iné ciele, ktoré považujú za protirečiace ich hodnotám.
- Hraničný hacker (Ethical Hacker): Hraniční hackeri sú odborníci na kybernetickú bezpečnosť, ktorí sa najímajú s cieľom testovať a zlepšovať bezpečnostné opatrenia organizácií. Majú povolenie na testovanie systémov, hľadanie slabých miest a identifikáciu bezpečnostných problémov. Ich účelom je poskytnúť odporúčania na zlepšenie bezpečnosti.

Je dôležité si uvedomiť, že nie všetci hackeri sú zlí alebo nezákonní. Existujú aj etickí hackeri a bezpečnostní odborníci, ktorí sa snažia chrániť systémy pred zneužitím a pomáhajú zlepšovať bezpečnosť v digitálnom prostredí.

5.2 Dôvody, prečo hackeri podnikajú útoky

Existuje niekoľko dôvodov, prečo hackeri podnikajú útoky. Medzi najbežnejšie patrí:

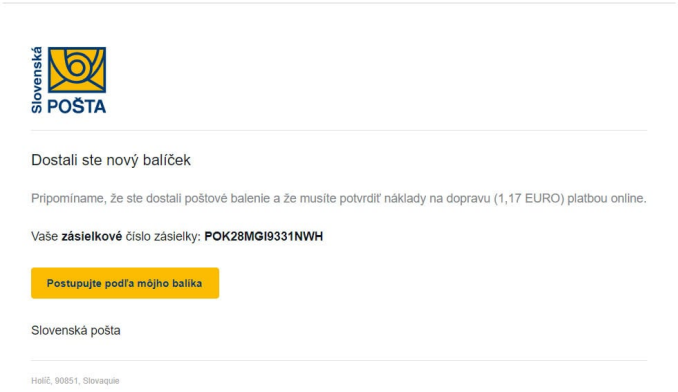
- Finančný zisk: Mnoho hackerov sa snaží získať finančný prospech z ich činnosti. Môžu sa zameriavať na krádež finančných údajov, kreditných kariet, hesiel alebo vykonávať podvodné transakcie.
- Krádež identít: Hackeri môžu útočiť na osobné údaje a identitu používateľov s cieľom získať prístup k bankovým účtom, úverom alebo iným cenným informáciám.
- Sabotáž: Niektorí hackeri útočia s cieľom spôsobiť škody alebo chaos. Môžu vykonávať DoS (Denial of Service) útoky, ktoré bránia prístupu k webovým stránkam alebo systémom, alebo môžu infikovať počítače malvérom, čím spôsobia ich nefunkčnosť.
- Atavizmus: Skupiny hackerov môžu vykonávať útoky s politickými, ideologickými alebo sociálnymi motiváciami. Môžu sa snažiť prezentovať svoje stanoviská alebo vyjadriť nesúhlas s určitou organizáciou alebo vládou.
- Praktický dôkaz alebo výskum: Niekedy hackeri útočia s cieľom preukázať slabiny alebo bezpečnostné chyby v systémoch a informovať o nich. Títo hackeri môžu byť považovaní za etických hackerov alebo "white-hat" hackerov, ktorí sa snažia zlepšiť bezpečnosť.

Je dôležité poznamenať, že nelegálne útoky a hacking sú nezákonné a porušujú súkromie a bezpečnosť ostatných. Tieto činnosti majú vážne dôsledky pre jednotlivcov aj organizácie. Ochrana a zabezpečenie systémov je dôležité na minimalizáciu rizika útokov a ochranu pred nežiaducimi následkami hackerov.

5.3 Phishing

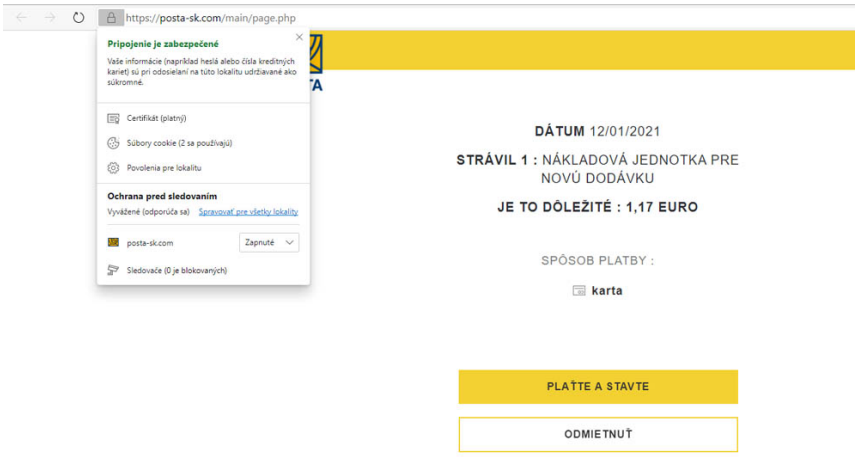
Phishing je typ kybernetického útoku, ktorý sa zameriava na získanie citlivých informácií od používateľov. Útočník sa vydáva za dôveryhodnú organizáciu alebo osobu a snaží sa získať prihlasovacie údaje, finančné informácie alebo iné citlivé údaje od svojej obete.

Útok phishingom sa obvykle uskutočňuje prostredníctvom e-mailov, správ v sociálnych sieťach, SMS správ alebo falošných webových stránok.



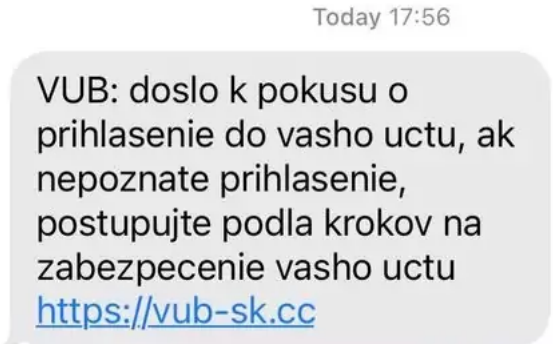
Obrázok 10 E-mailový phishing [26]

Útočník sa snaží presvedčiť obeť, aby poskytla svoje citlivé údaje tým, že sa predstavuje ako spoľahlivá osoba alebo organizácia, ako napríklad banka, online platobná brána, sociálna sieť alebo vládny úrad. V správe sa často nachádza odkaz na falošnú webovú stránku, kde sa používateľovi žiada, aby zadával svoje prihlasovacie údaje, heslá, čísla kreditných kariet alebo iné citlivé informácie.



Obrázok 11 Falošné prelinkovanie na webovú stránku [26]

Cieľom phishingu je získať neoprávnený prístup k účtom používateľov alebo ich osobným a finančným údajom. Útočníci potom môžu tieto informácie zneužiť na krádež identity, finančnú podvod a iné zločinné aktivity.



Obrázok 12 SMS phishing [26]

Aby sa používatelia chránili pred phishingom, je dôležité byť opatrný pri klikaní na odkazy v zvláštnych správach alebo e-mailoch a vždy skontrolovať adresu URL webovej stránky, na ktorú sa môže používateľ dostáť, aby sa uistil, že je skutočná. Je tiež dôležité byť obozretný pri poskytovaní citlivých informácií cez internet a používať silné a jedinečné heslá pre rôzne účty.

Phising je možné realizovať rôznymi kanálmi, v pokračovaní podkapitoly si uvedieme najčastejšie formy phishingu.

Útočník sa vydáva za banku a posiela falošný e-mail, v ktorom žiada používateľa, aby aktualizoval svoje bankové údaje. E-mail obsahuje odkaz na falošnú webovú stránku, kde sa používateľa vyžaduje, aby zadal svoje prihlasovacie údaje, heslo a ďalšie citlivé informácie.

Útočník vytvorí falošný profil na sociálnej sieti a kontaktuje používateľov so žiadosťou o overenie účtu alebo aktualizáciu ich osobných informácií. V skutočnosti ide o pokus získať prístup k ich prihlasovacím údajom.

Používateľ dostane e-mail, v ktorom sa tvrdí, že vyhral súťaž a musí poskytnúť svoje osobné údaje, ako je napríklad číslo kreditnej karty, aby získal svoju cenu. E-mail môže mať profesionálny (legitímny) vzhľad a obsahuje odkaz na falošnú stránku na zadanie informácií.

Používateľ dostáva SMS správy, ktoré sa tvária byť od banky alebo iného finančnej inštitúcie. Správa obsahuje upozornenie na podozrenie ohľadom neoprávneného použitia účtu a žiada používateľa, aby klikol na odkaz a prihlásil sa na svoj účet. Odkaz v skutočnosti vedie na falošnú stránku, kde útočník získa prístupové údaje.

Používateľ dostáva oznámenie o dostupnosti nového softvéru alebo aktualizácie, ktorá je nevyhnutná na pokračovanie v používaní určitého softvéru alebo služby. Po kliknutí na odkaz na sťahovanie sa však namiesto toho môže inštalovať škodlivý softvér, ktorý môže zhromažďovať citlivé informácie alebo spôsobiť iné škody.

Existuje niekoľko opatrení, ktoré je možné prijať na ochranu pred phishingovými útokmi. V pokračovaní si uvedieme niekoľko s nich.

Pri klikaní na odkazy buďte obozretní. Skontrolujte si odkazy v e-mailoch, správach a na webových stránkach pred ich kliknutím. Pokiaľ by odkaz vypadal podozrivý alebo neznámy,

je najlepšie ho ignorovať alebo overiť jeho pravosť priamo prostredníctvom oficiálnej webovej stránky.

Obrázok 13 Porovnanie URL adries [27]

Dbajte na to, aby ste nezdieľali citlivé informácie. Nikdy neposkytujte svoje prihlasovacie údaje, heslá, čísla kreditných kariet alebo iné osobné informácie prostredníctvom e-mailu, správ na sociálnych sieťach alebo neoverených webových stránkach. Dôveryhodné organizácie nežiadajú o tieto informácie prostredníctvom nedôveryhodných kanálov.

Dôkladne si overte dôveryhodnosť odosielateľa. Skontrolujte e-mailovú adresu odosielateľa, pravopis a gramatiku samotnej správy. Buďte ostražití voči e-mailom, ktoré sú príliš významné, požadujú okamžitú akciu alebo sú plné gramatických chýb, pretože to môžu byť známky phishingového útoku.

Uistite sa, že máte nainštalovaný spoľahlivý antivírusový program a pravidelne ho aktualizujte. Tento softvér môže napomôcť odhaliť a blokovať potenciálne škodlivé súbory a webové stránky.

Využívajte viacúrovňové overenie, pokiaľ je k dispozícii. Ak je dostupná možnosť, povoľte viacúrovňové overenie pre svoje online účty. To znamená, že okrem prihlasovacieho mena a hesla budete musieť poskytnúť ďalšiu formu overenia, ako je jednorazový kód, SMS potvrdenie alebo biometrická identifikácia.

Vzdelávajte sa o technikách a nových spôsoboch realizovania phishingu. Existujú rôzne online školenia a zdroje, ktoré pomôžu lepšie porozumieť tejto problematike. Pokiaľ máte pochybnosti o správnosti alebo dôveryhodnosti akéhokoľvek odkazu alebo požiadavky na poskytnutie citlivých údajov, je najbezpečnejšie sa obrátiť priamo na danú organizáciu prostredníctvom oficiálnych kontaktov a overiť správnosť informácie.

5.4 Scam

Scam označuje podvod a zahrňuje nelegálne, klamlivé alebo zavádzajúce praktiky, ktoré majú za cieľ oklamať alebo okrádať ľudí. Scamy sa často vyskytujú prostredníctvom rôznych komunikačných kanálov, vrátane internetu, telefónu, e-mailov, sociálnych sietí a ďalších prostriedkov.

Podvody môžu mať rôzne formy a snažia sa zasiahnuť do rôznych oblastí, vrátane finančných prostriedkov, osobných údajov, identity, zdravia, investícií a ďalších.

V súčasnosti existujú rôzne formy scamov, ktoré môžu zahŕňať:

- Phishing: Podvodníci sa vydávajú za dôveryhodné inštitúcie alebo organizácie a snažia sa získať citlivé informácie, ako sú heslá, bankové účty alebo kreditné karty (detailnejšie v podkapitole 5.3).
- Falošné lotérie alebo súťaže: Ľudia dostávajú správy o výhre v lotériách alebo súťažiach, do ktorých sa nikdy neprihlásili, a sú požiadaní o platbu alebo osobné údaje.
- Romantický podvod: Podvodníci vytvárajú online vzťahy s ľuďmi a potom žiadajú o peniaze na cestu, liečbu alebo iné dôvody.
- Investičné podvody: Ponúkajú sa ziskové investície do podnikania alebo kryptomien s vysokými výnosmi, avšak investori následne zistia, že boli podvedení a ich peniaze sú preč.
- Technická podpora: Podvodníci sa vydávajú za technickú podporu a tvrdia, že počítač používateľa je napadnutý, po čom žiadajú prístup k systému alebo platbu za opravu.

Podobne ako pri phisingu, čo predstavuje časť scamu je veľmi dôležité sa chrániť aj pred scamom v online priestore. V pokračovaní si uvedieme niekoľko tipov, ako je možné sa chrániť:

Buďte opatrní voči neznámym odosielateľom e-mailov, správ na sociálnych sieťach a telefonátom. Buďte podozrievaví voči nevyžiadaným správam, ktoré žiadajú o osobné údaje alebo platby.

Nikdy nezverejňujte svoje citlivé informácie, ako sú heslá, čísla kreditných kariet, bankové údaje alebo osobné identifikačné čísla na nedôveryhodných webových stránkach alebo v odpovediach na nevyžiadané správy.

Používajte silné heslá, ktoré kombinujú rôzne znaky, ako sú veľké a malé písmená, číslice a špeciálne znaky. Navyše, pre každú službu používajte jedinečné heslo, aby sa minimalizovalo riziko prístupu do vášho účtu v prípade, že sa heslo dostane do rúk podvodníkov (detailnejšie v podkapitole 4.4).

Udržujte váš operačný systém, internetový prehliadač a iné softvéry aktuálne. Aktualizácie zvyčajne obsahujú opravy chýb a bezpečnostné zlepšenia, ktoré môžu ochrániť systém pred známymi hrozbami.

Vždy skontrolujte dôveryhodnosť webových stránok, služieb a spoločností, s ktorými máte interakcie. Skúmajte recenzie a hodnotenia iných používateľov a vyhľadávajte informácie o spoločnostiach od dôveryhodných zdrojov.

Buďte opatrní pri poskytovaní súkromných informácií na verejných miestach: Dbajte na to, aby ostatní nevideli vaše citlivé informácie, keď ich zadávate na verejných miestach, ako sú kaviarne, knižnice alebo verejné Wi-Fi siete.

5.5 Spam

Spam je nevyžiadaná komunikácia, ktorá je často masovo rozosiela elektronickou poštou, správami na sociálnych sieťach alebo inými komunikačnými kanálmi. Tento typ komunikácie je zvyčajne nežiaduci a často obsahuje reklamy, propagáciu nelegálnych alebo neetických služieb, falošné informácie alebo podvodné správy.

Spam sa často používa na rozšírenie nevyžiadaných reklám, phishingové pokusy o získanie citlivých informácií od používateľov, propagáciu falošných produktov alebo služieb, a mnoho ďalších nežiaducich aktivít. Tieto správy môžu byť veľmi rušivé a nepríjemné pre príjemcu.

Existujú rôzne techniky, ktoré sa používajú na boj proti spamu. Napríklad filtračný softvér, ktorý identifikuje a blokuje spamové správy, označovanie správ ako spamu používateľmi, zoznamy blokovaných adries alebo domén a ďalšie metódy. Tieto opatrenia pomáhajú minimalizovať množstvo spamu, ktoré dostávame do našej elektronickej pošty alebo na sociálnych sieťach.

Pokiaľ dostanete spamovú správu, odporúča sa ju označiť ako spam a odstrániť ju zo svojho doručeného priečinka. Dbajte tiež na to, aby ste nedávali svoju e-mailovú adresu na nedôveryhodných webových stránkach alebo ju nezverejňovali verejne, pretože to môže zvýšiť pravdepodobnosť dostávania spamu.

Spam je nežiaduci a obťažujúci, a preto je dôležité mať vhodné opatrenia na ochranu pred ním a minimalizovať jeho vplyv na online komunikáciu.

5.6 Počítačový vírus

Počítačový vírus je zvyčajne veľkosťou malý nástroj, ktorý sa šíri medzi počítačmi a môže spôsobiť rôzne škodlivé účinky. Škodlivé programy sa najčastejšie šíria prostredníctvom nežiaducich súborov, e-mailových príloh, infikovaných webových stránok alebo zdieľaných médií.

Počítačové vírusy majú rôzne formy a môžu vykonávať rôzne škodlivé činnosti. Medzi bežné typy počítačových vírusov patria:

- Logické vírusy: Tieto vírusy sa vkladajú do programov a sú schopné prepísať kód programov. Môžu spôsobiť poruchy alebo nežiaduce správanie programov.
- Bootovacie vírusy: Tieto vírusy infikujú sektor na pevnom disku a spúšťajú sa pri každom zapnutí počítača. Môžu narušiť zavádzanie operačného systému alebo iných dôležitých súborov.
- Makrovírusy: Tieto vírusy sa často šíria prostredníctvom dokumentov, ako sú dokumenty Word alebo Excel, ktoré obsahujú infikované makrá. Po otvorení infikovaného dokumentu sa vírus šíri do iných dokumentov alebo vykonáva škodlivé akcie.
- Ransomvér: Tento typ vírusu šifruje súbory na počítači a požaduje výkupné za ich obnovenie. Ransomvér môže spôsobiť veľkú straty údajov a finančnú škodu.

- Spyware: Tento typ škodlivého softvéru sleduje aktivity používateľa a zhromažďuje osobné údaje, ako sú heslá, bankové informácie alebo históriu prehliadania, ktoré sa potom môžu použiť na nelegálne účely.

Ochrana pred počítačovými vírusmi zahŕňa používanie aktualizovaného antivírusového softvéru, pravidelné aktualizácie operačného systému a aplikácií, opatrnosť pri sťahovaní a otváraní súborov z dôveryhodných zdrojov, vyhýbanie sa pochybným webovým stránkam a nedôverčivým e-mailom s prílohami. Dôležité je tiež pravidelne vytvárať zálohy dát, aby sa minimalizovali straty v prípade infekcie vírusom.

5.7 Otestujte svoje znalosti z témy ohľadom hackerov a škodlivých kódov

Otázka 1: Čo je spam?

a) Proces odosielania nevyžiadaných hromadných správ
b) Program na odstránenie vírusov z počítača
c) Metóda získavania hesiel pomocou podvodných webových stránok
d) Termín označujúci nežiadanú poštu alebo reklamné správy

Otázka 2: Čo je scam?

a) Typ počítačového vírusu
b) Systém, ktorý blokuje nechcené správy
c) Podvodná činnosť s cieľom oklamať a získať peniaze
d) Technika prenosu dát pomocou šifrovania

Otázka 3: Kto je hacker?

a) Osoba, ktorá vyvíja antivírusový softvér
b) Počítačový program na odhaľovanie hesiel
c) Osoba, ktorá neoprávnene preniká do počítačových systémov
d) Profesionálny bezpečnostný expert

Otázka 4: Aké je dôležité pravidlo pre zabránenie spamu?

a) Nikdy neotvárajte žiadne e-maily
b) Neklikajte na odkazy v nevyžiadaných e-mailoch a neposielajte im žiadne osobné údaje
c) Odstraňujte všetky e-maily bez ohľadu na to, kto ich posiela
d) Používajte iba počítače bez internetového pripojenia

Otázka 5: Čo je phishing?

a) Útok, pri ktorom sa hacker pokúša získať citlivé informácie od používateľov

b) Metóda prenosu vírusov medzi počítačmi v sieti
c) Ochranný softvér na zamedzenie phishingu
d) Sociálna sieť zameraná na profesionálne kontakty

Otázka 6: Aký je hlavný cieľ spamerov?

a) Infikovať počítače a získať kontrolu nad nimi
b) Rozšíriť počítačové vírusy
c) Poslať čo najviac nevyžiadaných správ na čo najväčší počet ľudí
d) Zbierať e-mailové adresy pre marketingové účely

Otázka 7: Čo je ransomvér?

a) Metóda zabezpečenia súborov na pevnom disku
b) Počítačový program na odstraňovanie spamu
c) Malvér, ktorý blokuje prístup k súborom a požaduje výkupné
d) Bezplatný softvér na ochranu pred vírusmi

Otázka 8: Ako sa môžete chrániť pred vírusmi?

a) Vykonávaním pravidelných aktualizácií softvéru a inštaláciou antivírusového programu
b) Otváraním všetkých e-mailových príloh, ktoré dostanete
c) Zdieľaním svojho hesla s priateľmi
d) Pripájaním neznámych zariadení k počítaču

Otázka 9: Čo je keylogger?

a) Metóda odstraňovania spamu z e-mailov
b) Počítačový program na monitorovanie a zaznamenávanie stlačených kláves
c) Hacker, ktorý používa klávesnicu na získanie hesiel
d) Program na rýchle písanie na klávesnici

Otázka 10: Čo je antivírusový softvér?

a) Program na odosielanie nevyžiadaných správ
b) Program na ochranu počítača pred vírusmi a iným malvérom
c) Program na získavanie hesiel od iných používateľov
d) Softvér na správu súborov a priečinkov

6 KYBERŠIKANOVANIE

Kyberšikanovanie, známe aj ako kyberšikana, je forma zneužívania elektronických komunikačných kanálov, ako sú internet, sociálne siete a iné online kanály na útoky, obťažovanie, vydieranie alebo šírenie nenávisti voči jednotlivcom alebo skupinám. Kyberšikanovanie môže zahŕňať rôzne formy, vrátane posielania hrozivých alebo urážlivých správ, zverejňovania neprimeraných alebo manipulatívnych informácií, šírenia manipulovaných obrázkov alebo videí, vytvárania falošných profilov na sociálnych sieťach s cieľom uškodiť obete alebo šíriť dezinformácie, a mnoho ďalších aktivít.

Kyberšikanovanie môže mať závažné dôsledky pre obete, vrátane psychologických, emocionálnych a sociálnych problémov. Môže viesť k strate sebavedomia, depresii, úzkosti a dokonca k úvahám o samovraždе. Je dôležité si uvedomiť, že kyberšikanovanie nie je iba nevinné obťažovanie alebo žartovanie, ale je to skutočný problém, ktorý si vyžaduje seriózne riešenie.

Mnohé krajiny majú zákony, ktoré zakazujú kyberšikanovanie a poskytujú obetiam právnu ochranu. Spoločnosti a organizácie sa tiež snažia bojovať proti kyberšikanovaniu prostredníctvom vytvárania bezpečnejších online prostredí, monitorovania a blokovania nevhodného obsahu, a poskytovania nástrojov a zdrojov pre obete.

Pokiaľ sa stane niekto obeťou kyberšikanovania, je dôležité, aby sa o tomto probléme hovorilo a aby obete dostali podporu a pomoc od svojho okolia a príslušných autorít.

6.1 Ako kyberšikanovanie rozoznať

Rozpoznať kyberšikanovanie môže byť niekedy ťažké, pretože sa často odohráva online a môže sa prejaviť rôznymi spôsobmi. Existuje viacero príznakov, na ktoré by ste mali byť pozorní, keď sa snažíte rozpoznať kyberšikanovanie:

- Opakujúce sa nevhodné správy: Obetiam kyberšikanovania často prichádzajú nevhodné, urážlivé alebo hrozivé správy cez e-maily, sociálne siete, textové správy alebo iné komunikačné kanály. Tieto správy sa môžu vyskytovať opakovane a s cieľom zneužívať, zastrašovať alebo uraziť obete.
- Manipulovaný alebo urážlivý obsah: Kyberšikana môže zahŕňať zverejňovanie alebo šírenie manipulovaných obrázkov, videí alebo iného obsahu, ktorý má za cieľ poškodiť obete alebo ich diskreditovať. Tento obsah môže byť upravený tak, aby obete vyzerali negatívne alebo aby ich zdiskreditoval.
- Vydieranie: Kyberšikanovanie môže zahŕňať aj pokusy o vydieranie obetí, ako napríklad hrozby zverejnením osobných informácií, fotografií alebo iných citlivých údajov obeti.
- Vytváranie falošných profilov: Kyberšikanovatelia často vytvárajú falošné profily na sociálnych médiách alebo iných platformách s cieľom šíriť dezinformácie, škodiť reputácii obete alebo šíriť nenávisť voči nim.

- Psychologické a emocionálne dôsledky: Obete kyberšikanovania často zažívajú negatívne dôsledky na svoje psychické a emocionálne zdravie. Môžu sa cítiť nahnevané, zraniteľné, úzkostlivé, depresívne alebo majú problémy so spánkom.

6.2 Metódy a spôsoby ako sa brániť proti kyberšikanovaniu

Existuje niekoľko spôsobov, ako sa brániť proti kyberšikanovaniu:

- Buďte obozretní pri zverejňovaní osobných informácií online. Neposkytujte neznámym ľuďom svoje adresy, telefónne čísla, heslá alebo iné citlivé údaje, ktoré by mohli byť zneužité.
- Skontrolujte a upravte svoje nastavenia súkromia na sociálnych médiách a iných online platformách. Obmedzte prístup k svojim osobným informáciám a prispôsobte si, kto môže vidieť váš profil, príspevky a fotografie.
- Ak vám niekto posiela nevhodné správy alebo sa vám snaží ublížiť online, použite možnosti blokovania a nahlásenia na danej platforme. Týmto spôsobom sa zbavíte nežiaduceho kontaktu a poskytnete informácie administrátorom služby, ktorí môžu vykonať potrebné kroky.
- Pokiaľ by ste boli obeťou kyberšikanovania, urobte si screenshoty alebo si zachovajte kópie nevhodných správ, obrázkov alebo iných dôkazov o kyberšikanovaní. Tieto dôkazy môžu byť neskôr dôležité pri nahlásení incidentu príslušným orgánom alebo poskytovateľom služieb.
- Nehanbite sa hovoriť o svojom probléme s dôvernou osobou, ako je rodina, priatelia, učitelia alebo pracovníci školy. Môžu vám poskytnúť podporu, poradenstvo a pomôcť vám prijať ďalšie kroky.
- Preskúmajte zákony a predpisy týkajúce sa kyberšikanovania vo svojej krajine. Môže existovať legislatíva, ktorá chráni obete a trestá kyberšikanovanie. Ak sa jedná o závažný prípad, môžete podať sťažnosť príslušným orgánom.

Je dôležité si uvedomiť, že každý prípad kyberšikanovania je iný a nie všetky metódy obrany budú rovnako účinné.

6.3 Ako sa postaviť za iných

Stáť sa spojivom a podporiť iných ľudí, ktorí sú obeťami kyberšikanovania, môže byť dôležitým krokom na boj proti tomuto problému.

Buďte empatickí voči obetiam kyberšikanovania a prejavte im svoju podporu. Aktívne počúvajte ich skúsenosti a povedzte im, že im rozumiete a že im veríte. Poskytnutie bezpodmienečnej podpory môže pomôcť obetiam cítiť sa menej izolovane.

Nenechajte kyberšikanovanie bez povšimnutia. Ak vidíte alebo počujete o prípade kyberšikanovania, prejaviť sa a vyjadriť svoje nesúhlas s takýmto správaním. Môžete sa postaviť za obete a jasne vyjadriť, že kyberšikanovanie je neprijateľné.

Použite svoj hlas a platformy na zvýšenie povedomia o kyberšikanovaní. Napíšte článok, zdieľajte informácie na sociálnych médiách, usporiadajte podujatie alebo sa zapojte do kampane, ktorá sa zameriava na zastavenie kyberšikanovania. Informovanosť a osvetová činnosť sú dôležité prostriedky na boj proti tomuto problému.

Vytvárajte a podporujte bezpečné a inkluzívne online prostredie. Aktívne sa angažujte v komunitách a fórach, aby ste zabezpečili, že sa dodržiavajú pravidlá slušného správania. Odmietajte kyberšikanovanie a podporujte rešpekt a toleranciu voči všetkým.

Ak ste svedkom kyberšikanovania, neváhajte to nahlásiť príslušným orgánom alebo administrátorom danej platformy. Poskytnite im všetky relevantné dôkazy a informácie, ktoré môžu pomôcť pri vyšetrovaní a riešení prípadu.

Ak poznáte niekoho, kto je obeťou kyberšikanovania, ponúknite mu podporu. Môžete im byť oporou, počúvať ich, ponúknuť pomoc pri riadení situácie alebo odporučiť odbornú pomoc, ak je to potrebné.

6.4 Príklady kyberšikany

Samotná kyberšikana môže mať rôzne podoby a prejavovať sa rôznymi spôsobmi.

- Vernostné útoky: Osoba môže byť terčom kyberšikany zo strany bývalého partnera alebo partnerky, ktorý/a sa snaží zneužiť osobné informácie, fotky alebo intímne záznamy na jej poškodenie. Tieto materiály môžu byť zverejnené online, posielať iným osobám alebo používať na vydieranie.
- Hanobenie a urážky online: Osoba môže byť terčom neustáleho hanobenia, urážok alebo nenávistných komentárov na sociálnych sieťach, diskusných fórach alebo komunitných stránkach. Tieto komentáre môžu mať negatívny vplyv na psychický stav obete a jej pocity sebahodnoty.
- Stalking sa prejavuje neustálym sledovaním osoby online. Stalker môže prenasledovať obeť prostredníctvom sociálnych médií, sledovať jej aktivity, komentovať príspevky alebo posielať neustále správy. Toto správanie môže obeti cítiť sa ohrozene a pocit stratenia súkromia.
- Šírenie falošných informácií: Osoba môže byť terčom kyberšikany prostredníctvom šírenia falošných informácií. Tieto informácie môžu mať negatívny vplyv na reputáciu, vzťahy alebo profesionálny život. Falošné informácie môžu byť zverejnené na webových stránkach, sociálnych sieťach alebo fóroch.
- Nekonzistentné zverejňovanie osobných informácií: Kyberšikanovanie môže zahŕňať nekonzistentné zverejňovanie osobných informácií o osobe. To môže zahŕňať zverejnenie mena, adresy, telefónneho čísla alebo iných citlivých údajov s cieľom spôsobiť škodu, vydierať alebo zastrašovať.

V predchádzajúcej podkapitole sme uviedli iba niektoré príklady kyberšikany a existuje mnoho ďalších spôsobov, akými sa môže prejavovať. Je dôležité si uvedomiť, že kyberšikana má reálne dôsledky na psychické a emocionálne zdravie obetí a je dôležité ju riešiť a bojovať proti.

6.5 Otestujte svoje znalosti z témy ohľadom kyberšikany

Otázka 1: Čo znamená termín "kyberšikana"?

a) Útočenie na počítačové siete.
b) Zneužívanie internetu na šírenie nenávisti alebo útočenie na iné osoby.
c) Bezpečné používanie sociálnych sietí.
d) Pravidlá pre ochranu osobných údajov.

Otázka 2: Ktoré z nasledujúcich príkladov je príkladom kyberšikany?

a) Nechcená reklama v e-mailovej schránke.
b) Zdieľanie pozitívnych správ na sociálnych sieťach.
c) Vytváranie silných hesiel na online účty.
d) Vysmievanie a šírenie hanlivých komentárov na internete.

Otázka 3: Ktoré z nasledujúcich je najlepším spôsobom, ako sa chrániť pred kyberšikanou?

a) Zdieľať osobné údaje s neznámymi osobami.
b) Vyberať si silné heslá a meniť ich pravidelne.
c) Ignorovať všetky negatívne správy na sociálnych sieťach.
d) Sťahovať pirátske kópie softvéru.

Otázka 4: Ktorá z nasledujúcich tvrdení je pravdivá o kyberšikane?

a) Postihuje iba mladých ľudí.
b) Má vždy rovnakú formu a techniku.
c) Môže mať vážne psychologické dôsledky pre obeť.
d) Obeť vždy pozná svojho kyberšikanéra.

Otázka 5: Čo je potrebné urobiť, ak ste obeťou kyberšikany?

a) Vydať to na súd.
b) Odpovedať na útok agresívnym spôsobom.
c) Oznámiť to príslušným autoritám alebo správcovi webovej stránky.
d) Ignorovať to a nechať to tak.

Otázka 6: Aký je účel kyberšikany?

a) Zábava a vtipkovanie.
b) Uškodiť, zastrašiť alebo ponížiť obeť.
c) Zviditeľniť obeť na internete.

d) Pomôcť obetiam rozvíjať odolnosť.

Otázka 7: Ktorý z nasledujúcich príznakov by mohol naznačovať, že niekto je obeťou kyberšikany?

a) Zlepšená duševná pohoda a sebavedomie.
b) Vyhýbanie sa používaniu internetu a sociálnych sietí.
c) Zdieľanie nadmerného množstva informácií o sebe.
d) Vlastnenie množstva ocenení a pochvaly online.

Otázka 8: Aká je dôležitosť informovania o kyberšikane?

a) Neexistuje žiadna dôležitosť.
b) Môže sa zhoršiť situácia obetí.
c) Môže pomôcť osvietiť ľudí o probléme a zabezpečiť podporu obetiam.
d) Je to zbytočné, pretože kyberšikana je nezvrátiteľná.

Otázka 9: Ktorá z nasledujúcich aktivít je príkladom kyberšikany?

a) Hranie online hier s priateľmi.
b) Zdieľanie pozitívnych správ na sociálnych sieťach.
c) Sledovanie videí na YouTube.
d) Neustále zasielanie urážlivých správ iným ľuďom.

Otázka 10: Aký je dôležitý prvý krok v boji proti kyberšikane?

a) Ukončenie všetkých online aktivít.
b) Rozhovor s dôveryhodnou osobou alebo dospelým.
c) Zverejnenie všetkých informácií o kyberšikanéri na internete.
d) Ignorovanie problému, pretože to prejde samo.

7 DIGITÁLNE UČENIE

Digitálne učenie (alebo online vzdelávanie) je proces získavania vzdelania alebo zručností prostredníctvom digitálnych technológií a nástrojov. Tento spôsob učenia sa stal populárnym v posledných rokoch vďaka technologickému pokroku a rozšíreniu prístupu k internetu.

Digitálne učenie ponúka študentom príležitosť študovať online, či už prostredníctvom kurzov, interaktívnych videí, webových seminárov alebo špeciálnych vzdelávacích platformách. Tieto online zdroje môžu byť prístupné cez počítače, tablety alebo smartfóny.

Digitálne učenie môže mať niekoľko výhod. Poskytuje flexibilitu a prístup k vzdelávaniu z rôznych miest a kedykoľvek je to pre študenta dostupné. Ďalšou výhodou je možnosť individuálneho tempa učenia, kde študenti môžu postupovať vo vlastnom tempe a opakovať študijné materiály podľa potreby.

Digitálne učenie môže zahŕňať rôzne interaktívne prvky, ako sú testy, kvízy, simulácie alebo diskusné fóra. Tieto prvky môžu pomôcť študentom lepšie si upevniť a aplikovať svoje vedomosti.

Existuje veľa online vzdelávacích platforiem, ktoré poskytujú rôzne typy kurzov a programov. Niektoré z týchto platforiem zahŕňajú napríklad MOOC (Masívne online otvorené kurzy), ktoré poskytujú bezplatné vzdelávanie od popredných univerzít a iných vzdelávacích inštitúcií.

V súčasnej dobe digitálne učenie zohráva dôležitú úlohu vo vzdelávaní a poskytuje príležitosť pre študentov, aby sa vzdelávali a získavali nové zručnosti prostredníctvom online prostredia.

7.1 Prečo sa nebáť online vzdelávania

Existuje nespočetne veľa dôvodov, prečo nie je potrebné mať strach pred online vzdelávaním. V nasledovnej podkapitole si uvedieme niekoľko dôvodov.

- Flexibilita: Online vzdelávanie poskytuje veľkú flexibilitu, pretože si môžete prispôsobiť čas a miesto svojho učenia. Nemusíte sa viazať na pevný časový plán alebo školský rok. Môžete si organizovať štúdium podľa vlastných potrieb a záujmov.
- Prístup k rôznym kurzom a programom: Online vzdelávacie platformy ponúkajú širokú škálu kurzov a programov z rôznych oblastí. Môžete si vybrať témy, ktoré vás zaujímajú, a mať prístup k špičkovému vzdelaniu od popredných inštitúcií a odborníkov.
- Vzdelávanie na diaľku: Online vzdelávanie umožňuje študentom vzdelávať sa aj na diaľku. Toto je obzvlášť výhodné pre tých, ktorí majú obmedzený prístup k tradičným vzdelávacím inštitúciám alebo žijú v odľahlých oblastiach. Okrem toho, vzdelávanie na diaľku umožňuje aj ľuďom so zdravotným postihnutím alebo s obmedzenou pohyblivosťou získať prístup k vzdelaniu.

- Interaktívne učebné materiály: Online vzdelávanie často obsahuje interaktívne učebné materiály, ako sú videá, kvízy, simulácie a diskusné fóra. Tieto prvky robia učenie zaujímavým a angažujúcim. Môžete sa naučiť nové veci prostredníctvom vizuálnych a auditívnych prostriedkov, čo môže uľahčiť zapamätávanie a porozumenie učiva.
- Výhodné náklady: Online vzdelávanie môže byť často cenovo výhodnejšie v porovnaní s tradičným vzdelávaním. Nemusíte platiť za presuny, ubytovanie alebo tradičné učebnice. Okrem toho existuje mnoho bezplatných online zdrojov a kurzov, ktoré si môžete vyskúšať.
- Komunita a podpora: Online vzdelávacie platformy často poskytujú komunitu študentov a možnosť vzájomnej podpory. Môžete sa zapojiť do rôznych diskusií, zdieľať skúsenosti a riešiť otázky s ďalšími študentmi a vyučujúcimi z celého sveta.

Samozrejme, online vzdelávanie má svoje výhody aj nevýhody. Niektorí ľudia uprednostňujú tradičný spôsob vyučovania a interakciu tvárou v tvár. Avšak s rastúcou dostupnosťou internetu a technologických pokrokov, online vzdelávanie ponúka nové a inovatívne spôsoby získavania vzdelania a zručností.

7.2 Ako z internetu vyťažiť čo najviac

Aby boli dosiahnuté čo najlepšie výsledky v online vzdelávaní, je dôležité miesto odkiaľ čerpať informácie a z akých kurzoch sa vzdelávať.

Internet je obrovským zdrojom informácií, takže sa naučte efektívne vyhľadávať. Skúste rôzne vyhľadávacie nástroje a naučte sa používať pokročilé vyhľadávacie operátory, ktoré vám pomôžu nájsť presnejšie výsledky.

Využite bohatú ponuku online kurzov a vzdelávacích platforiem, ktoré vám umožnia študovať nové témy a rozvíjať svoje zručnosti. Napríklad sú to platformy Coursera, Udemy, Khan Academy a ďalšie. Taktiež aj na Slovensku existuje Centrum vedecko-technických informácií SR (CVTI), ktorý ponúka bezplatný prístup k vedeckým databázam ako sú Scopus, Web of Science, Science Direct a podobne.

Vstúpte do online komunít a sociálnych sietí, ktoré sa zameriavajú na záujmy a oblasti, v ktorých chcete získať viac informácií. Zapojte sa do diskusií, sledujte relevantné profily a vyhľadávajte odborníkov, ktorí zdieľajú užitočné informácie. Avšak treba mať na zreteli aj z kapitoly o sociálnych sieťach a dezinformáciách a hoaxoch, že je veľmi dôležité a potrebné si informácie najprv overiť, či ide o skutočnosť.

Existuje množstvo podcastov a YouTube kanálov, ktoré poskytujú vzdelávací obsah v rôznych oblastiach. Taktiež existujú rôzne platformy, ktoré poskytujú audio podcasty na rôzne témy.

Mnohí odborníci zdieľajú svoje skúsenosti a znalosti prostredníctvom blogov a online publikácií.

Niektoré organizácie a inštitúcie ponúkajú online kurzy a webináre v reálnom čase, kde môžete získavať nové poznatky a odpovedať na otázky priamo od odborníkov v danej oblasti.

Je dôležité si uvedomiť, že internet je obrovským a dynamickým prostredím, preto je dôležité byť kritický a hodnotiť (detailnejšie v kapitole 8) zdroje, ktoré využívate. Vyberajte si dôveryhodné a overené zdroje informácií.

7.3 Najlepšie zdroje pre učenie v digitálnej podobe

Existuje mnoho vynikajúcich zdrojov pre učenie v digitálnej podobe. V nasledujúcej podkapitole si popíšeme rôzne zdroje rozdelené do kategórií, kde je možné nadobudnúť nové poznatky práve digitálnym vyučovaním.

Online kurzové platformy:

- Coursera (www.coursera.org)
- Udemy (www.udemy.com)
- edX (www.edx.org)
- Khan Academy (www.khanacademy.org)
- LinkedIn Learning (www.linkedin.com/learning)

Open-Access vzdelávacie zdroje:

- MIT OpenCourseWare (ocw.mit.edu)
- Harvard Online Learning (online-learning.harvard.edu)
- Stanford Online (online.stanford.edu)
- OpenLearn (www.open.edu/openlearn)
- TED-Ed (ed.ted.com)

Digitálne knižnice a zdroje:

- Project Gutenberg (www.gutenberg.org)
- Google Books (books.google.com)
- Internet Archive (archive.org)
- Open Library (openlibrary.org)
- ResearchGate (www.researchgate.net)

Jazykové zdroje:

- Duolingo (www.duolingo.com)
- Babbel (www.babbel.com)
- Memrise (www.memrise.com)
- Rosetta Stone (www.rosettastone.com)
- Lingoda (www.lingoda.com)

Programovanie a technológie:

- Codecademy (www.codecademy.com)

- FreeCodeCamp (www.freecodecamp.org)
- W3Schools (www.w3schools.com)
- Mozilla Developer Network (developer.mozilla.org)
- Udacity (www.udacity.com)

Online videá a tutoriály:

- YouTube (www.youtube.com) - Kanály ako TED, CrashCourse, Vsauce a podobne
- Lynda.com (www.lynda.com)
- Skillshare (www.skillshare.com)
- Pluralsight (www.pluralsight.com)
- 3Blue1Brown (www.3blue1brown.com) - Matematické videá

Tieto zdroje poskytujú široký rozsah kurzov, tutoriálov, videí a kníh, ktoré umožnia získať nové vedomosti a zručnosti v rôznych oblastiach.

Okrem svetových platforiem, existuje veľký počet slovenských platforiem, ktorých cieľom je vzdelávanie v online priestore.

- Slovensko.digital - Platforma Slovensko.digital ponúka online kurzy a vzdelávacie materiály zamerané na digitálne zručnosti, ako napríklad kurz "Základy IT pre ne-IT" alebo kurz "Digitálna gramotnosť pre seniorov".
- CodeWeek.sk - CodeWeek.sk je iniciatíva, ktorá sa zameriava na podporu digitálneho vzdelávania a programovania na Slovensku. Na ich webovej stránke sú rôzne vzdelávacie zdroje pre výučbu programovania pre rôzne vekové kategórie.
- IT e-learning - Portál IT e-learning poskytuje online kurzy z oblasti informačných technológií. Ponúkajú široký výber kurzov z rôznych tém, vrátane programovania, sietí, databáz a iných.
- eSlovensko - Projekt eSlovensko prináša vzdelávacie kurzy a materiály zamerané na digitálne nástroje a technológie. Obsahuje online kurzy pre rôzne skupiny používateľov, vrátane vzdelávania pre učiteľov a seniorov.
- UPnGO.sk - UPnGO.sk je vzdelávací portál zameraný na podnikanie, inovácie a digitálnu transformáciu. Ponúka online kurzy a tréningy, ktoré pomáhajú rozvíjať podnikateľské a digitálne zručnosti.
- eLearning.sk - Portál eLearning.sk poskytuje rôzne online kurzy a vzdelávacie materiály pre rôzne oblasti, vrátane IT, jazykov, manažmentu a ďalších. Obsahuje kurzy od rôznych poskytovateľov a inštitúcií.

Hore uvedené slovenské zdroje môžu pomôcť získať nové vedomosti a zručnosti v digitálnej oblasti. Podobne ako aj pri svetových platformách, uistite sa, že preveríte obsah a hodnotenie kurzov, aby ste si vybrali tie najvhodnejšie pre vaše potreby a záujmy.

7.4 V čom je online vzdelávanie lepšie ako “tradičné”

Pri podkapitole prečo sa nebáť online vzdelávania, boli popísané výhody online vzdelávania a jeho možnosti. Na záver kapitoly by sme zhrnuli a zopakovali najdôležitejšie výhody online

vyučovania oproti „tradičnému“. Online vzdelávanie ponúka niekoľko výhod oproti tradičnému vzdelávaniu:

- Flexibilita: Online vzdelávanie umožňuje prispôsobiť si študijný čas a tempo podľa vašich individuálnych potrieb a povinností.
- Prístup k rozmanitým zdrojom: Online vzdelávanie otvára dvere k bohatej škále digitálnych zdrojov, vrátane interaktívnych učebných materiálov, videí, online knižníc, výskumných článkov a ďalších.
- Individualizácia a personalizácia: Online vzdelávanie často umožňuje individuálny prístup k učebnému obsahu. Možnosť vybrať si kurzy a materiály podľa záujmov a potrieb.
- Medzinárodná spolupráca a komunita: Online vzdelávanie umožňuje komunikovať a spolupracovať s ľuďmi z celého sveta.
- Náklady a prístupnosť: Online vzdelávanie často poskytuje cenovo dostupnejšie možnosti vzdelávania ako tradičné vzdelávacie inštitúcie.
- Vývoj digitálnych zručností: Online vzdelávanie umožňuje získať a rozvíjať digitálne zručnosti, ktoré sú dôležité v súčasnom digitálnom prostredí.

7.5 Otestujte svoje znalosti z témy ohľadom digitálneho učenia

Otázka 1: Čo znamená skratka LMS vo vzťahu k digitálnemu učeniu?

a) Language Management System
b) Learning Management System
c) Local Monitoring Service
d) Lesson Mastery System

Otázka 2: Akým spôsobom môže digitálne učenie podporovať personalizáciu vzdelávania?

a) Poskytovaním štandardizovaných osnov pre všetkých študentov.
b) Umožnením študentom voliť si tematické smerovanie svojho štúdia.
c) Odmietnutím používania technológií vo vyučovaní.
d) Zavádzaním viac povinných testov a skúšok online.

Otázka 3: Aký nástroj by sa dal použiť na vytvorenie interaktívnej prezentácie pre digitálne učenie?

a) Microsoft Word
b) Google Sheets
c) PowerPoint
d) Adobe Photoshop

Otázka 4: Čo je MOOC vo vzťahu k digitálnemu učeniu?

a) My Online Open Course
b) Massive Open Online Course
c) Modern Online Offline Course
d) Master of Online Open Courses

Otázka 5: Aký je hlavný cieľ gamifikácie vo vzdelávaní?

a) Zabaviť študentov a stratiť čas.
b) Umožniť študentom vyhrávať ceny v súťažiach.
c) Zvýšiť motiváciu a angažovanosť študentov pri učení.
d) Zjednodušiť prácu učiteľom tým, že nahrádza ich úlohy.

Otázka 6: Ktorá z týchto platforiem je populárnym príkladom online kurzov a tutoriálov?

a) YouTube
b) LinkedIn
c) Twitter
d) Spotify

Otázka 7: Čo je BYOD vo vzťahu k digitálnemu učeniu?

a) Bring Your Own Device
b) Build Your Own Database
c) Be Your Own Director
d) Best Year of Development

Otázka 8: Aké sú výhody online diskusií a fór pri digitálnom vzdelávaní?

a) Možnosť stretnúť sa osobne so spolužiakmi.
b) Vytvorenie platformy pre výmenu názorov a spoluprácu.
c) Ochota učiteľov odpovedať na všetky otázky
d) Znižovanie potreby samoštúdia a prípravy.

Otázka 9: Čo je flipped classroom model vo vzťahu k digitálnemu vzdelávaniu?

a) Študenti učia učiteľov, miesto aby to bolo naopak.
b) Vyučujúci učia študentov, miesto aby sa študenti vzdelávali samostatne.
c) Študenti sa pripravujú doma a na vyučovaní sa riešia úlohy.
d) Vyučujúci a študenti spoločne vytvárajú učebné osnovy.

Otázka 10: Akým spôsobom môžu študenti získať spätnú väzbu pri digitálnom učení?

a) Iba prostredníctvom písomných testov.
b) Odovzdávaním úloh učiteľom na papieri.
c) Prostredníctvom online testov a hodnotení.
d) Ochotou učiteľov hovoriť so študentmi počas hodín.

8 KRITICKÉ MYSLENIE

Kritické myslenie je schopnosť analyzovať, hodnotiť a skúmať informácie, tvrdenia a situácie z rôznych perspektív. Je to schopnosť premýšľať nezávisle, racionálne a systematicky, aby sme dospeli k objektívnemu a informovanému záveru.

Kritické myslenie sa zakladá na schopnosti otvorenosti, zvedavosti, logiky, rozsiahleho porozumenia, schopnosti vyhodnotiť dôkazy a argumenty a schopnosť vyvodiť závery. Pomocou kritického myslenia si kladieme otázky, skúmame predpoklady, hodnotíme zdroje a identifikujeme slabé miesta v argumentoch.

Táto schopnosť umožňuje objektívne hodnotiť informácie, rozpoznať manipulatívne taktiky a klamy a chrániť sa pred neobjektívnymi názormi. Kritické myslenie je tiež dôležité pri riešení problémov, pretože umožňuje identifikovať a vyhodnotiť rôzne možnosti a nájsť najlepšie riešenie.

Kritické myslenie je cennou schopnosťou vo viacerých oblastiach života, vrátane vzdelávania, profesionálneho rozvoja, medziľudských vzťahov a osobného rastu. Pomáha prijímať informované rozhodnutia, rozvíjať nové nápady a riešiť komplexné problémy.

8.1 Pojem „dôveryhodná informácia“

Dôveryhodná informácia je informácia, ktorá je spoľahlivá, pravdivá a založená na overených zdrojoch. Dôveryhodné informácie sú tie, ktorým môžeme veriť a na ktoré sa môžeme spoľahnúť pri rozhodovaní, učení sa, alebo vytváraní si názorov.

Existuje niekoľko kritérií, ktoré pomáhajú posúdiť dôveryhodnosť informácií. Medzi spomenuté kritéria patria napríklad:

- Zdroj informácie: Dôveryhodná informácia pochádza z overeného a spoľahlivého zdroja, ktorý je kompetentný a má odborné znalosti v danej oblasti. Napríklad, ak potrebujete informácie o medicíne, je vhodné hľadať ich v publikáciách alebo webových stránkach uznávaných lekárov, vedeckých štúdiách alebo renomovaných zdravotníckych organizáciách.
- Objektivita: Dôveryhodná informácia je vyvážená a nepreukazuje zjavné predsudky alebo zaujatosť. Je dôležité vyhýbať sa informáciám, ktoré sa zameriavajú na manipuláciu alebo presviedčanie bez základu v dôkazoch.
- Overiteľnosť: Dôveryhodné informácie je možné overiť prostredníctvom dôkazov, zdrojov alebo zverejnených faktov. Je dôležité, aby informácie mali jasný základ a boli podložené overiteľnými dôkazmi.
- Aktualita: Dôveryhodná informácia je čo najaktuálnejšia a založená na najnovších dostupných poznatkoch a údajoch. Informácie, ktoré sú zastarané alebo nepreukazujú súčasný stav vecí, môžu byť menej dôveryhodné.
- Konsenzus: Dôveryhodné informácie sú často podporované viacerými nezávislými zdrojmi, ktoré súhlasia s podobnými tvrdeniami. Keď viacero zdrojov poskytuje podobné informácie, zvyšuje sa pravdepodobnosť ich dôveryhodnosti.

Je dôležité, aby sme si vždy skúmali zdroje a kriticky posudzovali informácie. V dobe šírenia dezinformácií (kapitola 3, o ktorej sme už detailne hovorili) je schopnosť rozpoznať a využívať dôveryhodné informácie dôležitá pre získanie správneho a objektívneho pohľadu na svet.

8.2 Využitie kritického myslenia

Kritické myslenie je potrebné v mnohých oblastiach nášho života. V nasledovnej podkapitole uvedieme niekoľko príkladov, kde je kritické myslenie dôležité a možné uplatniť.

Kritické myslenie je nevyhnutné pri štúdiu a učení sa. Pomáha nám vyhodnocovať informácie, rozvíjať analytické schopnosti a rozumieť hlbším súvislostiam. Kritické myslenie umožňuje nechať sa ovplyvniť len dôveryhodnými a podloženými faktami a vyhnúť sa klamstvám a nezmyslom.

V pracovnom prostredí je kritické myslenie cennou zručnosťou. Pomáha pri riešení problémov, analyzovaní situácií, rozhodovaní a inovácii. Schopnosť kriticky a logicky uvažovať pomáha prijímať informované rozhodnutia a riešiť výzvy, s ktorými sa stretávame vo svojej práci.

Kritické myslenie pomáha vnímať a chápať rozdielne perspektívy, rozoznávať manipulatívne taktiky a byť kritickí voči predsudkom a stereotypom. Týmto spôsobom môžeme vytvárať zdravé a vzájomne prospešné vzťahy založené na informovanom rozhodovaní a rešpektovaní iných ľudí.

Kritické myslenie je dôležité v oblasti verejného života a politiky. Pomáha rozpoznať manipuláciu, klamstvá a falšované informácie. Kritické myslenie umožňuje analyzovať politické platformy, argumenty a dôkazy, aby sme mohli rozhodne vyjadriť svoje názory a podporovať informovanú diskusiu.

Kritické myslenie je nevyhnutné aj pre osobný rast a sebareflexiu. Pomáha prehodnotiť presvedčenia, návyky a postoje. Kritické myslenie umožňuje pozerať sa na seba kriticky a objektívne, identifikovať naše silné a slabé stránky a vyvíjať sa ako jednotlivci.

V každom aspekte nášho života môže kritické myslenie pomôcť zlepšiť rozhodovanie, riešenie problémov a pochopenie sveta. Je to kľúčová zručnosť, ktorú je vhodné rozvíjať a používať vo všetkých oblastiach.

8.3 Overovanie informácií na internete

Overovanie správ a informácií na internete je dôležitým krokom pri kritickom myslení a zabránení šíreniu dezinformácií. V pokračovanie podkapitoly si poukážeme na fakty, ktoré je potrebné brať do ohľadu pri overovaní informácií.

Skúmajte a overte zdroj informácie. Zistite, či ide o renomované a dôveryhodné organizácie, univerzity, vládne agentúry alebo známeho odborníka v danej oblasti. Vyhnite sa anonymným zdrojom alebo stránkam, ktoré nemajú jasne uvedené svoje zdroje.

Skúste zistiť, či je web dôveryhodný. Napríklad sa môžete pozrieť na doménu (.gov pre vládne weby alebo .edu pre vzdelávacie inštitúcie), skontrolovať si ich históriu a reputáciu. Existujú aj faktické kontroly, ako napríklad *snopes.com* alebo *factcheck.org*, ktoré môžu pomôcť identifikovať pravdivosť informácií.

Porovnávajte informácie z viacerých zdrojov. Ak viacero spoľahlivých zdrojov potvrdzuje rovnakú informáciu, zvyšuje sa pravdepodobnosť jej pravdivosti. Vyhnite sa závislosti iba na jednom zdroji.

Zamerajte sa na kontext informácie. Skúste zistiť, kedy bola informácia zverejnená, či je aktuálna a aké sú okolnosti, v ktorých bola prezentovaná. Niekedy je manipulatívne použitie informácie alebo jej vytrhnutie z kontextu spôsobom, ako klamať alebo manipulovať.

Ak sa informácia týka konkrétnych faktov, ako sú číselné údaje, štatistiky alebo histórie, skúste ju overiť pomocou spoľahlivých zdrojov. Získanie nezávislých a overiteľných údajov vám pomôže oddeliť pravdu od dezinformácie.

Nezdieľajte informácie, o ktorých nie ste si istí ich dôveryhodnosťou. Snažte sa predísť šíreniu dezinformácií tým, že budete opatrní pri zdieľaní a podporujte len overené a spoľahlivé zdroje.

Kritické myslenie a overovanie informácií si vyžaduje čas a úsilie. Je dôležité byť informovaný a kriticky posudzovať informácie na internete.

8.4 Náznaky podozrivej správy

Existuje niekoľko príznakov, ktoré by sme mali mať na pamäti pri posudzovaní dôveryhodnosti správ. Prvým z nich je zdroj správy. Ak pochádza z neznámeho alebo neoveriteľného zdroja, ktorý nedokážeme overiť alebo ktorý neobsahuje relevantné informácie o svojej dôveryhodnosti, môže to vyvolať podozrenie.

Ďalším príznakom je použitie senzačných nadpisov alebo emocionálne ladeného obsahu. Správy, ktoré sa snažia vyvolať silné emocionálne reakcie, ako je hnev, strach alebo pobúrenie, by mali byť podrobené väčšej kritickej analýze.

Dôležitým faktorom je aj nedostatok dôkazov alebo zdrojov v správe. Ak nedokáže poskytnúť konkrétne dôkazy, zdroje alebo odkazy na podloženie svojich tvrdení, môže to byť varovný signál. Dôveryhodná informácia by mala byť podložená spoľahlivými zdrojmi alebo dôkazmi, ktoré umožňujú overenie informácie.

Ďalším aspektom, na ktorý by sme mali klásť pozornosť, sú nekonzistentnosti alebo protirečenia v správe. Ak obsahuje zjavne protirečiace si tvrdenia, nejasnosti alebo nekonzistentnosti v logike alebo faktoch, je dôležité byť ostražitý. Dôveryhodné informácie by mali byť konzistentné a logické.

Tiež by sme mali dbať na dostupnosť kontextovej informácie v správe. Správy, ktoré vynechávajú dôležitý kontext alebo sú neúplné, môžu zavádzať alebo klamať. Je preto dôležité si skontrolovať, či správa poskytuje dostatočné množstvo informácií a či je jej prezentácia vyvážená.

Okrem toho, gramatické chyby a nedostatočná kvalita samotného textu môžu slúžiť ako ďalší príznak nedôveryhodnosti. Správy s veľkým množstvom gramatických chýb, pravopisných chýb alebo zlou kvalitou prezentácie môžu naznačovať nedôkladnú redakčnú kontrolu a tým aj možnú nízku kvalitu informácií.

Je však dôležité poznamenať, že tieto príznaky nie sú stopercentnou zárukou toho, že správa je dezinformácia. Môžu však slúžiť ako varovné signály, ktoré by mali čitateľa podnietiť k ďalšiemu overovaniu informácií.

8.5 Emócie a kritické myslenie

Emócie a kritické myslenie sú dve dôležité zložky ľudského intelektu, ktoré môžu vzájomne ovplyvňovať. Vplyv emócií na kritické myslenie môže mať rôzne formy, ktoré si v pokračovaní detailnejšie popíšeme.

Prvým aspektom je predispozícia k potvrdzovaciemu zmätku. Keď sme emocionálne viazaní na určitý názor alebo postoj, môžeme byť náchylní k hľadaniu a preferovaniu informácií, ktoré potvrdzujú naše existujúce presvedčenia. Toto môže obmedziť náš objektívny pohľad na vec a brániť v prijímaní nových perspektív.

Druhým aspektom je skreslenie vnímania a hodnotenia informácií. Emócie môžu mať vplyv na spôsob vnímania a hodnotenia informácií. Ak sme napríklad nahnevaní alebo znechutení, môžeme byť náchylní k zaujatosti alebo skresleniu pri hodnotení informácií. Toto môže viesť k iracionálnym rozhodnutiam a založeniu hodnotenia na emocionálnych reakciách namiesto logického a faktického skúmania.

Tretím aspektom je manipulácia prostredníctvom emócií. Niektoré dezinformačné kampane a manipulatívne správy zámerne využívajú emócie, ako sú strach, hnev alebo znechutenie, na ovplyvnenie kritického myslenia. Tieto správy vytvárajú silné emocionálne reakcie, ktoré môžu prinútiť prijať informácie bez kritického skúmania alebo overovania.

Všetky tieto aspekty ukazujú, aký význam má emocionálna inteligencia a kontrola emócií pre kritické myslenie. Schopnosť rozpoznať, porozumieť a riadiť svoje emócie je kľúčová. Keď sme schopní udržať emócie pod kontrolou, môžeme lepšie analyzovať informácie a rozhodovať sa na základe objektívnych kritérií.

Ak chceme minimalizovať vplyv emócií na kritické myslenie, musíme si uvedomiť svoje vlastné emócie a byť si vedomí, ako môžu ovplyvniť náš pohľad na informácie. Je dôležité mať zdravý skepticizmus, vyhľadávať viacero zdrojov a overovať informácie, aby sme sa vyhli vplyvu emócií a dosiahli objektívnejšie rozhodnutia.

8.6 Návyky v kritickom myslení

Kritické myslenie je dôležitým nástrojom, ktorý umožňuje analyzovať a hodnotiť informácie s logikou a objektivitou. Vývoj návykov kritického myslenia je dôležitý pre schopnosť správne posudzovať a spracovávať informácie.

Overovanie informácií je nevyhnutné, aby sme si boli istí presnosťou a dôveryhodnosťou týchto informácií. Preto sledujeme zdroje, z ktorých pochádzajú, a vyhľadávame overiteľné a spoľahlivé zdroje.

Je dôležité identifikovať vlastné predsudky a zaujatosti, ktoré môžu ovplyvniť naše hodnotenie informácií. Snažíme sa byť objektívni a vyhodnocovať informácie na základe faktov a dôkazov.

Pamätáme si, že existuje viacero perspektív na danú tému, a snažíme sa pochopiť rôzne názory. Toto nám pomáha získať širší obraz a vyhnúť sa úzkemu mysleniu.

Pri hodnotení informácií sa zameriavame aj na analýzu argumentov. Skúmame logiku a kvalitu argumentov a vyhľadávame dôkazy a overiteľné zdroje, aby sme posúdili presvedčivosť a logiku argumentácie.

Okrem toho analyzujeme aj dôsledky informácií. Zohľadňujeme možné dopady a dôsledky informácií a porovnávame ich s uvedenými výhodami alebo dôsledkami.

Kladieme si aj kritické otázky s cieľom získať hlbšie porozumenie danej téme. Položenie otázok, ako napríklad "Prečo?", "Aké sú dôkazy?" a "Existujú alternatívne vysvetlenia?" nám pomáha lepšie posúdiť informácie.

Navyše sme pripravení prispôsobiť sa novým informáciám a revidovať naše názory a presvedčenia, ak získame nové dôkazy alebo argumenty.

Návyky kritického myslenia sa vyvíjajú prostredníctvom cvičenia a praktického uplatňovania. S časom sa stávame lepšími v hodnotení informácií a kritickom myslení.

8.7 Otestujte svoje znalosti z témy ohľadom kritického myslenia

Otázka 1: Čo je kritické myslenie?

a) Schopnosť pamätať si veľké množstvo údajov.
b) Proces hodnotenia a analýzy informácií.
c) Vnútorné presvedčenie bez skúmania fakty.
d) Zručnosť v riešení matematických problémov.

Otázka 2: Ktorá z nasledujúcich vlastností je súčasťou kritického myslenia?

a) Kreativita
b) Rýchle rozhodovanie
c) Schopnosť učiť sa z pamäti

d) Emocionálna reakcia

Otázka 3: Prečo je kritické myslenie dôležité?

a) Zvyšuje úroveň intelektuálnej nadradenosti.
b) Umožňuje ignorovať protichodné názory.
c) Umožňuje objektívne posudzovanie informácií.
d) Uľahčuje prijímanie rozhodnutí bez premýšľania.

Otázka 4: Aká je hlavná fáza kritického myslenia?

a) Hodnotenie a vyhodnocovanie.
b) Prijímanie predpokladov bez skúmania.
c) Rýchle odhadovanie bez analýzy.
d) Vytváranie zaujatých súdov.

Otázka 5: Ktorý z nasledujúcich prístupov sa nepovažuje za súčasť kritického myslenia?

a) Zhromažďovanie relevantných informácií.
b) Skúmanie logiky a presnosti argumentov.
c) Uvažovanie o alternatívnych možnostiach.
d) Kritizovanie a odmietanie bez uvažovania.

Otázka 6: Aká je úloha otázok v kritickom myslení?

a) Pomáhajú identifikovať chyby v logike.
b) Bránia premýšľaniu o problémoch.
c) Odpovedajú na všetky otázky predložené problému.
d) Uľahčujú prijatie prvotných dojmov bez skúmania.

Otázka 7: Ktorý z nasledujúcich postupov je súčasťou kritického myslenia?

a) Priradenie hodnoty informáciám bez skúmania.
b) Vyhodnotenie dostupných dôkazov.
c) Akceptovanie všetkých tvrdení ako pravdivých.
d) Pripisovanie významu neovereným zdrojom.

Otázka 8: Ktorá z nasledujúcich tvrdení najlepšie definuje logické skúmanie?

a) Prejavenie silného emócie voči nejakému problému.
b) Vnútorné presvedčenie o pravdivosti informácií.
c) Proces hodnotenia dôkazov a vzťahov.

d) Rýchle prijatie prvotných dojmov bez analýzy.

Otázka 9: Aká je úloha empatie v kritickom myslení?

a) Pomáha pochopiť a oceniť rôzne perspektívy.
b) Vylučuje potrebu zhromažďovať dôkazy.
c) Zabráni rozvoju schopností analýzy a hodnotenia.
d) Umožňuje prijímať informácie bez otázok.

Otázka 10: Aká je najlepšia stratégia pre rozvoj kritického myslenia?

a) Priradiť hodnotu emocionálnym impulzom.
b) Udržiavať status quo bez skúmania nových nápadov.
c) Sledovať jednostranné médiá.
d) Skúmať rôzne zdroje informácií.

9 GAMING

Gaming v kontexte kybernetickej bezpečnosti v online priestore je dôležitou oblasťou, pretože existuje množstvo potenciálnych hrozieb, ktoré môžu ovplyvniť bezpečnosť hráčov. Tieto dve oblasti sú úzko prepojené a majú veľký vplyv na online herné prostredie. Niektorým oblastiam sme sa venovali v predchádzajúcich kapitolách, ktoré taktiež súvisia aj s hraním hier v online priestore a v pokračovaní kapitoly ich detailnejšie popíšeme.

Prvým dôležitým aspektom je ochrana účtov a osobných údajov hráčov. Účty hráčov online hier obsahujú citlivé informácie a digitálne aktíva, ktoré je nevyhnutné chrániť pred neoprávneným prístupom a krádežou. Z tohto dôvodu je dôležité, aby vývojári hier implementovali bezpečnostné opatrenia, ako je dvojfaktorová autentifikácia a šifrovanie údajov, aby zabezpečili súkromie a bezpečnosť hráčov.

Okrem toho je potrebné riešiť aj hrozby spojené s podvodmi a phishingom. Taktiež aj v online hernom prostredí existuje riziko podvodných aktivít, ako sú pokusy o získanie citlivých informácií od hráčov pomocou phishingu. Vývojári hier musia venovať pozornosť identifikácii a blokovaniu takýchto podvodných pokusov a zároveň hráčov informovať o opatreniach, ktoré môžu prijať na ochranu pred podvodmi.

Bezpečnosť online hier a anti-cheat systémy sú ďalším dôležitým aspektom. Aby sa zabezpečila spravodlivá hra a zabránilo sa podvádzaniu, je potrebné mať v hre efektívne anti-cheat systémy. Tieto systémy slúžia na odhaľovanie a sankcionovanie hráčov, ktorí sa snažia používať nečestné metódy, ako sú cheaty a hacky.

Prevencia šikanovania a nevhodného správania je tiež dôležitým cieľom pri kybernetickej bezpečnosti v online hrách. V online hernom prostredí môže dôjsť k šikanovaniu a nevhodnému správaniu medzi hráčmi, čo narušuje pozitívnu atmosféru a zážitok z hry. Je nevyhnutné implementovať moderovanie komunikačných nástrojov, umožniť hráčom nahlásiť nevhodné správanie a rýchlo a spravodlivo reagovať na takéto incidenty.

Tiež, dôležitým aspektom je aj pravidelné aktualizovanie hier a odstraňovanie zraniteľností. Vývojári hier musia byť ostražití a pravidelne aktualizovať svoje hry, aby odstránili zraniteľnosti a chyby, ktoré by mohli ohroziť bezpečnosť hráčov. Zároveň je dôležité informovať hráčov o týchto aktualizáciách a zabezpečiť, aby ich implementovali, aby minimalizovali riziko zneužitia bezpečnostných chýb.

Celkovo je prepojenie medzi hraním online hier a kybernetickou bezpečnosťou dôležité, pretože poskytuje bezpečné a zábavné herné prostredie pre všetkých hráčov. Je nevyhnutné, aby vývojári hier a hráči spolupracovali na zabezpečení a ochrane pred rôznymi bezpečnostnými hrozbami, čím sa vytvára lepšia a bezpečnejšia herná komunita.

9.1 Ako tvoriť bezpečnú hráčsku komunitu

Tvorenie bezpečnej hráčskej komunity vyžaduje implementáciu niekoľkých kľúčových krokov. Jedným z opatrení je vytvorenie jasných pravidiel a etických zásad, ktoré stanovujú

akceptovateľné a neprijateľné správanie v komunite. Tieto pravidlá by mali byť viditeľne dostupné pre všetkých hráčov.

Dôležitým aspektom je tiež prítomnosť moderátorov alebo správcov, ktorí monitorujú herné prostredie a reagujú na nevhodné správanie. Títo moderátori by mali byť schopní rýchlo a spravodlivo riešiť konflikty a sankcionovať hráčov, ktorí porušujú pravidlá.

Zabezpečenie regulácie komunikačných nástrojov je ďalším dôležitým krokom. Je potrebné mať komunikačné kanály, ktoré majú filtráciu nevhodného správania, ako sú urážky, nadávky a šikanovanie.

Komunita by mala mať aj efektívne mechanizmy na nahlásenie hráčov, ktorí sa správajú nevhodne. Je dôležité, aby tieto nahlásenia boli pravidelne kontrolované a aby boli podniknuté opatrenia na riešenie problémov.

Posilňovanie pozitívneho správania je taktiež rovnako dôležité. Hráčov, ktorí prispievajú k pozitívnej atmosfére a správaniu, je potrebné odmeňovať a podporovať. To môže zahŕňať organizovanie výziev, súťaží, odmien a ďalších foriem motivácie. Edukácia hráčov o význame bezpečnej a rešpektujúcej komunikácie je tiež nevyhnutná.

Transparentnosť a zapojenie sú dôležité pre budovanie dôvery a zodpovednosti v rámci komunity. Je vhodné zapájať členov komunity do tvorby pravidiel a riešenia konfliktov. Okrem toho je dôležitá aj komunikácia s vývojármi hier. Poskytovanie informácií o bezpečnostných problémoch a správaní hráčov pomáha vylepšovať hru a komunitu ako celok.

Je dôležité si uvedomiť, že tvorenie bezpečnej hráčskej komunity je dlhodobý proces, ktorý si vyžaduje aktívne úsilie a spoluprácu zo strany všetkých zainteresovaných strán.

9.2 Symptómy hráčskej závislosti

Hráčska závislosť je komplexný fenomén, ktorý môže mať vážne dôsledky na fyzické, psychické a sociálne zdravie. Symptómy hráčskej závislosti sa prejavujú rôznymi spôsobmi a môžu byť rozdelené do niekoľkých skupín.

Prvou skupinou je sústavné venovanie sa hraniu hier na úkor iných povinností a záujmov. Osoba trpiaca hráčskou závislosťou často stráca záujem o aktivity, ktoré predtým považovala za dôležité alebo príjemné. Môže sa stať, že zanedbáva školské alebo pracovné povinnosti, zanedbáva vzťahy s rodinou a priateľmi, alebo prestáva cvičiť alebo angažovať sa v iných záujmoch, pretože jej väčšinu času zaberá hranie videohier.

Druhou skupinou je strata kontroly nad hraním a neúspešné pokusy obmedziť alebo prestať s hraním. Osoba trpiaca hráčskou závislosťou má často problém kontrolovať svoje herné správanie. Napriek snahám obmedziť alebo prestať s hraním sa jej to nedarí a pociťuje silný odpor alebo úzkosť. Tento nedostatok kontroly môže viesť k závislosti a zhoršovať situáciu.

Ďalšou skupinou je zvýšená podráždenosť a nepokoj pri pokuse obmedziť hranie alebo keď je osoba nútená byť bez prístupu k videohrám. Osoba trpiaca hráčskou závislosťou môže mať návaly hnevu, podráždenosti alebo nepokoj, keď je odrezaná od svojho herného

prostredia. Tieto emocionálne reakcie môžu byť prehnané a neprimerané voči situácii, čo môže mať negatívny vplyv na jej vzťahy a celkový pohodu.

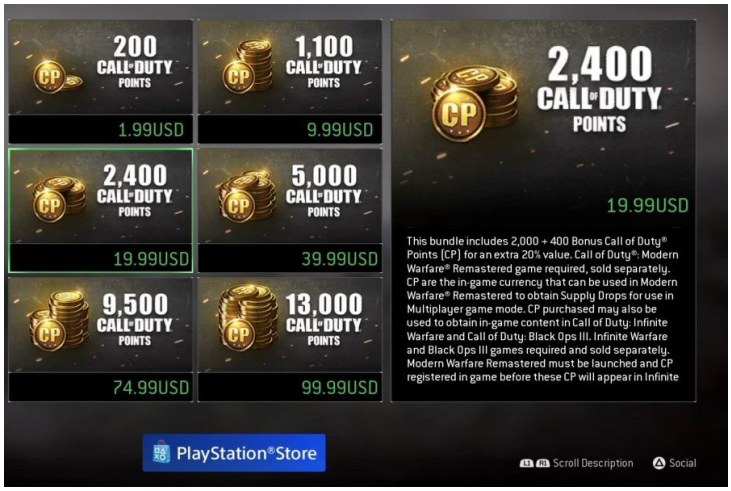
Ďalšou významnou skupinou je odskúšanie toho, že hranie videohier slúži ako únikový mechanizmus od negatívnych emócií alebo stresu. Osoba trpiaca hráčskou závislosťou môže využívať hranie videohier ako prostriedok na únik pred problémami, ako spôsob relaxácie alebo ako spôsob vyhýbania sa emocionálnym ťažkostiam. Tento vzor sa môže stať deštruktívnym, pretože osoba nemusí aktívne riešiť svoje problémy a môže sa ďalej pohrúžiť do hráčskej závislosti.

Je dôležité si uvedomiť, že tieto symptómy musia byť prítomné v dostatočnej miere aby spôsobili výrazný negatívny dopad na život jednotlivca, aby sme mohli hovoriť o hráčskej závislosti.

9.3 Mikrotransakcie a nákupy v hrách

Mikrotransakcie a nákupy v hrách sú súčasťou moderného herného priemyslu a predstavujú možnosť zakúpiť si virtuálne predmety, doplnky alebo „in-game“ obsah za reálne peniaze. Tieto transakcie môžu mať rôzne formy, ako sú mikroplatby, DLC (downloadable content) alebo loot boxy.

Mikrotransakcie sú malé platby, ktoré hráči môžu uskutočniť v hre za účelom získania určitých výhod alebo virtuálnych predmetov. Môžu to byť napríklad kozmetické zmeny vzhľadu postavy, vylepšenia, rýchlejší postup v hre alebo predmety, ktoré uľahčujú hranie. Tieto mikrotransakcie môžu byť buď jednorazové nákupy alebo opakujúce sa platby, ktoré sa často viažu na online hry s trvalým rozvojom obsahu.



Obrázok 14 Príklad mikrotransakcií [28]

DLC je forma obsahu, ktorý je dostupný na stiahnutie a je zvyčajne platený. DLC môže zahŕňať nové úrovne, príbehy, postavy, zbrane, misie alebo rozšírenia do hry, ktoré hráči môžu zakúpiť, aby rozšírili svoje herné skúsenosti. Tieto prídavné obsahy môžu priniesť nové a zaujímavé prvky do hry, ale zároveň môžu mať aj vplyv na rovnováhu a súťaživosť v online hernom prostredí.

Loot boxy sú kontroverznou formou mikrotransakcií, ktoré fungujú na princípe náhody. Hráči kupujú loot boxy, ktoré obsahujú náhodne vybraný obsah, ako sú virtuálne predmety, postavy, vylepšenia a podobne. Spomenutá forma je podobné hazardným hrám, pretože hráči nemajú zaručený obsah a môžu minúť veľa peňazí na loot boxy, aby získali požadované predmety.

Obrázok 15 Príklad lootboxov [29]

V niektorých prípadoch môžu mikrotransakcie a nákupy v hrách prinášať výhody a nový obsah, ktorý hráčom zlepšuje herný zážitok. Na druhej strane môže toto modelovanie podnikania viesť k nevyváženosti, vytváraniu nerovností medzi hráčmi a považuje sa aj za formu komerčného vplyvu na hráčov. Existuje aj obava, že mikrotransakcie a loot boxy môžu mať negatívny dopad na mladších hráčov a vyvolávať závislosť.

Je dôležité, aby hráči boli informovaní o tom, ako a za čo platia v hre, aby si mohli urobiť informované rozhodnutia o svojich nákupoch. Niektoré krajiny zaviedli regulácie týkajúce sa mikrotransakcií a loot boxov s cieľom chrániť hráčov, najmä mladšiu populáciu, pred potenciálnymi negatívnymi dôsledkami.

9.4 Zdroje na overenie vhodnosti hier

Keďže na trhu existuje nespočetne veľa hier, ktoré môžu mať rôzny obsah, odlišní zámer alebo vekové obmedzenie, je dôležité overiť vhodnosť hier. Z toho dôvodu existujú dostupné zdroje a nástroje, ktoré môžu poskytnúť potrebné informácie o hrách.

ESRB (Entertainment Software Rating Board) je americká organizácia, ktorá poskytuje hodnotenia a vekové kategórie pre videohry v Severnej Amerike. Ich hodnotenia obsahujú informácie o obsahu hry, či sa v hre nachádza násilie, vulgárny jazyk, sexuálny obsah a ďalšie. ESRB hodnotenie je možné vyhľadať na zadnej strane obalu hry alebo na online obchodoch.

PEGI (Pan European Game Information) je európsky systém hodnotenia hier. Poskytuje vekové kategórie a symboly, ktoré upozorňujú na obsah hry, ako je násilie, strach, sexuálny obsah a iné. Tieto hodnotenia sú zobrazené na obaloch hier a online platformách.

Common Sense Media je nezisková organizácia, ktorá poskytuje recenzie a hodnotenia hier, filmov, kníh a ďalších médií. Ich hodnotenia obsahujú informácie o vekových prístupových obmedzeniach a posudzujú obsah a prípadné problematické prvky v herných tituloch.

GameSpot a podobné webové stránky poskytujú podrobné recenzie a hodnotenia hier. Ich recenzie zahŕňajú informácie o obsahu, hernom zážitku a vhodnosti pre rôzne vekové skupiny.

Diskusné fóra a komunitné platformy venované hrám, kde je možnosť sa pripojiť a možnosť získať názory a skúsenosti od iných hráčov. Mnohí ľudia tam zdieľajú svoje dojmy a diskutujú o vhodnosti a obsahu hier.

Väčšina moderných herných konzol má funkciu rodičovského ovládania, ktoré umožňuje nastaviť obmedzenia pre prístup k určitým hrám na základe vekových kategórií a obsahu.

Je však dôležité si uvedomiť, že tieto zdroje poskytujú iba odporúčania a hodnotenia, avšak rozhodnutie o vhodnosti hry by malo byť individuálne a zohľadňovať osobné hodnoty a toleranciu pre určité obsahové prvky.

10 BEZPEČNÉ NAKUPOVANIE NA INTERNETE

V súčasnej dobe je nevyhnutné, aby sme venovali pozornosť bezpečnému nakupovaniu na internete, aby sme zabezpečili ochranu osobných a finančných údajov pred potenciálnymi kybernetickými hrozbami. V rámci oblasti kybernetickej bezpečnosti sa naskytá potreba dodržiavať niekoľko základných postupov, s cieľom znížiť riziko úniku dôležitých informácií a podvodov. Ďalšie časti tejto kapitoly sa detailne zameriavajú na konkrétne spôsoby, prostredníctvom ktorých môžeme posilniť úroveň bezpečnosti pri nakupovaní cez internet.

Udržiavajte svoje zariadenia, ako sú počítače, smartfóny a tablety, aktualizované na najnovšie verzie operačných systémov a softvéru. Spomenuté aktualizácie často obsahujú opravy bezpečnostných chýb, ktoré môžu chrániť systém pred hrozbami.

Používajte silné a jedinečné heslá pre rôzne online účty. Ideálne by mali obsahovať kombináciu písmen, číslic a špeciálnych znakov (o nastavení silného hesla sme detailnejšie hovorili v kapitole o osobných údajoch). Pre dvojúrovňovú autentifikáciu (2FA) použite možnosti, ako je SMS kód, e-mailové potvrdenie alebo autentifikačná aplikácia, ktorá zabezpečuje, že len vy máte prístup k vašim účtom.

Predtým ako vykonáte akýkoľvek nákup, skontrolujte, či ste na správnej webovej stránke. Overte si URL adresu a hľadajte dôkazy, že webová stránka online predajne je dôveryhodná, ako napríklad zámok vedľa URL, indikujúci bezpečné pripojenie.

Obrázok 16 Zámok indikujúci bezpečnosť webovej stránky [30]

Pri nakupovaní na internete dávajte prednosť bezpečným spôsobom platby, ako sú kreditné karty alebo platobné brány s ochranou proti podvodom. Vyhnite sa poskytovaniu citlivých finančných údajov prostredníctvom e-mailu alebo nezabezpečeného spojenia.

Pred nákupom skúmajte recenzie a skúsenosti iných zákazníkov s konkrétnym obchodom. Zoznámte sa s podmienkami vrátane politiky vrátenia a záruky produktu, v prípade, že by ste zakúpený tovar chceli vrátiť, pokiaľ by nákup nebol uspokojivý.

Pri nákupoch sa vyhýbajte verejným a nezabezpečeným Wi-Fi sieťam. Verejné siete môžu byť náchylné k odpočúvaniu a útokom (Man-in-the-middle útok), čo by mohlo ohroziť údaje.

Pravidelne si skontrolujte bankové výpisy a transakcie na účtoch. Pokiaľ zistíte nezvyčajné alebo neoprávnené transakcie, rýchlo o tom informujte svoju banku.

Online nakupovanie môže byť pohodlné, ale je dôležité byť obozretný a chrániť svoje osobné údaje. Dôkladné dodržiavanie týchto bezpečnostných opatrení napomôže minimalizovať riziko padnutia za obeť kybernetickým hrozbám.

10.1 Identifikácia podvodného internetového obchodu

Identifikovanie podvodného internetového obchodu predstavuje kritické zhodnotenie obchodu s cieľom ochrany osobných a finančných údajov. Existuje niekoľko indikátorov, ktoré popíšeme v pokračovaní podkapitoly, na základe ktorých je možné minimalizovať riziko stáť sa obeťou podvodu.

Veľmi dôležité je overiť URL adresu obchodu. Falošné webové stránky môžu mať podobné, avšak mierne odlišné adresy od legitímnych. Je veľmi podstatné, aby URL adresa začínala "https://" a zároveň by mal byť zobrazený zámok vedľa adresy, signalizujúci bezpečné pripojenie (obrázok z predchádzajúcej časti).

Pokiaľ stránka pôsobí amatérsky, obsahuje gramatické chyby, alebo nemá dostatočné informácie o produktoch a kontaktoch na zákaznícku podporu, môže to predstavovať varovný signál. Dôveryhodné obchody obvykle investujú do kvalitného vzhľadu stránky a podpory so zákazníkmi.

V prípade, že cena produktu je príliš nízka, nižšia než bola realistická, je to ďalší dôvod na odhalenie podvodného obchodu. Je dôležité porovnať ceny s inými obchodmi (napríklad prostredníctvom portálu *heureka.sk*) a byť opatrní voči veľmi výhodným zľavám a ponukám, ktoré by mohli byť príliš dobré, aby boli pravdivé.

Taktiež je veľmi dôležité skontrolovať, či sú na stránke uvedené kontaktné údaje, ako napríklad telefónne číslo, e-mail a fyzická adresa obchodu. Absencia týchto informácií alebo ich nedostupnosť by mohla signalizovať, že obchod nie je dôveryhodný.

Pokiaľ obchod ponúka iba nezvyčajné platobné metódy, mohlo by to taktiež naznačovať podvod. Zvyčajne dôveryhodné obchody umožňujú rôznorodé možnosti platby, či už priamo prostredníctvom bánk alebo platobných brán.

Recenzie a hodnotenia od iných zákazníkov sú taktiež dôležitým faktorom pre overenie internetového obchodu. Pokiaľ sa pri danom obchode nachádza množstvo negatívnych hodnotení alebo varovaní o danom obchode, môže to byť ďalší dôvod, prečo v danom obchode nekupovať.

Pri online nákupoch je nesmierne dôležité byť dobre informovaný o danom obchode. Pokiaľ by sa pri prehľadávaní obchodu nachádzal, jeden z vyššie uvedených nedostatkov, je lepšie vyhnúť sa nákupu a hľadať spoľahlivejšie alternatívy.

10.2 Zásady bezpečného online nakupovania

Aby bolo zaistené bezpečné nakupovanie online, je veľmi dôležité dodržiavanie zásad, ktoré môžu napomôcť pri nakupovaní a minimalizovať riziko podvodov a úniku osobných údajov. O niektorých zásadách sme hovorili aj pri iných kapitolách, ktoré sú všeobecné v rámci kybernetickej bezpečnosti. Taktiež popíšeme aj zásady, ktoré sú úzko späté pri online nakupovaní.

Je dôležité zistiť, či internetový obchod je dôveryhodný. Môžete začať kontrolou URL adresy obchodu, aby ste overili, či začína "https://". Navyše, hľadanie informácií o obchode, ako napríklad o histórii, kontaktných údajoch a spätných väzbách, môže poskytnúť predstavu o jeho spoľahlivosti.

Pri vytváraní účtu v internetovom obchode je nevyhnutné venovať pozornosť prihlasovacím údajom. Odporúča sa vytvoriť si silné heslo, ktoré zahŕňa kombináciu rôznych prvkov, ako sú veľké a malé písmená, číslice a špeciálne znaky. Zároveň je dôležité mať rôzne heslá pre rôzne účty a služby, aby sa minimalizovalo riziko úniku informácií.

Keď pri nákupe nasleduje krok zaplatenia za daný tovar je veľmi dôležité zhodnotiť, akú platobnú metódu použiť. Vo väčšine prípadov sa ponúka možnosť pre platbu na dobierku, čo znamená, platenie pri doručení tovaru. Týmto spôsobom sa môže zabezpečiť istota, že nakupujúci zaplatí iba vtedy keď tovar dostane. Na druhej strane, použitie platobných služieb ako PayPal môže poskytnúť ďalšiu vrstvu ochrany a možnosti reklamácie.

Pred vkladaním citlivých údajov pre platbu je dôležité sa uistiť, že internetový obchod používa zabezpečenú platobnú bránu. Vyhýbajte sa odovzdávaniu kreditných kariet a iných citlivých informácií na nezabezpečených stránkach. Pokiaľ by nastála situácia, že pre daný tovar sa môže platiť iba platobnou kartou je vhodné zvážiť nad využitým služieb, ktoré poskytujú digitálna platobné karty, napríklad Revolut, Wise, N26 a podobne.

10.3 Otestujte svoje znalosti z témy ohľadom bezpečného nakupovania na internete

Otázka 1: Čo je dvojfaktorová autentifikácia?

a) Ochranný antivírusový program.
b) Bezpečný spôsob platby cez internet.
c) Postup overovania, ktorý vyžaduje dve rôzne formy identifikácie.
d) Názov internetového obchodu.

Otázka 2: Ktorý typ spojenia je najbezpečnejší pre online nákupy?

a) Verejná Wi-Fi sieť.
b) Zabezpečená Wi-Fi sieť s WPA2 ochranou.
c) Mobilné dáta.
d) Nezabezpečená Wi-Fi sieť.

Otázka 3: Čo je SSL certifikát?

a) Druh online platobnej karty.
b) Bezpečný internetový prehliadač.
c) Špeciálny druh softvéru pre online nakupovanie.
d) Protokol na zabezpečenú komunikáciu medzi internetovým prehliadačom a webovým serverom.

Otázka 4: Aký je vhodný spôsob vytvárania silných hesiel pre online účty?

a) Používať rovnaké heslo pre viacero účtov.
b) Používať svoje meno a dátum narodenia.
c) Kombinovať písmená, číslice a špeciálne znaky.
d) Písať heslá na papier a uchovávať ich v dosahu.

Otázka 5: Čo je phishing?

a) Športový druh rybolovu.
b) Útok, pri ktorom sa útočník vydáva za dôveryhodnú osobu alebo inštitúciu s cieľom získať citlivé údaje.
c) Bezpečný spôsob online platieb.
d) Online hra, ktorá je populárna medzi rybármi.

Otázka 6: Aká je odporúčaná prax pri zadávaní údajov platobnej karty online?

a) Zverejniť číslo karty na sociálnych sieťach.
b) Uchovávať si fotografiu karty na smartfóne.
c) Používať overené a dôveryhodné stránky na platby.
d) Zdieľať údaje o karte s priateľmi.

Otázka 7: Čo je dočasný virtuálny číselník (CVV) na platobnej karte?

a) Sériové číslo karty.
b) Dátum exspirácie karty.
c) Bezpečnostný kód, ktorý sa nachádza na zadnej strane karty.
d) Heslo pre online platby.

Otázka 8: Ktorý typ recenzií môže byť pri online nákupoch často falošný?

a) Recenzie od overených zákazníkov.
b) Negatívne recenzie.
c) Recenzie s konkrétnymi detailmi o produkte.
d) Recenzie, ktoré majú všetky hodnotenia na maximum.

Otázka 9: Čo je "cookies" (súbory cookies) v kontexte internetových stránok?

a) Sladká pochúťka, ktorú si môžete objednať online.
b) Malé textové súbory, ktoré sa ukladajú na váš počítač a sledujú váš online správanie.
c) Bezpečnostné softvérové programy na ochranu pred hackermi.
d) Nový druh internetového prehliadača.

Otázka 10: Čo znamená "HTTPS" v URL adrese internetovej stránky?

a) Hypertext Transfer Protocol Secure - zabezpečený protokol pre prenos hypertextu.
b) Hyperlink Text Sharing Protocol.
c) High-Tech E-mail Processing System.
d) Home Page Testing and Security.

11 TIPY A TRIKY ČO ROBIŤ PRI RÔZNYCH SITUÁCIÁCH V ONLINE PRIESTORE

V dnešnej digitálnej dobe je online pôsobenie neoddeliteľnou súčasťou života. Bez ohľadu na to, či sme na sociálnych sieťach, komunikuje prostredníctvom e-mailu, nakupujeme online alebo hráme online hry, je dôležité mať na pamäti, že existujú rôzne situácie, ktoré môžu vyžadovať našu obozretnosť a rýchlu reakciu.

V nasledovnej kapitole sa pozrieme na rôzne tipy a triky, ktoré môžu pomôcť čeliť rôznym situáciám v online priestore s väčšou dôverou a bezpečnosťou. Napríklad, ako chrániť svoje účty, vyhýbať sa podvodom, riešiť problémy s pripojením, udržiavať si súkromie a ešte viac.

11.1 Zamietnutý prístup k účtu

Pokiaľ je z nejakého dôvodu znemožnený prístup dostať do účtu, bez ohľadu na to, či ide o e-mailový účet, sociálnu sieť alebo inú online službu, môže to byť frustrujúce, ale dôležité je postupovať krok za krokom, s cieľom obnoviť prístup k účtu. Existuje niekoľko krokov, ktoré je možné v takýchto situáciách vyskúšať:

- Skontrolovanie prihlasovacích údajov: Uistite sa, že zadávate správne prihlasovacie meno a heslo.
- Obnovenie hesla: Ak ste zabudli svoje heslo, využite možnosť obnovy hesla. Zvyčajne sa pri prihlasovaní nájde možnosť "Zabudli ste heslo?" alebo "Obnoviť heslo". Postupujte podľa pokynov a získajte nové heslo prostredníctvom e-mailu, telefónneho čísla alebo iných overovacích metód.
- Skontrolovanie funkčnosti pripojenia na internet: Ak ste si istí, že prihlasovacie údaje sú správne a stále nie je možne pripojiť sa do účtu, skontrolujte pripojenie na internet.
- Kontaktovanie podpory: Pokiaľ všetky obnovovacie kroky zlyhali alebo máte podozrenie, že účet mohol byť narušený alebo ukradnutý, existuje možnosť obrátiť sa na podporu poskytovateľa služieb.
- Overenie bezpečnostných otázok: Pokiaľ sú na účte nastavené bezpečnostné otázky pre obnovu, odpovedajte na otázky správne s cieľom získania prístupu k účtu.
- Skontrolovanie spamovej poštu: Niekedy sa e-maily na obnovu hesla môžu objaviť v iných priečinkoch ako je primárny, napríklad ako je spam alebo nevyžiadaná pošta.
- Prekontrolovanie zariadenia: Pokiaľ sa nemôžete prihlásiť z určitého zariadenia, skúste to z iného zariadenia. Možno je problém v zariadení, z ktorého sa snažíte prihlásiť.

Ak ani jedna z týchto možností nefunguje a aj naďalej nemôžete získať prístup k účtu, je nevyhnutné obrátiť sa na podporu poskytovateľa služieb, ktorý môže poskytnúť presnejšie rady a pomôcť s obnovením účtu.

11.2 Zdieľanie hesiel

Ako sme hovorili v kapitole o osobných údajoch, heslo prostredníctvom ktorého sa prihlasuje či už na sociálne siete alebo iné platformy, predstavuje určitú formu osobného údaje, ktoré je tajné a oddeľuje verejnú časť online sveta od súkromného.

V prípade, že známa osoba od vás žiada požičanie hesla, je dôležité postupovať opatrne. Poskytnutie hesla môže mať vážne dôsledky pre bezpečnosť a súkromie.

- Nezdieľanie hesla: Neposkytujte svoje heslo nikomu, ani známej osobe. Ako sme spomínali, heslo je osobnou informáciou a mali by ste si ho uchovávať dôverne.
- Informovanie známej osoby: Slušne a priateľsky vysvetlite známej osobe, že je to z bezpečnostných dôvodov a že nemôžete zdieľať svoje heslo s nikým, vrátane blízkych priateľov.
- Bezpečnosť: Pripomeňte známej osobe, že zdieľanie hesla môže byť nebezpečné a môže viesť k úniku dôverných informácií.
- Opatrne s citlivými informáciami: Vysvetlite známej osobe, že zdieľanie hesla môže otvoriť dvere pre prístup k iným citlivým informáciám, ako sú bankové údaje alebo osobné účty.
- Poukázanie na pravidlá: Ak ide o online službu alebo platformu, pripomeňte známej osobe, že zdieľanie hesla môže porušovať pravidlá a podmienky používania.
- Ponúknutie iného riešenia: Ak známa osoba potrebuje prístup k niečomu, čo máte na svojom účte, zistite, či existuje iné bezpečné riešenie, ako mu pomôcť bez zdieľania hesla.
- Uvedomenie si rizík: Myslite na to, že ak by sa niečo stalo s vaším účtom počas času, kedy známa osoba vlastní vaše heslo, mohlo by to viesť napríklad aj k sporom a nepríjemnostiam.

Dôležité je chrániť si heslá a súkromie. Je taktiež dôležité vysvetliť známej osobe dôvody, prečo sa neodporúča zdieľať heslo, a ak je to možné, ponúknite alternatívne spôsoby.

11.3 Vyhrážky a vydieranie

Situácia, keď sa niekto vyhráža alebo vydiera na internete, je vážna a vyžaduje okamžitú reakciu. O vyhrážkach a podozrivom správaní sa sme hovorili v kapitole o kyberšikane a v nasledujúcej podkapitole zhrnieme kroky ako chrániť svoje bezpečie v online priestore.

- Ignorovanie príspevkov: Je prirodzené cítiť sa vystrašene alebo nahnevané, avšak niekedy je vhodnejšie nereagovať na vydierača alebo vyhrážajúcu osobu. Odpovedanie môže viesť k ďalšiemu nežiaducemu správaniu alebo eskalácii situácie.
- Vytvorenie snímkov obrazovky alebo záznamu: Pokiaľ je to možné, vytvorte snímku obrazovky alebo záznamy všetkých správ alebo dôkazov o vydieraní či vyhrážaní sa. Tieto dôkazy môžu byť užitočné.
- Neotváranie odkazov a podozrivých príloh: Pokiaľ vydierač alebo vyhrážajúca osoba poslala odkazy alebo prílohy, neprehliadajte ich. Tieto odkazy môžu obsahovať

škodlivý softvér, o ktorom sme hovorili alebo ich použitie môže byť súčasťou pokusu získať viac informácií.

- Uzamknutie účtu: Pokiaľ máte podozrenie, že sú účty ohrozené, zmeňte svoje heslá a ak pokiaľ existuje možnosť, aktivujte viacúrovňovú autentifikáciu pre účty.
- Zablokovanie osoby: Pokiaľ existuje možnosť, zablokujte vydierača alebo podozrivú osobu. Týmto spôsobom je možné zabrániť ďalšiemu kontaktu.
- Nahlásenie situácie poskytovateľovi platformy: Ak sa vydieranie alebo vyhrážanie deje na sociálnej sieti alebo inom online fóre, je vhodné oznámiť situáciu administrátorovi alebo poskytovateľovi platformy s dôkladným popisom situáciu a s možnosťou priloženia dôkazov.
- Nahlásenie miestnym orgánom: Pokiaľ sa vyhrážky alebo vydieranie stále pokračujú, je vhodné obrátiť sa na miestnu políciu za účelom nahlásenia situácie a poskytnutím dostupných dôkazov.

Dôležité je chrániť svoju bezpečnosť a poveriť príslušné osoby, aby mohli situáciu vyšetriť a podniknúť opatrenia na zabezpečenie bezpečnosti online komunity.

11.4 Podozrivé správy

Na tému ohľadom hoaxov a osobných údajov sme písali v prechádzajúcich kapitolách a v pokračovaní si priblížme ako sa zachovať pri podozrivých správach.

V prípade podozrivých správ, je dôležité zachovať sa opatrne a vykonať niekoľko krokov, za účelom minimalizovania rizika pre bezpečnosť a súkromie.

- Neotváranie odkazov: Pokiaľ dostanete e-mail alebo správu obsahujúcu odkazy od neznámej osoby alebo zdroja, nepreklikávajte sa cez odkaz. Odkazy môžu viesť na škodlivé webové stránky alebo stiahnutie škodlivých softvérov.
- Neotváranie príloh: Podobne, neotvárajte prílohy od neznámych osôb, najmä ak sú v podozrivých formátoch (napríklad .exe súbory), pretože môžu obsahovať škodlivý kód.
- Skontrolovanie adresáta: Uistite sa, že správa je skutočne určená vám a niekomu inému. Niekedy môže prísť e-mail s chybnou adresou.
- Neposkytovaniu citlivých informácií: Nikdy neposielajte svoje heslá, osobné identifikačné čísla alebo iné citlivé informácie na základe nežiaducej správy. Dôveryhodné organizácie nikdy nebudú žiadať o tieto informácie e-mailom.
- Skontrolovanie gramatiky a pravopisu: Podozrivé správy často obsahujú gramatické chyby a nejasné formulácie. Buďte ostražití pri čítaní správ.
- Zablokovanie a nahlásenie: Pokiaľ dostávate opakované podozrivé správy od rovnakej osoby, je vhodné ju zablokovať a nahlásiť správcovi príslušnej platformy.
- Kontaktovanie poskytovateľov služieb: Pokiaľ ste si aj naďalej neistí ohľadom pravosti správy, môžete kontaktovať poskytovateľa služieb (napr. e-mailového poskytovateľa) a informovať ich o situácii.

- Používanie bezpečnostných softvérov: Dobrým opatrením je mať na zariadení aktualizovaný antivírusový program a softvér na ochranu pred spamom a škodlivými e-mailmi (o antivírusovom programe sme hovorili v prvej kapitole).

Prevencia je kľúčom k zachovaniu bezpečia na internete.

11.5 Správy od verejne známych osôb

V predchádzajúcej sme si detailne priblížili situácie ohľadom falošných správ. Medzi falošné správy je možné zahrnúť správy od verejne známych osôb, za ktoré sa môže ukrývať iná osoba. V prípade, že by správu poslala celebrita, môže to byť na prvý pohľad potešujúci moment, ale zároveň je dôležité zachovať si opatrnosť a rozumne sa správať.

- Overenie identity: Pokiaľ píše niekto tvrdiac, že je celebrita, je potrebné byť opatrný a skúsiť overiť totožnosť. Niekedy sa môže jednať o falošný profil alebo podvodníka. Rôzne online platformy, či už sú to sociálne siete alebo iné, vlastnia určitý mechanizmus na overovanie používateľov a verejne známym osobám napríklad k menu pridajú ikonku overenia a podobne.

Obrázok 17 Ikona overenej osoby na Instagrame [31]

- Nezdieľanie citlivých informácií: Bez ohľadu na to, aká je osoba na druhej strane, neposkytujte svoje osobné údaje, ako sú adresa, telefónne číslo, číslo kreditnej karty a podobne.
- Vyhnutie sa žiadosti o peniaze: Je potrebné byť opatrný na žiadosti o finančnú pomoc od celebrít, pretože môže ísť o pokus o podvod.
- Neklikanie na podozrivé odkazy: Pokiaľ celebrita posiela odkazy, je potrebné byť opatrný a neotvárať zaslané odkazy.
- Vyhýbanie sa tajne komunikácie: Buďte skeptickí voči celebritám, ktoré žiadajú, aby ste komunikovali s nimi tajne mimo verejných sociálnych sietí alebo iných platformách.
- Príliš rýchla reakcia: Buďte ostražití a neriešte dôležité veci alebo transakcie s celebritou príliš rýchlo. Je vhodné si vždy potvrdiť, že komunikujete so skutočnou osobou.
- Automatické odpovede: V niektorých prípadoch môžu byť odpovede celebrít na sociálnych sieťach alebo iných platformách automatické, a nie osobne písané.

Kontakty od celebrít alebo verejne známych osôb nemusia byť vždy autentické. Pokiaľ máte podozrenie, že niekto falšuje totožnosť, je potrebné o tom informovať príslušné orgány alebo platformu, kde k tomu dochádza.

11.6 Zapojenia sa do online súťaží

Pokiaľ sa na sociálnych sieťach zobrazí súťaž, ktorá sa zdá byť až príliš super, môže to byť pokušenie sa zapojiť a vyhrať. Je však veľmi dôležité kritický sa na súťaž pozrieť a zvážiť niekoľko faktorov pred tým, než sa rozhodnete do súťaže zapojiť.

- Skontrolovanie dôveryhodnosti: Pred zapojením do súťaže je potrebné si overiť, či je organizátor dôveryhodný a legitímny. Napríklad sa pozrieť na oficiálnu webovú stránku organizátora alebo hľadať recenzie alebo skúsenosti iných ľudí s podobnými súťažami.
- Pravidlá súťaže: Dôležité je prečítať si pravidlá súťaže, aké sú podmienky a aké sú pravidlá účasti.
- Neposkytovanie citlivých údajov: Buďte opatrní pri poskytovaní osobných údajov. Seriózne súťaže nepožadujú citlivé údaje, ako sú heslá alebo čísla kreditných kariet, pre potreby vyhodnotenia výhercu.

Cieľom súťaží by malo byť najmä zábava a možnosť získania nejakých cien. Avšak pri každej súťaži je potrebné zhodnotiť, či je skutočná a že nejde o určitú formu podvodu.

11.7 Označovanie na fotografiách

O zdieľaní fotografií na sociálnych sieťach sme hovorili v druhej kapitole. Sociálne siete ponúkajú okrem samotného zdieľania fotografií, označenie osôb, ktoré sa na fotografii nachádzajú. Častokrát sa stáva, že práve nestane situácia, kde je osoba označená nesprávne, alebo označená na fotku ohľadom súťaže a podobne. Pokiaľ nastane spomenutá situácia, je možné postupovať viacerými spôsobmi, ktoré si v pokračovaní podkapitoly popíšeme.

- Skontrolovanie nastavení súkromia: Pokiaľ si neželáte, aby sa vaša identita zobrazovala na fotografii verejne, môžete zvážiť zmenu nastavení súkromia. Na niektorých sociálnych sieťach je možnosť zvoliť, kto môže vidieť označenie na profile.
- Skontrolovanie obsahu fotografie: Predtým, ako sa rozhodnete ako na označenie zareagovať, skontrolujte, aký obsah sa nachádza na fotografii. Ak ide o nevhodnú alebo neželanú fotografiu, môžete požiadať, aby bola fotografia odstránená.
- Zablokovanie označenia: V prípade, že iná osoba pokračuje v označovaní na neželaných fotografiách, existuje možnosť zablokovanie označenia, aby bolo označovanie v budúcnosti znemožnené.

Sociálne siete ponúkajú a umožňujú kontrolu nad tým, čo sa zobrazuje na profile. Z toho dôvodu je potrebné zamyslieť sa nad tým aký obsah zdieľať s ostatnými používateľmi.

11.8 Online hry s virtuálnymi kamarátmi

O gamingu a hraní online hier sme hovorili v deviatej kapitole. Podobne ako pri iných online platformách rovnako aj pri gamingu nastávajú rôzne situácie, pri ktorých je dôležite správne

sa zachovať. Pri hraní hier s virtuálnymi kamarátmi, je dôležité dodržiavať etiketu online hier a správať sa ohľaduplne a s rešpektom.

- Byť priateľský a zdvorilý: Komunikujte s ostatnými hráčmi tak, ako by ste chceli, aby oni komunikovali s vami. Buďte priateľskí, zdvorilí a rešpektujte názory ostatných.
- Vyvarovanie sa nevhodného správania: Nepoužívajte vulgárne slová, neobťažujte ostatných hráčov, nešírte dezinformácie a nezastrašujte nikoho. Vyhýbajte sa agresívnemu alebo šikanujúcemu správaniu.
- Spolupráca s ostatnými spoluhráčmi: Hra je zábavná a efektívnejšia, keď hráči spolupracujú. Je dôležité byť tímový hráč a pomáhať ostatným dosahovať spoločné ciele.
- Vyvarovanie sa negatívnych konfliktov: Pokiaľ sa stretnete s nedorozumením alebo konfliktom, pokúste sa ho riešiť konštruktívnou komunikáciou. Nepúšťajte sa do hádok a nepoužívajte agresívne argumenty.
- Trpezlivosť a ústretovosť: Každý hráč má svoje individuálne schopnosti a skúsenosti. Je dôležité vyť trpezlivý a ústretový voči novým hráčom a pomáhať im, pokiaľ by mali problémy.
- Rešpektovanie herných pravidiel: Dodržujte pravidlá hry a nepodvádzajte. Podvody môžu spôsobiť zlé pocity a narušiť zážitok pre ostatných hráčov.
- Udržiavanie súkromia a osobných údajov: Vyhnite sa zdieľaniu príliš osobných informácií. Je dôležité byť opatrný, s kým zdieľate svoje kontaktné údaje a iné citlivé informácie.
- Ochrana vlastných pocitov: Pokiaľ narazíte na hráčov, ktorí šikanujú alebo narušujú pocity, nie je vhodné riešiť to s nimi. Namiesto toho hovor o tom s moderátorom alebo správcom hry, ktorí môžu prijať opatrenia.

Online prostredie je viac anonymné a niektorí ľudia sa môžu správať inak, než by robili v reálnom živote. Je veľmi dôležité zostať dôstojný, rešpektovať pravidlá a ostatných hráčov. Online hranie môže byť zábavný a spoločenský zážitok, ak sa všetci hráči správajú s tolerantne a navzájom sa podporujú.

11.9 Podvádzanie v online hrách

O situáciách, ktoré môžu nastáť pri hraní online hrách sme hovorili v predchádzajúcej kapitole. V pokračovaní si detailne popíšeme situácie, ktoré by mohli nastáť, pokiaľ by niekto pri hraní online hrách chcel podvádzať.

Zistenie, že niekto z tímu chce podvádzať v hre, môže byť nepríjemné a náročné. Je dôležité zachovať sa zodpovedne a zvážiť nasledujúce kroky:

- Otvorená komunikácia: Pokojne a otvorene sa porozprávať so spoluhráčom o jeho snahách podvádzať.
- Podporovanie fair play: Vysvetliť spoluhráčovi, že podvádzanie žiadnym spôsobom neprispeje k zábavnému a spravodlivému hernému zážitku. Podpora fair play je dôležitá pre vzájomné uznávanie a rešpekt medzi hráčmi.

- Byť príkladom: Ukázať svojím správaním a postojom, že dodržiavanie pravidiel hry a čestné hranie je správna cesta. Následne môže spoluhráč nasledovať príklad.
- Použitie interných mechanizmov hry: Pokiaľ je to možné, je vhodné upozorniť moderátora alebo správcu hry na nečestné správanie. Niektoré hry majú interné mechanizmy na odhalenie a potrestanie hráčov, ktorý podvádzajú.
- Ukončenie spolupráce v tíme: Pokiaľ niekto zo spoluhráčov neustúpi od podvádzania je vhodné zvážiť, či je to stále dobrý spoločník na hranie.

Je dôležité zachovať sa s rešpektom a dôstojnosťou voči spoluhráčom, ale zároveň treba dať najavo, že podvádzanie v hrách nie je rešpektované a nie je vhodné sa na tom podieľať.

11.10 Osobné stretnutie s online kamarátom

Pri hraní online hier sa častokrát vytvárajú kamarátske vzťahy, ktoré sa môže pretransformovať do skutočného kamarátstva aj mimo online priestoru. Pokiaľ nastane situácia, že sa kamarát z internetu chce stretnúť osobne, je dôležité byť obozretný a bezpečný. Stretnutie s neznámou osobou môže byť riskantné, preto je dôležité dodržiavať niekoľko opatrení na ochranu vlastnej bezpečnosti.

- Dôkladne sa spoznanie online: Predtým, ako sa rozhodnete stretnúť osobne, dôkladne spoznajte danú osobu online. Hovorte spolu napríklad cez správy, videohovory alebo telefón. Uistite sa, že ste sa dozvedeli čo najviac o ich záujmoch, záľubách a osobnosti.
- Stretnutie na verejnom mieste: Pokiaľ sa rozhodnete stretnúť osobne, vyberte si verejné miesto, napríklad kaviareň, reštaurácia alebo park. Verejné miesta poskytujú viac bezpečia, keďže sú často osvetlené a pohybujú sa v nich ľudia.
- Informácia o pláne blízkym osobám: Predtým, ako sa stretnete s novým kamarátom, informujte niekoho blízkeho o svojom pláne. Povedzte im, s kým sa stretávate, kde sa stretávate a očakávaný čas trvania stretnutia.
- Nezdieľanie osobných údajov: Nezdieľajte osobné údaje, ako sú adresa, telefónne číslo alebo informácie o rodine, s novým kamarátom, ak ho nepoznáte dostatočne dobre.
- Časový odstup: Ak si nie ste istí, či sa chcete s novým kamarátom stretnúť osobne, dajte si čas na zváženie.
- Dôverovanie vlastnému inštinktu: Ak sa v akomkoľvek okamihu stretnutia necítite pohodlne alebo bezpečne, neváhajte a ukončite stretnutie.

Bezpečnosť a pohoda sú na prvom mieste. Dôležité je zachovávať opatrnosť a zdravý úsudok pri stretnutiach s neznámymi osobami z internetu.

11.11 Finančné podporovanie online hráčov

V poslednej dobe na rôznych platformách sa objavujú možnosti ako podporiť hráčov, ktorý hranie online hier natáčajú a svoje herné zážitky zdieľajú s verejnosťou. Posielanie finančnej odmeny hráčom je spôsob, ako prejaviť podporu a oceniť ich obsah.

V pokračovaní popíšeme tipy, ako sa zachovať pri finančnom podporovaní online hráčov a na čo si dať pozor.

- Vyber dôveryhodnej platformy: Uprednostniť posielanie finančnej odmeny cez dôveryhodné a overené platformy. Veľa online hráčov používa služby ako *PayPal*, *Patreon*, *Twitch Cheer*, alebo iné platobné brány, ktoré zabezpečujú bezpečnú platbu.
- Udržiavanie rozumného množstva finančnej odmeny: Je veľmi dôležité nastaviť si rozpočet, akú výšku a ako často odosielať finančné odmeny hráčom. Uistite sa, že vaše posielanie je v súlade s finančnými možnosťami.
- Motivácia: Posielanie finančnej odmeny by malo byť predovšetkým motivačnou podporou a ocenením hráčovho obsahu.
- Rešpektovanie pravidiel platformy: Niektoré platformy majú pravidlá týkajúce sa obsahu finančných odmien.
- Finančné odmeny ako nástroj kontroly: Nepoužívajte finančné odmeny ako nástroj na manipuláciu s hráčom alebo s obsahom. Finančné odmeny by mali byť primárne prejavom podpory danému hráčovi.
- Rešpektovanie autorských práv: Pokiaľ hráč hrá hudbu alebo iný obsah, je dôležité rešpektovať autorské práva a nepožadovať zábavu, ktorá by mohla porušovať tieto práva.

Posielanie finančnej odmeny nie je záväzok, a predovšetkým by mal byť motivovaný úprimnou podporou. Uistite sa, že to robíte z dobrého dôvodu a s rešpektom voči hráčom a pravidlám platformy.

ZÁVER

V súčasnosti, kde digitálna revolúcia prenikla do každého aspektu našich životov, je kybernetická bezpečnosť kľúčovým kameňom nášho digitálneho blahobytu. Cieľom predlženej knihy bolo preskúmanie širokej škály tém týkajúcich sa tejto problematiky.

Kapitola o osobných údajoch ukázala, aký cenný aktív máme vo svete údajov a aké dôležité je ich správne chrániť. Čoraz viac sa stávame cieľmi pre zlomyseľných aktérov, ktorí by radi využili údaje na nekalé účely. Je našou zodpovednosťou chrániť si osobné údaje a podnikať kroky na minimalizáciu rizík.

Sociálne siete sú dvojsečným mečom, ktorý nám umožňuje spojiť sa so známymi a rodinou, ale zároveň predstavujú priestor pre šírenie dezinformácií, hoaxov a manipuláciu. Musíme sa naučiť kriticky hodnotiť informácie, ktoré konzumujeme a zdieľame, aby sme udržali integritu online komunít.

Hackeri a kybernetickí zločinci nám každodenne pripomínajú, že digitálny svet nie je imúnny voči zločinu. Preto je nevyhnutné, aby sme sa zoznámili s rôznymi metódami útokov, s cieľom adekvátne reagovať a ochrániť zariadenia a dáta.

Gaming a online nakupovanie sú príkladmi toho, ako digitálna transformácia mení tiež zábavné a konzumné zvyklosti. Je dôležité, aby sme si uvedomili, že aj na týchto miestach hrozia riziká a že je potrebné dodržiavať bezpečnostné opatrenia.

Ako sa chrániť na internete, existuje mnoho odporúčaní, ktoré by sme mali dodržiavať, aby sme minimalizovali riziká a zvýšili svoju kybernetickú bezpečnosť. Medzi tieto odporúčania patria používanie silných hesiel, aktualizácia softvéru na našich zariadeniach, používanie softvéru na ochranu proti vírusom a malvér, zabezpečenie súkromia a chránenie svojich osobných údajov, používanie dvojfaktorovej autentifikácie a opatrnosť pri klikaní na odkazy a sťahovaní súborov.

V závere môžeme povedať, že kybernetická bezpečnosť je dôležitou témou, ktorú by sme mali brať vážne. S rýchlym vývojom technológií sa množstvo rizík a nebezpečenstiev, ktoré nám hrozia na internete, neustále zväčšuje. Preto je dôležité, aby sme si uvedomili tieto riziká a používali internet s rozvahou a zodpovednosťou. Dodržiavaním základných zásad kybernetickej bezpečnosti môžeme minimalizovať riziká a chrániť svoju online identitu a súkromie.

Kybernetická bezpečnosť nie je iba zodpovednosťou jednotlivcov, ale aj spoločností, vlád a medzinárodných organizácií. Je potrebná spolupráca, vzdelávanie a neustále zdokonaľovanie sa, aby sme mohli úspešne čeliť výzvam, ktoré digitálny svet prináša. Zatiaľ sme niekde na začiatku dlhej cesty, avšak vedomosti a odhodlanie, ktoré sme nadobudli aj v rámci tejto knihy, nás povzbudzujú v tom, že môžeme dosiahnuť bezpečnejšiu a prosperujúcu digitálnu budúcnosť.

LITERATÚRA

[1] J. Ward and L. Kolodny, “The FBI has formed a national database to track and prevent ‘swatting,’” 2023. https://www.nbcnews.com/news/us-news/fbi-formed-national-database-track-prevent-swatting-rcna91722 (accessed Aug. 18, 2023).

[2] M. Wadud, “In Bangladesh a Facebook post can land you in jail for 14 years - South Asia News,” 2017. https://www.wionews.com/south-asia/when-a-facebook-post-can-land-you-in-jail-for-14-years-18085 (accessed Aug. 18, 2023).

[3] S. Le-Net, “Dog news: Awful puppy scam is targeting Facebook users: ‘It hurts my heart’ | Express.co.uk,” 2023. https://www.express.co.uk/life-style/life/1765669/dog-news-scam-warning-facebook-dxus (accessed Aug. 18, 2023).

[4] ADT, “Burglars Use Social Media to Find Targets - Blog | ADT,” 2017. https://www.adt.co.uk/blog/adts-top-tips-for-online-security (accessed Aug. 18, 2023).

[5] P. Lisovskaya, “Facebook virus - a modern spam campaign. - Step By Step With Trojan Killer,” 2022. https://trojan-killer.net/facebook-virus/ (accessed Aug. 18, 2023).

[6] C. Billingsley, “Facebook Privacy Settings: A Complete Walk-Through | Seek Social Media,” 2013. http://www.seeksocialmedia.com/facebook-privacy-settings-a-complete-walk-through/ (accessed Aug. 22, 2023).

[7] L. Smith-Spark, “F1 driver Jenson Button, wife robbed; was gas used? | CNN,” 2015. https://edition.cnn.com/2015/08/07/motorsport/jenson-button-france-burglary/index.html (accessed Aug. 18, 2023).

[8] S. Grover, “Easy Guide on How to Post Anonymously on Facebook Groups in 2023,” 2023. https://www.convosight.com/blogs/how-to-post-anonymously-on-facebook-group/ (accessed Aug. 22, 2023).

[9] A. S. Woodward, “Note on the Piltdown Man (Eoanthropus Dawsoni),” 1913. https://www2.clarku.edu/faculty/djoyce/piltdown/map_report_finds/note_pilt_man.html (accessed Aug. 18, 2023).

[10] Britanica, “Roswell incident | Overview, Theories, Hoaxes, & Facts | Britannica,” 2023. https://www.britannica.com/event/Roswell-incident (accessed Aug. 18, 2023).

[11] T. N. Y. Times, “Opinion | Autism Fraud - The New York Times,” 2011. https://www.nytimes.com/2011/01/13/opinion/13thu2.html (accessed Aug. 18, 2023).

[12] M. Kocis and K. K. Korff, “Exposing Roger Patterson’s 1967 Bigfoot Film Hoax,” 2004, Accessed: Aug. 18, 2023. [Online]. Available: www.michaelakocis.com.

[13] Europol, “COVID-19: Fake News | Europol,” 2021. https://www.europol.europa.eu/covid-19/covid-19-fake-news (accessed Aug. 22, 2023).

[14] BBC, “Chemtrails: What’s the truth behind the conspiracy theory? - BBC News,” 2022. https://www.bbc.com/news/blogs-trending-62240071 (accessed Aug. 18, 2023).

[15] M. Zennie, “Sandy memes: Sharks in post-Sandy spoof pictures of flooded neighborhoods | Daily Mail Online,” 2012. https://www.dailymail.co.uk/news/article-2226091/Sandy-memes-Sharks-post-Sandy-spoof-pictures-flooded-neighborhoods.html (accessed Aug. 22, 2023).

[16] Hvg.hu, “Itthon: 9/11: bocsánatot kért fotója miatt a titokzatos magyar turista | hvg.hu,” 2011. https://hvg.hu/itthon/20110912_tourist_guy_bocsanatkeres (accessed Aug. 22, 2023).

[17] D. Express Web, “Video: Is that really a dragon that’s been caught on tape in China? | Trending News - The Indian Express,” 2016. https://indianexpress.com/article/trending/viral-videos-trending/video-is-that-a-real-dragon-caught-on-tape-in-china-3098424/ (accessed Aug. 22, 2023).

[18] H. Pettit, “Image of crashed ‘UFO’ on the moon spurs conspiracy theories,” 2022. https://nypost.com/2022/06/29/image-of-crashed-ufo-on-the-moon-spurs-conspiracy-theories/ (accessed Aug. 22, 2023).

[19] A. FactCheck, “‘Vienna COVID protest’ photo is actually Moscow in 1991 - Australian Associated Press,” 2021. https://www.aap.com.au/factcheck/vienna-covid-protest-photo-is-actually-moscow-in-1991/ (accessed Aug. 22, 2023).

[20] V. Šnídl, “Šíri sa hoax: Vrátil som moslimovi peňaženku, varoval ma, nech nechodím na trhy,” 2017. https://dennikn.sk/956928/siri-sa-hoax-vratil-som-moslimovi-penazenku-varoval-ma-nech-nechodim-na-trhy/ (accessed Aug. 22, 2023).

[21] Tasr, “Informácie o problémoch po očkovaní sú nepravdivé | TREND,” 2021. https://www.trend.sk/spravy/informacie-vaznych-komplikaciach-ockovani-covid-19-su-nepravdive (accessed Aug. 22, 2023).

[22] L. Kovalčík, “Slováci naleteli hoaxu, šírila ho aj exministerka,” 2023. https://www.startitup.sk/statny-medved-na-prechadzke-v-martine-slovaci-naleteli-hoaxu-sirila-ho-aj-exministerka/ (accessed Aug. 22, 2023).

[23] M. Schwamberg, “5G siete a koronavírus: Konšpirácie už aj v Čechách,” 2020. https://www.mojandroid.sk/5g-vysielace-siria-koronavirus/ (accessed Aug. 22, 2023).

[24] Tasr, “Polícia upozorňuje na hoax, na Slovensku sa nepripravuje mobilizácia,” 2023. https://www.teraz.sk/slovensko/policia-upozornuje-na-hoax-na-slovens/685898-clanok.html (accessed Aug. 22, 2023).

[25] PasswordMonster, “Password Strength Meter,” 2023. https://www.passwordmonster.com/ (accessed Aug. 22, 2023).

[26] M. Menšík, “Polícia SR upozorňuje na podvodné SMS správy v mene slovenských inštitúcií - MojAndroid.sk,” 2023. https://www.mojandroid.sk/policia-sr-upozornuje-na-podvodne-sms-spravy/ (accessed Aug. 22, 2023).

[27] M. Mahútová, “Phishing láka obete aj cez sociálne siete | Tatra banka,” 2021. https://www.tatrabanka.sk/sk/blog/inovativne-bankovnictvo/pozor-novu-formu-phishingu-nachytat-vas-mozu-aj-cez-socialne-siete/ (accessed Aug. 22, 2023).

[28] D. Dubois, “Nickel and Dimed: Why Microtransactions Are Ruining Video Games – Tyrone Eagle Eye News,” 2018. https://tyroneeagleeyenews.com/nickel-and-dimed-microtransactions-are-ruining-video-games/# (accessed Aug. 22, 2023).

[29] D. Coldewey, “Loot boxes face scrutiny from an international coalition of gambling authorities | TechCrunch,” 2018. https://techcrunch.com/2018/09/17/loot-boxes-face-scrutiny-from-an-international-coalition-of-gambling-authorities/?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAALlaWN5Lay-2II6AeRzDDh-fr4QGZP8KQs5M3NlzGCD48bUDDIsU-NyYpyOrEZU2fJLIhfj (accessed Aug. 22, 2023).

[30] D. Vukadinovic, “What’s the difference between HTTP and HTTPS?,” 2018. https://www.globalsign.com/en/blog/the-difference-between-http-and-https (accessed Aug. 22, 2023).

[31] S. Srivastava, “How To Get Verified On Instagram: Here’s A Step-By-Step Guide -,” 2022. https://www.giznext.com/news/how-to-get-verified-on-instagram-heres-a-step-by-step-guide/ (accessed Aug. 22, 2023).

REGISTER (INDEX)

Názov: **Bezpečnosť na internete**

Autori: Mgr. Jan Francisti, PhD.

Vydavateľ: Univerzita Konštantína Filozofa v Nitre

Edícia: Prírodovedec č. 838

Schválené: Edičnou komisiou FPV UKF v Nitre dňa

Formát: A4

Rok vydania: 2023

Miesto vydania: Nitra

Počet strán: 91

Počet kusov: 100

ISBN 978-80-558-2114-6

PRÍLOHA 1 – SPRÁVNE ODPOVEDE Z TESTOV

Test z 1. kapitoly:

1b, 2b, 3d, 4a, 5b, 6b, 7c, 8b, 9b, 10a

Test z 2. kapitoly:

1a, 2d, 3c, 4a, 5d, 6a, 7b, 8a, 9c, 10d

Test z 3. kapitoly:

1b, 2b, 3c, 4d, 5b, 6d, 7d, 8b, 9c, 10b

Test z 4. kapitoly:

1b, 2b, 3c, 4c, 5d, 6b, 7b, 8c, 9a, 10b

Test z 5. kapitoly:

1a, 2c, 3c, 4b, 5a, 6c, 7c, 8a, 9b, 10b

Test z 6. kapitoly:

1b, 2d, 3b, 4c, 5c, 6b, 7b, 8c, 9d, 10b

Test z 7. kapitoly:

1b, 2b, 3c, 4b, 5c, 6a, 7a, 8b, 9c, 10c

Test z 8. kapitoly:

1b, 2a, 3c, 4a, 5d, 6a, 7b, 8c, 9a, 10d

Test z 10. kapitoly:

1c, 2b, 3d, 4c, 5b, 6c, 7c, 8d, 9b, 10a