

From Provoking Emotions to fake Images: The Recurring Signs of fake news and Phishing Scams Spreading on Social Media in Hungary, Romania and Slovakia

Kenyeres Attila Zoltán¹ and Lauren Weigand²

¹Eszterházy Károly Catholic University, Eger, Hungary

²Duquesne University Kline School of Law

kenyeres.attila.zoltan@uni-eszterhazy.hu

weigandl1@duq.edu

Abstract: The phenomenon of fake news and media manipulation has always existed in human history, long before the invention of digital technology. However, never before in the history of mankind has it been possible to spread fake news so quickly, in such large quantities and to such large masses, as now, in the age of the internet and social media. In this paper we identified 31 recurring signs of fake news and phishing scams spreading on social media in Hungary, Romania and Slovakia, based on the content analysis of 866 screenshots of social media posts, internet articles, phishing emails and SMS messages from these 3 countries. The most common group of signs are signs of provoking emotions. The second largest group of indicators include the characteristics of the media publishing the news. The third major category is the visual appearance and wording of the news. The fourth group of recurring signs refers to the original source of the news. The fifth group of indicators is the lack of reliable and/or official media coverage of the story. The elements of the sixth group of signs are the photoshopped and re-framed 'proof' images and videos that appear in the news. The seventh, and final group, of indicators refers to the prior beliefs and biases of the target audience. Provoking emotions, and thereby turning off the recipient's critical thinking, is the most common sign of fake news, scams and other hoaxes. Consequently, there is a great need for a high level of critical thinking and information literacy regarding social media contents on the part of the recipient. Our research was based on a fake news database collected in the framework of an international Erasmus+ project called "Media Detective". The aim of the project is to develop media literacy training modules for teachers and youth workers that could be used in school settings.

Keywords: fake news, social media, Hungary, Romania, Slovakia

1. Definition of fake news

The phenomenon of manipulation and fake news existed in media long before the invention of digital technology. There are numerous examples in print media. For example, Tengely (2001) analyzed the content of contemporary press reports on the 1913 sword duel between two Hungarian prime ministers (István Tisza and Mihály Károlyi). The researcher analyzed the extent to which newspapers of different political parties distorted reality. Thus, we are really dealing with a historical phenomenon when we discuss fake news and media manipulation. Yet, there is an almost endless debate in contemporary international literature on the definition of what we call nowadays "fake news". The controversy is not unfounded, as the term itself is difficult to grasp and interpret with a single clear definition. Allcott and Gentzkow define fake news as "*news articles that are intentionally and verifiably false, and could mislead readers*" (Allcott and Gentzkow, 2017:213). Veszelszki (2017) adopts this definition for a broader understanding of fake news, but narrows the definition to emphasize the pursuit of financial gain and create the appearance of credible journalism. She includes various internet scams (spamming, phishing, hoax, clickbait), news parody, and propaganda among the concepts related to fake news. She also discusses urban legends as a subtype of fake news. Royster then defines fake news as "*inaccurate articles published online in the guise of a genuine news story that are created without any concern as to their truth or falsity*." (Royster, 2017:276). Klein and Wueller also define fake news as "*the online publication of intentionally or knowingly false statements of fact*." (Klein and Wueller, 2017:6). They do not limit it to articles—fake news can also be video or graphics. Additionally, Pennycook and Rand consider the online publishing platform as one of the most important aspects. They define fake news as "*news content published on the internet that aesthetically resembles actual legitimate mainstream news content, but that is fabricated or extremely inaccurate. Also referred to as false, junk, or fabricated news*." (Pennycook and Rand, 2021:389). Disinformation, misinformation, hyper-aggrandized news and "yellow journalism" are also mentioned as related categories. Researchers Baptista and Gradim wanted to find a clear definition of fake news, so they conducted a content analysis of academic articles published on the topic between 2016 and 2020. They found 41 scientific articles in the Web of Science database and 22 in the Scopus database that attempted to provide a precise definition of fake news. Based on their analysis, fake news is: "*a type of online disinformation (1), with (2) misleading and/or false statements that may or may not be associated with real events, (3) intentionally created to mislead and/or manipulate a public (4) specific or imagined, (5) through the appearance of a news format with an opportunistic*

structure (title, image, content) to attract the reader's attention, in order to obtain more clicks and shares and, therefore, greater advertising revenue and/or ideological gain". (Baptista and Gradim, 2022:640).

Thus, based on our literature review above, we can summarize the concept of current digital "fake news" as follows: 1. fake information that is created on a digital device and published on an online platform; 2. in the form of a news article and/or image and/or video; 3. usually related to well-known people, public figures or controversial current events that are of high interest; 4. the news presents itself as reliable though in actuality it is fake; 5. it appears on dubious websites/social media sites with unverified backgrounds, without a classical editorial team behind it that adheres to ethical journalism rules and without a detailed imprint; 6. the author is intentional, i.e. he/she does not spread the lie by accident or out of ignorance/negligence, but knowingly, most often for political/ideological or commercial gain; 7. the main distribution platform is social media, where users who spread the fake news are not necessarily aware that they are spreading fake news.

2. Phishing and scams

Phishing, in its simplest definition, is data fishing, where fraudsters trick users into providing various personal details in order to abuse them— most often to steal their money. Liu et al. (2011) describe phishing as an ongoing "semantic attack" that tricks victims into sharing sensitive information unintentionally. Saberi et al. (2007) distinguish between "phishing" and "scam". "Phishing" is the process of data theft itself, the tool of which is "scam". They describe phishing as a form of "identity theft", in which fraudsters try to trick the victim into providing confidential information such as online bank account details. A typical process is when the attacker deceives the victim with a spoofed email, which is the "scam". According to Chaudhry et al. phishing "*is a form of cybercrime that aims to deceive users into providing personal and/or financial information, or to send money directly to the attacker. A phishing attack is generally initiated via some form of message, which includes a link to a deceptive domain name which appears to be a legitimate site but is actually controlled by the attacker.*" (Chaudhry et al, 2016:247). Wash provides a more general definition of email phishing when he writes: "*a phishing email is an email that pretends to be something that it is not, in order to get its recipient to take an action that they otherwise wouldn't do*" (Wash, 2020:1). Baykara and Gürel also consider phishing to be a form of cyber-crime, where the attacker poses as a real person or institution who "*sends malicious links or attachments through phishing e-mails that can perform various functions, including capturing the login credentials or account information of the victim. These e-mails harm victims because of money loss and identity theft.*" (Baykara and Gürel, 2018:1). However, according to Hong (2012) phishing can happen not only via email, but also via SMS, chat, voice messages, multiplayer online games, and various social media platforms. To summarize, in a phishing attack, the attacker(s) collect sensitive customer data (e.g. user account login credentials, credit/debit card numbers, etc.) via spoofed emails or fake websites (Basit et al, 2021).

3. About this research

In our modern digital environment, there is an increasing need to develop critical thinking skills towards media content in order to recognize fake news and other scams. Schools and teachers have a major role to play in developing these skills among students. Nowadays, as Molnár et al (2017) mention, almost all students have smart devices, which can also be used in education for pedagogical purposes, depending on the individual creativity of teachers. Smart devices and other digital equipment can be important tools for developing critical skills for assessing media content and supporting visual learning (Molnár and Szűts, 2015), as scams and fake news often carry visual signs. Digital pedagogy can be an excellent tool to develop a critical attitude towards fake news and phishing scams, since on the one hand, scams are also spread in such digital environments, and on the other hand, as Szűts (2020) writes, digital pedagogy can help students to develop their knowledge in a wide range of ways, building on their creativity, by using digital tools they use in their everyday lives (Szűts, 2020). Digital education is also possible and applicable for adults. Learning circles organized through online tools allow the development of a wide range of skills (Simándi, 2020), including a critical attitude towards media content. There are also opportunities for multi-disciplinary skills development even among the elderly through learning circles (Simándi and Oszláncki, 2018). Improving media literacy among youth communities is the aim of the "Media Detective" project, which produced a fake news database as the basis for this research. In this paper, we summarize the recurring signs of fake news and other scams spreading on social media by analyzing 866 screenshots of social media posts, internet articles, phishing emails. and SMS messages from Hungary, Romania and Slovakia. This content analysis is based on an international media-literacy project called "Media Detective for Young People: Recognizing and Handling Fake News and Media Manipulation" carried out in Hungary, Romania and Slovakia, funded by the Erasmus+ program in 2022 and 2023. One of the main goals of this project is to develop teaching materials that will enable teachers to show Hungarian, Romanian, and Slovakian students how to recognize fake news and phishing scams.

4. The recurring signs of fake news and phishing

In our content analysis, we were able to classify the signs of fake news and phishing scams into seven main categories, as follows:

4.1 Emotional manipulation: stimulating emotions

Perhaps the most common sign of fake news and phishing scams is that they evoke strong emotions. This is a way of "turning off" users' critical thinking. Montesi (2021) also points to this when he writes that in situations of uncertainty and high emotions, the spread of fake news increases dramatically (Montesi, 2021). According to Albrecht et al. (2010) when news is about us, it affects us on an especially high level, such that we will likely react emotionally. But when it is about "other" [non-personal] things, more physically and/or psychologically distant, we tend to think analytically. The signs of emotion-based manipulation are summarized in the table below:

Table 1: Recurring signs of fake news and phishing scams based on emotional manipulation

If something is too outrageous and/or scares us	For example, an SMS that your credit card has been blocked. Or an outrageous statement a politician never said. Or an alarm about a non-existent threat. Or a phishing email in the name of the national tax office scaring us into opening an attached file (which actually contains a virus or spyware).
When the message sets a deadline and urges us to do something	For example, a phishing SMS sent on behalf of Netflix telling you that you must provide your details within 24 hours to a suspicious link or your account will be suspended.
When the news is "too good to be true"	The fake news that all the members of the Croatian national football team donated the proceeds from the World Cup to charity for children in need has been all over the Hungarian and Romanian press.
If the news is extremely tear-jerking, touching or pleading for help	Social media posts of seriously ill children (mainly cancer patients) pleading for help. You can help sick children by liking and sharing. Such posts are also appearing on social media sites in Hungary, Romania, and Slovakia.
If a prize is too tempting and too easy to get	Offering unrealistically high value prizes (e.g. expensive cars, caravans, furniture, high-value shopping vouchers, iPhones etc.) that can be won for a like and share. In reality, there is never a draw, the aim is to increase the number of followers extremely quickly.

(Source: our own research results)

4.2 The medium that reports the news

The other large group of indicators of fake news and phishing scams includes the characteristics of the media publishing the news. These are the signs of suspicious media outlets:

Table 2: Recurring signs of fake news and phishing scams based on the medium that reports the news

If the link or the social media profile has an unknown and/or frivolous name	We don't often hear about the "NewsHat" website or the "Moneybasket" Hungarian Facebook page. Not by accident, as these are fake news sites. Always be suspicious if the news is not from a well-known, reliable, long-established news outlet.
If the URL does not have a country-specific ending	If the link does not end in ".ro" in Romania, ".hu" in Hungary or ".sk" in Slovakia, it is always suspicious. In the case of websites in Hungary, most of the fake news sites are not ".hu", but ".net", ".eu", ".com", ".me" etc. The reason is that the rules for creating ".hu" sites are stricter, more data must be provided, they are run from Hungarian servers, so they are easier for the Hungarian authorities to check and track down. For sites with other extensions, the rules are less strict, which is why they are so popular with fraudsters.
If the URL reminds you of a familiar/trustful company name, but the ending is unusual	For example: the official website of the supermarket chain Tesco in Hungary is "tesco.hu". The website "tesco-hu.com" is created by fraudsters. The official website of RTL television in Hungary is "rtl.hu", and fraudsters have created a website at "rtl-klub.me".
Copied websites - but with a different URL	A common form of fraud in all three countries is for phishing scammers to copy the official website of a bank or a trusted news site. At a glance, it looks just like the original, official site. However, the URL debunks the scam, because it immediately shows that you are not on the official site.
If there is no "about us" or "contact us" section of the website or it is incomplete	The "about us" section on the websites of reliable news sources contains details of the editorial office: its physical address, telephone number, online contact details, staff names, titles, personal contact details— in many cases even their photo. If there is no "contact us" or "about us" menu item with detailed information, it is a sign of unreliable sources.

Features of the social media profile	For example: If the followers of the social media profile also consist of suspicious/famous sites. Or if the social media profile has only just been created and is already giving away big prizes.
--------------------------------------	---

(Source: our own research results)

4.3 The visual appearance and wording of the news

The next major category is the visual appearance and wording of the news. That is, how it is written, what grammatical errors it contains, what design it has. The following table summarizes the external signs of fake news and phishing scams:

Table 3: Recurring signs of fake news and phishing scams based on the visual appearance and wording of the news

Unusual formatting: misuse of small and capital letters, unusual punctuation, too long of a title	In almost all cases, the unusual formatting marks are indicative of fake news. Examples include titles consisting of 3-4-5 lines. A professional journalist would never give a title without a headline. However, these signs are increasingly disappearing.
Spelling mistakes, punctuation errors, incorrect wording	Some of these errors are due to the fact that international scams do not use professional translation software to produce country-specific translations. These signs are also on the decline.
Mocking/sarcastic tone	In the case of heavily partisan, biased news, and fake news, a sarcastic and mocking style is often used.
Words and adjectives referring to spirituality, miracles	For example, the Hungarian Facebook page "Wonderful World", which posted a fake news story about rain in Brazil, which put out forest fires that were raging at the time. Or the Facebook post about the miraculous spiritual journey of bees, which is actually based on a photo stolen from a case in England.
"Amen" or "Done" comments lining up	"Amen" comments are often found under fake posts and fictional touching stories that collect likes, while "Done" comments are often found under fake sweepstakes.
Ask to share/agree/like	A recurring sign of fake news is that it asks to be shared. Professional journalists never ask to be shared, even in cases of missing persons. Be immediately suspicious if you come across a post requesting a share.
Two pictures side by side (in Hungarian cases)	In the case of Hungarian fake news, a recurring feature was the appearance of two (or sometimes three) pictures side by side in the post. This was very rarely seen in Romania and Slovakia.

(Source: our own research results)

4.4 The origin of the information itself

The next group of recurring signs of fake news and phishing scams refers to the original source of the news. Here, we are not referring to the medium or social media profile that shared the news, but to the original source of the information. The following table summarizes suspicious signs about the original source of the news that point to fake news or phishing scams:

Table 4: Recurring signs of fake news and phishing scams based on the origin of the information itself

If the origin is incorrect or missing, or if it just "came from somewhere"	For example: when a friend forwards you an SMS warning you about a rise in petrol prices, but it is unknown where this information originated. Or you receive a Messenger text warning of a weather threat, but you don't know who is the source of this information and the weather service it refers to doesn't actually exist.
If you were selected out of the blue and won something (Instagram, email, SMS)	A common trick used by phishing scammers is to inform you that you have suddenly won something. Often on Instagram, we receive tagging in fake posts announcing a win.
Unusual activities, messages and posts from your friends' social media profiles	Suddenly, from a friend who never writes, send us a link out of the blue and asking if we are in this video. It's suspicious when one of our friends starts suggesting dream-like bitcoin investment, who has never done anything like this before. Or shares a post with many other friends tagged. It's also possible that our friend's social media page has been hacked and the message is coming from scammers.
Vague reference to authorities without verifiable specifics	A common trick among fake news authors is to refer to well-known organizations, authorities, official bodies, governments (e.g. NASA). However, there is no evidence of it on the official pages of these organizations. If there is a link in the fake post, it is broken or points to an unofficial/fake site.

(Source: our own research results)

4.5 Lack of reliable and/or official media coverage

The next group of recurring signs that indicate fake news are those that indicate sensational and/or shocking news and revealed secrets that appear exclusively on social media and/or unreliable websites. Different media outlets may be reliable for everyone, but generally speaking, if a sensational news story is not reported by a major, well-known, long-established news outlet with professional journalists or official sources, we should be suspicious. The following signs may indicate this phenomenon:

Table 5: Recurring signs of fake news and phishing scams based on the lack of reliable/mainstream and/or official media coverage

Although the news is super-sensational and/or it affects many people, it is not reported by reliable international news sources, and/or official authorities	For example, when a private Facebook profile announces that after 112 years it has snowed again in Cairo and the pyramids are covered in white. If it had, it would have been reported by the entire international mainstream media. Or a fake news story that people born between 1951 and 1989 are receiving substantial discounts from a Romanian bank– but there is nothing about it on the bank's official website. Or a Facebook post about kidnapers in a village, while the police know nothing about it.
If the news promises to reveal secrets, confidential or inside information	When a post or article or message promises to reveal insider, confidential, secret information, you should always suspect that you are being scammed.
If a layman shows you some really sensational/amazing "lifehack" – especially prevalent in videos and on TikTok	One has to be very careful with videos and challenges on TikTok, as they can often cause damage, injury and accidents. Before anyone tries any dangerous chemical or physical processes at home, they should ask a professional. There are also lots of useful videos, many of them harmless, but some of them can be dangerous. Only trust serious, professional, official sources and verifiably credible professionals, or if the layman in the video is referring to serious sources that actually exist.

(Source: our own research results)

4.6 The photos and videos used in the posts: stolen, photoshopped and/or re-framed images

The next group of signs of fake news and hoaxes are 'proof' images and videos that appear in the news. In most cases, these are images and videos stolen from elsewhere, photos and videos that have been edited, or photos and videos that have been re-framed. These signals are summarized in the table below:

Table 6: Recurring signs of fake news and phishing scams based on the photos used

Photoshopped pictures	For example, a photoshopped photo was circulated on international social media showing Hungarian police officers using herds of swine to keep Muslim migrants away from the border. Among Muslims, pigs are considered unclean animals and are therefore shunned. However, the original photo was taken in the Philippines after a typhoon passed.
Re-framed images	Real photos, originally published in a different context. For example, "photo evidence" circulated on Hungarian and Romanian social network sites showing a lot of useless electric cars in Paris because the batteries are too expensive to replace. But the original photo was taken in China, which had nothing to do with expensive batteries.
Stolen photos used for emotional click-bait	Usually emotionally triggering photos of unfortunate and/or elderly people and/or sick or missing children, natural disasters, extraordinary phenomena (e.g.: stolen photos of special works of art). Their publishers call for sympathy, help, sharing and likes. Google Lens shows what other sites have used the image.
Re-framed videos	Videos that were originally made in a completely different place, at a different time, in a different context, possibly from video games. For example, a video allegedly showing Ukrainians pretending to be dead under body bags, as one of the "dead" emerges out from under the bag. The video was originally taken years earlier in Vienna during a demonstration against climate policy.

(Source: our own research results)

4.7 Building on the prior beliefs and biases of the target audience

When a news item tells us exactly what we want to hear, we should immediately become suspicious. This can also be a sign that we are dealing with fake news. Creators of fake news know well what their target audience wants to hear, and they say exactly that. They are exploiting our own preconceived beliefs, political, scientific and other views.

Table 7: Recurring signs of fake news and phishing scams based on the prior beliefs and biases of the target audience

When something suspiciously matches our prior expectations and stereotypes	Even the mainstream media reported the fake news that a Russian tank had been stolen by Ukrainian Roma. Many people have the stereotype that Roma are tricky people. This led many to believe that they had actually stolen a Russian tank. In reality, all we have seen is a re-framed video, originally showing Ukrainians towing a stalled combat vehicle with a tractor. Another fake news story is that Elon Musk spent Halloween in Dracula's castle in Transylvania. The super-rich and eclectic Elon Musk can be imagined deciding to spend Halloween in one of "Count Dracula's" castles. It fits in with the image of him.
When something fits perfectly with our political and other views/biases	For example, a fake Facebook post showing the results of an unspecified "scientific experiment" on how harmful microwaves are. Those who already think microwaves are harmful will believe the news even if every detail of the post tells them that it is about an experiment that never happened.

(Source: our own research results)

5. Summary

We found few differences between the fake news posts and internet scams we analyzed in Hungary, Romania, and Slovakia. Accordingly, it is worth watching for these aforementioned signs of fake news, as they were observed in all three countries. This is no small task. As well, we must be able to step back from our own preconceptions, our own worldview. In relying on them, we can easily fall victim to scams. In total, we were able to identify seven signs that rely on evoking emotions and prior convictions of the receiver. In addition to these, it may be easier to recognize other signs that come either from the source of the news, the medium that published the news, or from the images/videos presented. In this study, we identified a total of 31 signs of fake news and other scams in 7 categories. It is important that a fake news post or phishing scam usually involves several contemporaneous signs. Sometimes, it is not always possible to determine for sure whether news is fake or real based on a single sign. Several factors must always be carefully weighed. A “healthy” level of suspicion is needed, because it is also dangerous not believing in any media. For this reason, it is also very important to know what details to look out for to determine whether the news or the SMS or e-mail you receive is real. Some of these signs are disappearing (e.g. spelling mistakes, bad wording) because, as artificial intelligence develops, scams are becoming more sophisticated and harder to detect. Deepfake videos also fall into this category. This makes it essential to develop media awareness and heighten the critical faculties of the public.

References:

- Albrecht, K., Volz, K.G., Sutter, M., Laibson, D.I. and Von Cramon, D.Y. (2010) “What is for me is not for you: brain correlates of intertemporal choice for self and other”, [online], *Social Cognitive and Affective Neuro Science*. Vol. 6. No. 2. pp. 218–225.
https://scholar.harvard.edu/sites/scholar.harvard.edu/files/laibson/files/what_is_for_me_is_not_for_you_brain_correlates_of_intertemporal_choice_for_self_and_other.pdf
- Baykara, M. and Gürel, Z.Z. (2018) “Detection of phishing attacks”, [online], *6th International Symposium on Digital Forensic and Security (ISDFS)*, Antalya, Turkey, pp. 1-5. <https://ieeexplore.ieee.org/abstract/document/8355389>
- Baptista, J.P. and Gradim, A.G. (2022) *A Working Definition of Fake News*. [online], <https://www.mdpi.com/2673-8392/2/1/43>
- Basit, A., Zafar, M., Liu, X., Javed, A.R., Jalil, Z. and Kifayat, K. (2021) “A comprehensive survey of AI-enabled phishing attacks detection techniques” [online], *Telecommunication Systems* Vol. 76. 2021. pp. 139–154.
<https://link.springer.com/article/10.1007/s11235-020-00733-2>
- Chaudhry, J., Chaudhry, S.A. and Rittenhouse, R.G. (2016) “Phishing Attacks and Defenses”, [online], *International Journal of Security and Its Applications* Vol. 10, No. 1 pp.247-256. <http://dx.doi.org/10.14257/ijisa.2016.10.1.23>
- Hong, J. (2012) “The state of phishing attacks”, [online], *Communications of the ACM* Vol. 55. No. 101. pp 74–81.
<https://doi.org/10.1145/2063176.2063197>
- Klein, D.O. and Wueller, J.R. (2017) “Fake News: A Legal Perspective”, [online], *Journal of Internet Law*. Vol.20.No.10. pp.5-13.
<https://deliverypdf.ssrn.com/delivery.php?ID=348094069068099084119082124113004024022087061054024018026093004006065028028031105106002063005047108007015085105079086070118021046053082082007103072086071102015122030095085017074113113089083084111069105078096121014117095085004102088103081088013029101119&EXT=pdf&INDEX=TRUE>
- Molnár, Gy. and Szűts Z. (2015) “Visual Learning - Picture and Memory in Virtual Worlds” In: Benedek, A. and Nyíri, K. (eds) *Beyond Words : Pictures, Parables, Paradoxes* Frankfurt, Germany : Peter Lang Verlag. pp. 153-161.

- Molnár, Gy., Sik, T.D., and Szűts, Z. (2017) "IKT alapú mobilkommunikációs eszközök és alkalmazások módszertani lehetőségei a felsőoktatásban" In: Mrázik, J. (ed) *A tanulás új útjai*, Budapest, Hungary, Magyar Nevelés- és Oktatáskutatók Egyesülete (HERA) pp. 285-297.
- Montesi, M. (2021) "Understanding fake news during the Covid-19 health crisis from the perspective of information behaviour: The case of Spain", [online], *Journal of Librarianship and Information Science* Vol. 53. No.3. pp. 454–465 <https://journals.sagepub.com/doi/pdf/10.1177/0961000620949653>
- Liu, G., Xiang, G., Pendleton, B.A., Hong, J.I. and Liu, W. (2011) "Smartening the Crowds: Computational Techniques for Improving Human Verification to Fight Phishing Scams". [online], Symposium On Usable Privacy and Security (SOUPS) 2011, July 20-22, Pittsburgh, PA, USA. <https://dl.acm.org/doi/abs/10.1145/2078827.2078838>
- Pennycook, G, and Rand, D.G. (2021) "The Psychology of Fake News", [online], *Trends in Cognitive Sciences*, Vol. 25, No. 5. pp. 388-402. <https://www.sciencedirect.com/science/article/pii/S1364661321000516>
- Saberi, A., Vahidi, M. and Bidgoli, M.B. (2007) "Learn To Detect Phishing Scams Using Learning and Ensemble Methods", [online], 2007 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology – Workshops <https://ieeexplore.ieee.org/abstract/document/4427596>
- Simándi, Sz. (2019) *Közösségi tanulás felnőttkorban Tanulókörök az élethosszig tartó tanulás folyamatában*. Budapest, Akadémiai Kiadó.
- Simándi, Sz. – Oszlanczi, T. (2018): "Időskori tanulás - közösségi művelődés". In: Fodorné, T. K. (ed): *Social and economic benefits of university lifelong learning: research, development and innovation*. Debrecen, Hungary: MELLearn Felsőoktatási Hálózat az életén át tartó tanulásért Egyesület pp. 380-384.
- Szűts, Z. (2020) "A digitális pedagógia jelenségei és megnyilvánulási formái", [online], *Új Pedagógiai Szemle*, Vol. 70 No.5-6. pp. 14-36. <http://upszonline.hu/index.php?article=700506007>
- Tengely, A. (2001) "Tisza István 1913. januári politikai párbajai" In: Mátyás, B. (ed) *Grastyán Endre Szakkollégium tanulmánykötet 2*. Pécs, Pécsi Tudományegyetem Grastyán Endre Szakkollégium, pp. 239-276.
- Wash, R. (2020) "How Experts Detect Phishing Scam Emails", [online], *Proceedings of the ACM on Human-Computer Interaction*, Vol. 4, No. CSCW, pp. 1-28. <https://doi.org/10.1145/3415231>