



## BEZPEČNOSTNÉ ASPEKTY VYUŽÍVANIA INSTANT MESSAGINGU V AKADEMICKOM PROSTREDÍ

Lukáš Ježek<sup>1</sup>, Juraj Fabuš<sup>2</sup>

**Abstract:** In recent years, instant messaging (IM) has become an important communication tool in academic settings. Universities, students, and faculty use it to share information, collaborate, and coordinate educational activities. This paper focuses on a secondary analysis of academic sources to assess the benefits, risks, and security issues associated with students' use of instant messaging technology. Based on an analysis of more than 30 peer-reviewed publications, major threats such as social engineering, phishing, and insufficient encryption, along with the security level of each IM platform, are identified. At the same time, specific measures are proposed to enhance communication security in academic environments.

**Keywords:** instant messaging, communication security, students, colleges, encryption, MS Teams, Signal, digital literacy, secondary analysis, academia

### Úvod

Instant messaging (IM) sa stal neoddeliteľnou súčasťou modernej digitálnej komunikácie. V akademickom prostredí slúži nielen na neformálnu výmenu správ medzi študentmi, ale aj ako dôležitý nástroj pre spoluprácu, riadenie úloh, diskusie so školiteľmi a zdieľanie učebných materiálov. Jeho zvýšené využitie počas pandémie COVID-19 ešte viac zdôraznilo potrebu efektívnych a bezpečných komunikačných riešení.

Napriek mnohým výhodám, ako sú rýchlosť, dostupnosť a podpora multimédií, IM prináša aj viaceré bezpečnostné výzvy – od rizika úniku dát a phishingu až po nedostatočné šifrovanie správ. Vysoké školy sa tak musia vyrovnávať s potrebou nájsť rovnováhu medzi pohodlím používania a požiadavkami na ochranu údajov a súkromie.

Cieľom tohto odborného článku je preskúmať výhody a riziká používania IM v akademickom prostredí, identifikovať najbežnejšie bezpečnostné hrozby a navrhnúť konkrétne opatrenia na zabezpečenie bezpečného a efektívneho využívania týchto platforiem.

### Instant messaging

Instant messaging (IM) je forma digitálnej komunikácie, ktorá umožňuje okamžitú výmenu správ medzi používateľmi prostredníctvom internetu alebo iných sietí. V minulosti sa využíval predovšetkým na posielanie textových správ, avšak dnes ponúka široké spektrum

---

<sup>1</sup> Bc. Lukáš Ježek, Katedra spojov, FPEDAS, Žilinská univerzita v Žiline, Univerzitná 8215/1, 010 26 Žilina, e-mail: jezek@stud.uniza.sk

<sup>2</sup> Ing. Juraj Fabuš, PhD., Katedra spojov, FPEDAS, Žilinská univerzita v Žiline, Univerzitná 8215/1, 010 26 Žilina, e-mail: juraj.fabus@fpedas.uniza.sk

funkcií – od zdieľania súborov a multimediálneho obsahu až po hlasové a videohovory. Moderné IM aplikácie často obsahujú aj rôzne interaktívne prvky, ako sú emoji, nálepky a reakcie na správy. [1]

### Hlavné vlastnosti IM

1. Okamžitá komunikácia v reálnom čase  
IM umožňuje používateľom vymieňať si správy v reálnom čase, čo zvyšuje efektivitu a rýchlosť komunikácie. Štúdia publikovaná v *Journal of Computer-Mediated Communication* zdôrazňuje, že IM podporuje takmer synchronnú interakciu medzi používateľmi, čo je kľúčové pre efektívnu komunikáciu. [2]
2. Podpora multimediálnych prvkov  
Moderné IM aplikácie umožňujú nielen textovú komunikáciu, ale aj zdieľanie multimediálnych súborov, ako sú obrázky, videá či audio nahrávky. Tento aspekt bol analyzovaný v štúdiu publikovanej v *International Journal of Information and Education Technology*, kde sa uvádza, že IM platformy umožňujú efektívnu a účinnú komunikáciu prostredníctvom rôznych digitálnych formátov. [2]
3. Skupinové chaty a kolaborácia  
IM aplikácie často podporujú skupinové konverzácie, čo uľahčuje spoluprácu v tímoch a zdieľanie informácií medzi viacerými členmi naraz. Výskum v *Research in Learning Technology* ukazuje, že študenti využívajú IM na akademické účely, vrátane skupinových diskusií a riešenia administratívnych záležitostí. [3]
4. Indikátory prítomnosti a dostupnosti  
IM systémy často obsahujú funkcie, ktoré informujú o stave prítomnosti používateľov, ako napríklad “online”, “offline” alebo “zanepřázdněný”. Tieto indikátory pomáhajú koordinovať komunikáciu a zvyšujú efektivitu interakcií. Štúdia v *Journal of Computer-Mediated Communication* skúma, ako IM systémy podporujú rozvoj pracovných vzťahov prostredníctvom takýchto funkcií. [4]
5. Integrácia s inými nástrojmi a platformami  
Mnohé IM aplikácie sa integrujú s ďalšími službami, ako sú sociálne siete, e-mailové systémy či nástroje na správu projektov, čo umožňuje centralizovanú a efektívnu komunikáciu. Tento trend bol identifikovaný v prehľade publikovanom na platforme *ResearchGate*, kde sa diskutuje o vývoji a funkciách moderných mobilných messagingových aplikácií. [5]

### Technická architektúra IM

1. Klient-server model  
V klient-server architektúre IM systémov komunikujú všetci používatelia prostredníctvom centrálného servera, ktorý zaisťuje odosielanie a prijímanie správ. Tento model ponúka jednoduchú správu, monitorovanie a zabezpečenie komunikácie. Príklady takýchto systémov zahŕňajú AIM, MSN Messenger a Yahoo! Messenger. Medzi výhody patrí centralizovaná kontrola a bezpečnosť, keďže server môže implementovať jednotné bezpečnostné opatrenia. Na druhej strane, nevýhodou je riziko zlyhania servera a obmedzená škálovateľnosť pri vyššom počte používateľov. [6]
2. Peer-to peer (P2P) model  
V P2P architektúre komunikujú klienti priamo medzi sebou bez potreby centrálného servera. Každý uzol funguje ako klient aj server, čo zvyšuje odolnosť systému a zlepšuje ochranu súkromia. Príkladom takejto architektúry je aplikácia Tox, ktorá využíva end-to-end šifrovanie. Hlavnou výhodou je, že zlyhanie jedného prvku

nehrozuje celú sieť a priama komunikácia znižuje riziko sledovania. Na druhej strane, nevýhodou je vyššia komplexnosť správy, náročnejšia implementácia bezpečnostných politík a problémy so škálovateľnosťou pri veľkom počte používateľov. [7]

### Historický vývoj IM

Instant messaging (IM) sa od 60. rokov výrazne vyvinul. Prvým systémom, ktorý umožnil komunikáciu v reálnom čase, bol CTSS z roku 1961. V 70. rokoch sa objavil Talkomatic v systéme PLATO, nasledovaný Bulletin Board Systems (BBS). V roku 1988 bol predstavený Internet Relay Chat (IRC), ktorý umožňoval centralizovanú aj decentralizovanú textovú komunikáciu.

Deväťdesiate roky priniesli IM širokej verejnosti. V roku 1996 sa objavil ICQ, a o rok neskôr AOL Instant Messenger (AIM) s funkciou „Buddy List“. Následne prišli Yahoo! Messenger (1998) a MSN Messenger (1999). V Ázii dominoval čínsky QQ Messenger, ktorý neskôr ustúpil WeChat, vyvinutému na multifunkčnú platformu.

Veľkým zlomom v oblasti komunikácie bol príchod mobilných aplikácií, ako sú WhatsApp (2009), Facebook Messenger (2011) a Snapchat, ktorý zaviedol miznúce správy. Dnes aplikácie na okamžité správy, ako Signal a Telegram, kladú dôraz na súkromie, zatiaľ čo WeChat a WhatsApp ponúkajú aj funkcie pre platby a obchodné nástroje. Budúcnosť komunikácie prostredníctvom IM smeruje k vyššiemu zabezpečeniu, využívaniu umelej inteligencie a interaktívnejšej forme komunikácie. [8]

### Metodika a metódy skúmania

V článku bola použitá metóda sekundárnej analýzy, ktorá zahŕňa systematické preskúmanie, porovnanie a hodnotenie existujúcich odborných štúdií, článkov a výskumných správ týkajúcich sa instant messagingu v akademickom prostredí.

Do analýzy bolo zahrnutých viac ako 30 odborných, vedeckých a relevantných zdrojov, pričom sa kladol dôraz na aktuálnosť (obdobie 2019 – 2025), odbornú relevanciu a praktickú aplikovateľnosť v kontexte vysokých škôl.

Analyzované boli najmä tieto tematické okruhy:

- Funkčnosť a architektúra IM aplikácií
- Využitie IM v študentskej komunikácii
- Kybernetické riziká a útoky súvisiace s IM
- Prípadové štúdie z praxe
- Bezpečnostné odporúčania inštitúcií

Taktiež bola použitá metóda syntézy pre zlúčenie získaných poznatkov.

### Súčasný stav používania IM v akademickom sektore

V rokoch 2023 až 2025 sa instant messaging stal významným komunikačným nástrojom v akademických inštitúciách, pričom jeho využitie presahuje len neformálne rozhovory medzi študentmi. Výskumy ukazujú, že mobilné aplikácie na instant messaging (MIM) sú široko používané v akademickom aj profesionálnom prostredí. Táto forma komunikácie preukázateľne zlepšila tímovú prácu a produktivitu, pretože umožňuje rýchlu výmenu správ, súborov a videohovorov. Napríklad štúdia skúmajúca využitie WhatsApp v dištančnom vysokoškolskom vzdelávaní dospela k pozitívnemu hodnoteniu tejto platformy, s priemerným skóre 4,48 z 5, čo naznačuje jej prínos pre akademickú podporu vďaka jej prístupnosti a jednoduchosti používania. [9] [10]

Počas krízových situácií, ako bola pandémia COVID-19, sa význam instantnej komunikácie (IM) v akademickom prostredí ešte zvýšil. Obmedzenia fyzického kontaktu viedli k rastúcemu dopytu po nástrojoch virtuálnej komunikácie. Používanie IM, ako je WhatsApp, sa ukázalo ako cenný prostriedok pre výučbu a učenie. Učitelia mohli vytvárať

vzdelávací obsah, podporovať interakciu a dialóg, plánovať a riadiť čas učenia a vykonávať priebežné hodnotenie. Študenti mali možnosť zdieľať nápady, úvahy a študijné materiály v neformálnom prostredí, čo prispelo k väčšej účasti a rozvoju zručností v oblasti sebaorganizácie pri učení. [10] [11]

Napriek týmto výhodám existujú rozdiely v názoroch na efektívnosť instant messagingu (IM) medzi študentmi a inštruktormi. Výskumy naznačujú, že väčšina študentov (89 %) využíva IM na štúdium, zatiaľ čo inštruktori sú skeptickí voči jeho účinnosti a širšiemu prijatiu v oblasti vysokoškolského vzdelávania. Napriek tomu sa online chatovacie nástroje, vrátane WhatsApp, čoraz častejšie používajú na internú komunikáciu medzi zamestnancami. Skutočnosť, že väčšina študentov (95 %) nosí svoje telefóny do triedy a mnohí z nich počas vyučovania posielajú správy (92 %), naznačuje, že mobilné správy sú pre študentov prirodzenou formou komunikácie, ktorú by akademické inštitúcie mohli efektívnejšie využiť. [12] [13] [14]

### **Najpopulárnejšie IM platformy v rámci akademického sektora**

V akademickom sektore sa v období od 2023 do 2025 etablovalo niekoľko instant messagingových platforiem ako hlavné nástroje pre komunikáciu a spoluprácu. Medzi najobľúbenejšie patrí WhatsApp, Microsoft Teams, Slack a Telegram.

**WhatsApp** je obľúbený predovšetkým pre svoju dostupnosť a jednoduché ovládanie, čo z neho robí cenný nástroj na akademickú podporu a neformálnu komunikáciu medzi študentmi, a občas aj s učiteľmi. Jeho funkcie, ako zdieľanie multimédií a hlasových správ, umožňujú dynamickú výmenu informácií a poskytovanie personalizovanej spätnej väzby. [10] [11]

**Microsoft Teams** sa čoraz viac stáva komplexnou platformou pre akademické inštitúcie, ktorá integruje chat, zdieľanie súborov, zadávanie úloh, hodnotenie a videokonferencie. Jeho prepojenie s ďalšími aplikáciami balíka Microsoft 365 z neho robí silné riešenie na organizáciu tried, spoluprácu na projektoch a celkovú správu vzdelávacieho obsahu. Funkcie ako Immersive Reader a živé titulky zvyšujú prístupnosť platformy. [15]

**Slack** je ďalšou obľúbenou platformou, ktorá ponúka kanály pre organizovanú komunikáciu, priamu správu a integráciu s rôznymi nástrojmi, ako sú Zoom a systémy pre správu učenia (LMS). Často sa využíva na tímovú prácu, oznamovanie kurzov a budovanie študentských komunit. Jeho flexibilita a široké možnosti integrácie ho robia atraktívnym pre rôzne akademické účely. [16]

**Telegram** je známy svojou rýchlosťou, bezpečnosťou a bohatými funkciami, ako sú rozsiahle skupinové chaty a kanály. Aj keď nie je primárne určený na vzdelávanie, jeho obľúba medzi študentmi vedie k tomu, že sa často používa na neformálnu komunikáciu a zdieľanie študijných informácií. [17]

### **Bezpečnostné riziká spojené s používaním IM v akademickom kontexte**

Používanie instant messagingu v akademickom prostredí prináša množstvo výhod, ale aj významné bezpečnostné riziká, na ktoré je potrebné reagovať. Jednou z hlavných obáv je ochrana súkromia pri zdieľaní osobných informácií cez IM platformy. S ohľadom na to, že vyššie vzdelávanie sa v roku 2025 zameriava na posilnenie kybernetickej bezpečnosti, je dôležité starostlivo zvážiť potenciálne hrozby spojené s instant messagingom. [18] [19]

Mnohé systémy instant messagingu nie sú navrhnuté s dôrazom na bezpečnosť, čo uľahčuje kybernetickým útočníkom šírenie vírusov, spywaru, phishingových podvodov a malvéru. IM programy sa stávajú preferovanou metódou na šírenie sieťových vírusov a červov, a to vďaka ich nedostatočnej vstavanej bezpečnosti, možnosti sťahovania súborov a integrovanému zoznamu kontaktov, čo umožňuje rýchle rozšírenie škodlivého softvéru. [20]

**Phishing** predstavuje významné riziko. Útočníci môžu prostredníctvom instant messagingu posilať správy, ktoré sa zdajú byť dôveryhodné, s cieľom manipulovať používateľov, aby klikli na škodlivé odkazy, nainštalovali malvér alebo prezradili citlivé informácie, ako sú prístupové údaje. Rýchlosť a jednoduché šírenie správ cez IM robí tento spôsob útoku obzvlášť účinným. Výskumy naznačujú, že ľudia s vyššou sebaúčinnosťou môžu byť náchylnejší na phishingové útoky prostredníctvom instant messagingu. [21] [20] [22]

Ďalšie riziká zahŕňajú únik dôverných informácií prostredníctvom nezabezpečených komunikačných kanálov. Verejné platformy na okamžité správy často prenášajú nešifrované údaje, a preto by sa nikdy nemali používať na prenos citlivých alebo dôverných informácií. Správy odoslané cez internet sú náchylné na narušenie súkromia alebo neúmyselné odhalenie. [20] [23]

Hrozby pre sieť, ako sú trójske kone, útoky typu Denial of Service a únosy relácií, predstavujú ďalšie technické riziká spojené s používaním instant messagingu (IM). Keďže informácie prijaté prostredníctvom IM nie sú vždy overené, nie je možné potvrdiť, či správa skutočne pochádza od odosielateľa, s ktorým si príjemca myslí, že komunikuje. To otvára dvere k únosom relácií a k možnosti vydávať sa za inú osobu. [20]

V akademickom prostredí je dôležité zohľadniť aj právnu zodpovednosť spojenú so sťahovaním materiálov chránených autorským právom prostredníctvom IM sietí. [20]

V roku 2023 kybernetickí výskumníci odhalili množstvo škodlivých "modifikácií" instant messengeru Telegram, ktoré sú voľne dostupné na stiahnutie z Google Play. Tento nález poukazuje na pretrvávajúce bezpečnostné hrozby spojené s aplikáciami na okamžité správy. Vzhľadom na tieto riziká je pre akademické inštitúcie zásadné zaviesť komplexné bezpečnostné opatrenia a vzdelávať používateľov o bezpečnom používaní IM. [24]

### **Bezpečnostné opatrenia a odporúčania pre bezpečné používania IM v akademickom prostredí**

Na zníženie bezpečnostných rizík spojených s používaním instant messagingu v akademickom prostredí je potrebné zaviesť komplexné bezpečnostné opatrenia a dodržiavať odporúčané postupy. Akademické inštitúcie by mali vytvoriť jasné zásady pre používanie IM, ktoré určujú, čo je považované za prijateľné a neprijateľné správanie, a poskytnú pokyny na ochranu citlivých informácií. [23]

Dôležitým krokom je vzdelávanie študentov, učiteľov a zamestnancov o potenciálnych rizikách, ako sú phishingové útoky a šírenie malvéru prostredníctvom instant messagingu (IM). Používatelia by mali byť informovaní, aby neprezrádzali osobné údaje neznámym osobám a aby boli opatrní pri kliknutí na odkazy alebo otváraní príloh v správach, aj keď pochádzajú od známych kontaktov. Odporúča sa overiť totožnosť osôb, ktoré žiadajú o citlivé informácie cez IM, a v prípade pochybností kontaktovať danú osobu prostredníctvom iného komunikačného kanála. [20] [22]

Z technického hľadiska by mali inštitúcie preferovať bezpečné a šifrované platformy na okamžité správy. Platformy s end-to-end šifrovaním zabezpečujú, že obsah správ je prístupný iba odosielateľovi a príjemcovi, čím sa znižuje riziko odpočúvania zo strany tretích osôb. Pri výbere platformy je tiež dôležité zohľadniť jej súlad s predpismi o ochrane osobných údajov, ako je GDPR, najmä ak inštitúcia spolupracuje s medzinárodnými študentmi alebo vykonáva výskum, ktorý sa týka občanov EÚ. [26] [28] [27]

Používatelia by mali byť upozornení, aby nedovolili programom na okamžité správy (IM) zapamätať si heslá alebo automaticky sa prihlasovať do svojich účtov. Odporúča sa tiež neakceptovať automaticky prichádzajúce správy od neznámych používateľov a nezdierať súbory cez IM, pretože to môže viesť k šíreniu vírusov. [20]

Pri práci s citlivými údajmi je kľúčové vyhnúť sa diskusiám o nich prostredníctvom IM a neinštalovať IM aplikácie na počítače, ktoré obsahujú takéto údaje. Používatelia by mali mať na pamäti, že ich IM konverzácie nemusia byť súkromné ani bezpečné, a preto by sa mali vyhnúť zdieľaniu dôverných informácií týmto spôsobom. Namiesto posielania príloh s citlivými údajmi sa odporúča využívať zabezpečené šifrované siete a zdieľať odkazy na súbory uložené v bezpečných cloudových úložiskách. [20] [25]

Inštitúcie by mali zaviesť antivírusovú ochranu, ktorá pokrýva sieťové, desktopové a prenosné zariadenia, aby sa predišlo šíreniu malvéru prostredníctvom instant messagingu. Pravidelné aktualizácie softvéru IM aplikácií a operačných systémov sú taktiež kľúčové pre ochranu pred najnovšími hrozbami. [27] [20]

Na zvýšenie bezpečnosti sa odporúča implementovať dvojfaktorovú autentifikáciu všade, kde je to možné. Táto dodatočná vrstva ochrany pomáha chrániť účty pred neoprávneným prístupom. [29]

V rámci skupinových chatov by mali používatelia byť obozretní a opatrní pri klikaní na odkazy alebo volaní na telefónne čísla, ktoré zanechali neznámi členovia skupiny. Hostitelia skupín by mali zvážiť využitie svojich právomocí na kontrolu prístupu, aby predišli spamu a škodlivým aktivitám. [30]

Akademické inštitúcie by mali zvážiť sledovanie sieťovej prevádzky a zavedenie nástrojov na detekciu a prevenciu hrozieb, ktoré môžu pomôcť identifikovať a zablokovať škodlivé aktivity spojené s IM. [20]

## Záver

Sekundárna analýza ukázala, že aplikácie na okamžitú komunikáciu (IM) majú významný pozitívny vplyv na spoluprácu a komunikáciu medzi študentmi, najmä v tímových projektoch a počas dištančného vzdelávania. Študenti považujú IM za intuitívny a ľahko dostupný nástroj, pričom až 89 % z nich ho aktívne využíva na študijné účely.

Taktiež sa ukázalo, že rozdielne platformy majú rôznu úroveň bezpečnosti – Signal a Telegram sú vnímané ako bezpečné, WhatsApp je populárny, ale závislý od vlastníctva spoločnosti Meta, a MS Teams, hoci používaný v školách, neposkytuje end-to-end šifrovanie.

Výskumy zohľadnené v tomto článku zároveň poukazujú na to, že bezpečnostné opatrenia nie sú dostatočne nasadené na strane študentov, ale taktiež aj inštitúcií.

Instant messaging je nepochybne kľúčovým nástrojom v modernej komunikácii na vysokých školách. Jeho efektívnosť, dostupnosť a rýchlosť predstavujú jasné výhody, avšak so sebou prináša aj reálne riziká.

Výsledky sekundárneho výskumu ukázali, že najväčšími hrozbami sú sociálne inžinierstvo, nedostatočná ochrana súkromia a neznalosť používateľov.

Preto by bolo dobré zvážiť konkrétne odporúčania pre akademické inštitúcie a to:

- Uprednostňovať platformy s end-to-end šifrovaním
- Detailne vypracovať interné smernice pre študentov o vhodnom používaní
- Monitorovať a pravidelne hodnotiť bezpečnostné incidenty

Bezpečné a zodpovedné používanie instant messagingu medzi študentmi a zamestnancami vysokých škôl je možné dosiahnuť len kombináciou technického zabezpečenia, jasnej „politiky“ a vzdelávania.

## Literatúra

- [1] WIKIPEDIA CONTRIBUTORS (2019). *Instant messaging*. [online]. Wikipedia. Dostupné na: [https://en.wikipedia.org/wiki/Instant\\_messaging](https://en.wikipedia.org/wiki/Instant_messaging). [citované 20 Feb. 2025]

- [2] CHO, H.-K., TRIER, M. AND KIM, E. (2005). The Use of Instant Messaging in Working Relationship Development: A Case Study. *Journal of Computer-Mediated Communication*. [online]. Dostupné na: <https://academic.oup.com/jcmc/article/10/4/JCMC1044/4614493?utm> [citované 20 Feb. 2025]
- [3] ALT.AC.UK. (2025). *View of Exploring the use of text and instant messaging in higher education classrooms | Research in Learning Technology*. [online]. Dostupné na: <https://journal.alt.ac.uk/index.php/rlt/article/view/1345/html?utm> [citované 20 Feb. 2025]
- [4] CHO, H.-K., TRIER, M. AND KIM, E. (2005). The Use of Instant Messaging in Working Relationship Development: A Case Study. *Journal of Computer-Mediated Communication*. [online]. Dostupné na: <https://academic.oup.com/jcmc/article/10/4/JCMC1044/4614493?utm> [citované 20 Feb. 2025]
- [5] WANG, H.-Y. (2019). A Review of Instant Messaging and Mobile Messaging Applications. *International Journal of Economics, Finance and Management Sciences*. [online]. Dostupné na: [https://www.researchgate.net/publication/334483103\\_A\\_Review\\_of\\_Instant\\_Messaging\\_and\\_Mobile\\_Messaging\\_Applications](https://www.researchgate.net/publication/334483103_A_Review_of_Instant_Messaging_and_Mobile_Messaging_Applications) [citované 20 Feb. 2025]
- [6] INSTANT MESSAGING, *Internet Technologies and Applications*. [online]. Dostupné na: <https://sandilands.info/sgordon/teaching/its413y06s2/protected/ITS413Y06S2L10-Instant-Messaging.pdf?utm> [citované 20 Feb. 2025]
- [7] WIKIPEDIA CONTRIBUTORS (2024). *Tox (protocol)*. Wikipedia. [online]. Dostupné na: [https://en.wikipedia.org/wiki/Tox\\_%28protocol%29?utm](https://en.wikipedia.org/wiki/Tox_%28protocol%29?utm) [citované 20 Feb. 2025]
- [8] DESJARDINS, J. (2016). *The Evolution of Instant Messaging*. [online]. Visual Capitalist. Dostupné na: <https://www.visualcapitalist.com/evolution-instant-messaging/>. [citované 20 Feb. 2025]
- [9] YANG, Q. AND FENG, Y. (2024). Does the use of mobile instant messaging in the workplace increase employees' workload? *Behaviour & Information Technology*, [online]. Dostupné na: <https://doi.org/10.1080/0144929x.2024.2397681> [citované 20 Feb. 2025].
- [10] ROMERO-SARITAMA, J.M., ESPINOSA-TAPIA, S. AND PALACIOS-RODRÍGUEZ, A. (2025). Using WhatsApp in Distance Education: Assessing the Impact on Academic Interaction and Influencing Factors. *Social Sciences*, [online]. Dostupné na: <https://doi.org/10.3390/socsci14030183> [citované 20 Feb. 2025].
- [11] KEVIN (2024). *Instant Messaging: An Unexpected Resource for Learning English - World leading higher education information and services*. World leading higher education information and services. [online]. Dostupné na: <https://world.edu/instant-messaging-an-unexpected-resource-for-learning-english/>. [citované 20 Feb. 2025].
- [12] SOTILLO, S.M. (2006). *Using Instant Messaging for Collaborative Learning: A Case Study*. ResearchGate. [online]. Dostupné na: [https://www.researchgate.net/publication/242753905\\_Using\\_Instant\\_Messaging\\_for\\_Collaborative\\_Learning\\_A\\_Case\\_Study](https://www.researchgate.net/publication/242753905_Using_Instant_Messaging_for_Collaborative_Learning_A_Case_Study) [citované 20 Feb. 2025].
- [13] PROJECT.CO (2023). *Communication Statistics 2022*. [online]. Dostupné na: <https://www.project.co/communication-statistics/>. [citované 20 Feb. 2025].
- [14] BENNETT, S. (2025). *Classroom Messaging Statistics 2025 – Everything You Need to Know*. [online]. Dostupné na: <https://llcbuddy.com/data/classroom-messaging-statistics/> [citované 20 Feb. 2025].
- [15] Microsoft Teams for your classroom. [online]. Dostupné na: <https://www.microsoft.com/cms/api/am/binary/RWKBOr> [citované 20 Feb. 2025].

- [16] SLACK (N.D.). *Distance Learning with Slack*. [online]. Dostupné na: <https://slack.com/solutions/distance-learning>. [citované 20 Feb. 2025].
- [17] CONNELL, A. (2025). *10 Most Popular Messaging Apps In 2025 (Data + Trends)*. [online]. Dostupné na: <https://adamconnell.me/popular-messaging-apps/> [citované 20 Feb. 2025].
- [18] RESEARCHANDMARKETS.COM (2023). *Instant Messaging Market Size, Share & Forecast to 2030*. Researchandmarkets.com. [online]. Dostupné na: <https://www.researchandmarkets.com/report/instant-messaging> [citované 20 Feb. 2025].
- [19] KIM FAHEY (2025). *Top 8 Disruptive Trends Shaping Higher Ed in 2025 - Collegis Education*. [online]. Dostupné na: <https://collegiseducation.com/insights/resources/top-eight-disruptions-in-2025/> [citované 20 Feb. 2025].
- [20] UNIVERSITY, CARNEGIE MELLON (2023). *Instant Messaging Security and Usage Guideline - Information Security Office - Computing Services - Carnegie Mellon University*. [online]. Dostupné na: <https://www.cmu.edu/iso/governance/guidelines/im.html>. [citované 20 Feb. 2025].
- [21] CHECKPOINT.COM (2020). *What Is Phishing? Check Point Software*. [online]. Dostupné na: <https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/>. [citované 27 Feb. 2025].
- [22] LEE, Y.Y., GAN, C.L. AND LIEW, T.W. (2023). *Thwarting Instant Messaging Phishing Attacks: The Role of Self-Efficacy and the Mediating Effect of Attitude towards Online Sharing of Personal Information. International Journal of Environmental Research and Public Health*. [online]. Dostupné na: <https://doi.org/10.3390/ijerph20043514> [citované 27 Feb. 2025].
- [23] UWATERLOO.CA (2024). *E-mail & Instant Messaging | Information and Privacy | University of Waterloo*. [online]. Dostupné na: <https://uwaterloo.ca/privacy/guidelines/e-mail-instant-messaging> [citované 27 Feb. 2025].
- [24] WIKIPEDIA CONTRIBUTORS (2019). *Instant messaging*. [online]. Dostupné na: [https://en.wikipedia.org/wiki/Instant\\_messaging](https://en.wikipedia.org/wiki/Instant_messaging). [citované 27 Feb. 2025].
- [25] ITS.UCSC.EDU (n.d.). *Protect Information when using the Internet and Email*. [online]. Dostupné na: <https://its.ucsc.edu/security/internet.html>. [citované 27 Feb. 2025].
- [26] LIYANDA TEMBANI (2024). *Risks of using regular text messaging for mental health communication*. [online]. Dostupné na: <https://www.paubox.com/blog/risks-of-using-regular-text-messaging-for-mental-health-communication> [citované 27 Feb. 2025].
- [27] NORTHWESTERN ENGINEERING. (2025). *Tips for Increasing Your Privacy from Security Experts*. [online]. Dostupné na: <https://www.mccormick.northwestern.edu/news/articles/2025/02/tips-for-increasing-your-privacy-from-security-experts/> [citované 27 Feb. 2025].
- [28] TEXT-EM-ALL.COM (2025). *The Complete Guide to Mass Texting for Universities*. [online]. Dostupné na: <https://www.text-em-all.com/ultimate-guide-to-mass-texting-for-universities> [citované 27 Feb. 2025].
- [29] VPNSUPER.COM. (2025). *Is Academia.Edu Safe and Legit to Use in 2025*. [online]. Dostupné na: <https://www.vpnsuper.com/blog/is-academia-edu-safe> [citované 27 Feb. 2025].
- [30] FSU.EDU (2024). *Stay Secure: Top Cybersecurity Tips for Online Messaging Apps*. [online]. Dostupné na: <https://its.fsu.edu/article/stay-secure-top-cybersecurity-tips-online-messaging-apps> [citované 27 Feb. 2025].