THREATS AND DANGERS IN SOCIAL MEDIA.

Ijtimoiy fanlar kafedrasi o'qituvchilari
Ahmedov Abdulhay Toshto'xtayevich,
Jabborova Sayyoraxon Muxammadqobilovna
Andijon davlat pedagogika instuti ona tili adabiyot
ta'lim yo'nalishi 1-bosqch talabalari
Sobirova Dilorom Muzaffarjon qizi
Mamajonova Muslima Botirjon qizi

Annotatsiya: Ushbu maqola ijtimoiy tarmoqlarda yuzaga keladigan tahdidlar va xavf-xatarlar haqida kengroq ma'lumot beradi. Maqolada, shaxsiy ma'lumotlarning o'g'irlanishi, kiberhujumlar, kiberbullying, shuningdek, psixologik xavflar va feyk xabarlarga ishonish kabi muammolarni tahlil qilgan holda, foydalanuvchilarni bu xavflardan qanday himoya qilish mumkinligi haqida amaliy tavsiyalar keltirilgan. Ijtimoiy tarmoqlardan xavfsiz foydalanish uchun foydalanuvchilar maxfiylikni saqlash, xavfsiz internetni ishlatish va psixologik yordam olish kabi muhim choralarni ko'rishlari kerakligini ta'kidlaydi.

Abstract: This article provides more information about the threats and dangers that occur in social media. The article analyzes issues such as identity theft, cyberattacks, cyberbullying, as well as psychological risks and trusting fake news, and provides practical recommendations on how to protect users from these risks. In order to use social media safely, it emphasizes that users should take important steps such as maintaining privacy, using a safe internet, and seeking psychological support.

Абстрактный: В этой статье представлена дополнительная информация об угрозах и опасностях, возникающих в социальных сетях. В статье анализируются такие проблемы, как кража личных данных, кибератаки, кибербуллинг, а также психологические риски и доверие к фейковым новостям, а также даются практические рекомендации, как защитить пользователей от этих рисков. В нем подчеркивается, что для безопасного использования социальных сетей пользователи должны предпринять важные шаги, такие как сохранение конфиденциальности, использование безопасного Интернета и обращение за психологической поддержкой.

Kalit so’zlar: Ijtimoiymedia, Onlaynxavfsizlik, Internettahdidlari, Shaxsiyma'lumotlarnihimoyaqilish, Kiberxavfsizlik, Onlaynbulling,Aloqaxavfi, Internetdatahdidlar, Xavflicontent, Soxtaxabarlar (fakenews), Kiberjinoyatchilik, Shaxsiyhayotnibuzish, Ijtimoiymediaxavflari, Onlaynhiyla-nayranglar, Doxilbo'lishvakirishcheklovlari,Ma'lumotlarnio'g'irlash, Internetdastressvazo'ravonlik, Ijtimoiymediavapsixologikta'sir

Keywords: Social Media, Online Safety, Internet Threats, Privacy Protection, Cyber Security, Online Bullying, Communication Risk, Threats on the Internet, Dangerous Content, Fake News, Cybercrime, Violation of Privacy, Social Media Risks, Online Scams, Login and Access Restrictions, Data Theft, Stress and Violence on the Internet, Social Media and Psychological Impact

Ключевые слова: социальные сети, онлайн-безопасность, интернет-угрозы, защита конфиденциальности, кибербезопасность, онлайн-запугивание, коммуникационный риск, угрозы в Интернете, опасный контент, фейковые новости, киберпреступность, нарушение конфиденциальности, риски социальных сетей, онлайн-мошенничество, доступ. и ограничения доступа, кража данны

Threats and Risks in Social Networks Social networks have become an integral part of personal and professional life these days. However, although these platforms are not only convenient tools for communication and information sharing, there are also many threats and dangers associated with them

Risks in Social Networks: Threats and Risks in Social Networks Social networks have become an integral part of personal and professional life these days. However, although these platforms are not only convenient tools for communication and information sharing, there are also many threats and dangers associated with them. Along with the benefits of social networks for users, their dangers are also serious enough

Risks in Social Networks: Theft of Personal Information Many social media users share their personal information (phone number, address, passport details) on social platforms. Sometimes such information is inadvertently or carelessly released to the public. Such information can be stolen by malicious individuals and used for fraud or other crimes. For example, there has been an increase in attacks that trick users through "surveys" and "surveys" used in social networks. To protect themselves from such risks, users should make their profile private and set their privacy settings properly.

Cyber Attacks and Online Hacking Cyber attacks carried out through social networks are increasing. Hackers can attack by hacking social network accounts, stealing user's personal information or installing malware. Such attacks are often carried out in the form of phishing (theft of accounts through fake links) or installation of malicious software (virus, trojan). To protect against these risks, users are advised to set up two-factor authentication (2FA), use secure passwords, and use antivirus software.

Persistent Surveillance and Threats to Privacy: Online activity of users in social networks is constantly monitored.. To reduce such risk, users should set privacy settings correctly and carefully study the information policy of the platform.

such information is inadvertently or carelessly released to the public. Such information can be stolen by malicious i ideal" lives and feel low self-esteem or hate their own lives. The "good" life that is shown on social networks only reflects the most wonderful moments, but it does not really To protect themselv es from such risks, users should make their profile private and set their privacy settings properly. To protect against these risks, users are advised to set up two-factor authentication (2FA), use secure passwords, and use antivirus software. Persistent Surveillance and Threats to Privacy Online activity of users in social networks is constantly monitored. Platforms analyze the behavior and interests of users and present advertisements and other computer products.. To reduce such risk, users should set privacy settings correctly and carefully study the information policy of the platform. Cyberbullying (Online Harassment) Cyberbullying, that is, online bullying and harassment, is on the rise through social media. This is usually done by unknown persons or even close friends. Cyberbullying can cause many psychological problems, especially among young people. Insulting people in online discussions, intruding on their privacy or constantly harassing them can have a negative effect on a person's psyche[1]. To avoid such risks, users are advised to exercise caution in their online behavior and maintain respect in online and offline communication. Psychological Risks Loneliness and Psychological Effects Social networks connect many people with each other, but they can also cause loneliness and psychological difficulties in users. Users may view others' "ideal" lives and feel low self-esteem or hate their own lives. The "good" life that is shown on social networks only reflects

[1] Kaspersky Blog: https://www.kaspersky.com/blog/

the most wonderful moments, but it does not really represent the whole truth. As a result, users may feel bad, develop depression and other psychological disorders.

Therefore, it is important to maintain a balance between the right approach to social networks and self-evaluation.

Trusting Fake News

Fake messages (false information) are often distributed on social networks. These messages may distort political or social events, mislead people, or increase social fear. Spreading fake news is done not only for political manipulation but also for personal gain. Users must verify each message, identify sources, and make informed decisions.

Ways of Protection from Dangers Maintain Privacy Share personal information on social media only with people you trust. Make your profile settings private, control who can see them, and avoid making unnecessary information public. Safe Internet Use Vigilance is necessary to identify and avoid online risks. Avoid clicking on links from unknown sources, stay on secure websites, and use anti-virus software. Also, installing two-factor authentication (2FA) systems and using strong passwords can help ensure security. Psychological and social support If you or someone is under psychological pressure on social networks, it is necessary to consult a specialist or psychologist. It is also important to maintain mutual respect and caution, and ask friends and family for help.

Social networks have become an integral part of our daily lives, but there are also risks associated with them. Users need to exercise caution, protect their privacy and be educated about safe internet usage to protect themselves from these threats..This article provides a comprehensive analysis of the dangers of social media and provides users with practical advice on how to avoid them. Social networks are platforms created for communication and information exchange between people over the Internet (for example, Facebook, Instagram, Twitter, TikTok).

Threat - Actions taken with the purpose of harming, attacking or endangering a person or organization.

Cyberattack – The process of illegally accessing computer systems or using malicious software to disable the system or steal data.

Phishing - An online scam that uses fake websites or emails to steal personal information (such as passwords or credit card numbers) from users.

Privacy – Protecting personal information and making it available only to certain individuals or groups. Antivirus software – Software used to detect and remove malicious software (viruses, trojans, spyware) from computers or mobile devices. Two-Factor Authentication (2FA) – A system that requires an additional security step beyond a password to make a user's account more secure. For example, entering a code sent by phone.Psychological impact – the effect of activity on social networks and the attitude towards the content of others on the user's mental state, self-esteem and psychological health. Online Security – Ensuring that personal data and systems are protected online, avoiding malware and fraud. When writing an article about social media threats and risks, you can consider the following points:

Dangers in social networks: Theft of Personal Information: Personal information (phone number, address, passwords) can be stolen or misused through social media.

Cyber Attacks and Online Hacking: Hackers hacking social media accounts or harvesting users' personal information.

Persistent Surveillance and Threats to Privacy: Monitoring of users' online activities, invasion of privacy and violation of privacy.

Cyberbullying (online harassment): Insulting, harassing, or harassing users on online platforms.

Psychological risk :Loneliness and psychological effects: Constant competition on social media and seeing others' "ideal" lives can lead to personal dissatisfaction and low self-esteem. Believing in fake news: Incorrect or false information (fake news) spread on social networks can cause change, fear and danger.

Online Scams: Cases of scamming people, stealing money or tricking them into scams through social media.

How to protect yourself from dangers in social networks?

Protecting Personal Information: Make passwords strong, share personal information only with trusted individuals, and check privacy settings.Safe internet usage: Recognize online dangers, avoid clicking on links from unknown sources, and beware of fraud. Psychological and social support: Psychological support and counseling options for users who feel bad about themselves on the social network. Phishing attacks: Definition: Phishing is a method of fraud aimed at deceiving a user via e-mail, social networks or SMS. A malicious message usually contains a link or false information, asking the user to enter their personal or financial information. Example: A fraudster may pretend to be a bank employee and ask for credit card information from a customer.

Vishing and Smishing: Vishing: This is phishing done over the phone. Fraudsters pretend to be important people or organizations and force users to hand over their financial information. Smishing: Phishing via SMS. Scammers try to steal user's personal information by sending a fake link.

Ponzi and pyramid schemes: Ponzi scheme: This is a fraudulent scheme in which the funds of new investors are used to pay the returns of previously participating investors. The promises of profit are high, and the scheme can collapse when the flow of new entrants stops.

Investment scams: Cryptocurrency scams: Scammers trick people into investing in new crypto projects and then disappear with the funds. High Yield Investment Schemes (HYIP): Investors are promised high returns, but these schemes work mainly on new investors and disappear over time.

Romance Scams: Scams on online dating platforms: Fraudsters create false relationships and coerce people into providing financial assistance or revealing personal information.

Fake technical support schemes: Description: Scammers offer "technical support" by claiming that the user's computer is broken or infected with a virus. They try to extort money for identity theft or bad service.

Counterfeit electronic payments: Credit card and payment system fraud: Fraudsters hack into payment systems to make fraudulent payments or steal card information.

Incomplete or fake services: Scammers ask for upfront payment for services or products, but then don't deliver or deliver on what was promised.Below is more information about this type of scam:

Credit card fraud: Data theft: Fraudsters use phishing attacks, spyware, or fake websites to steal users' credit or debit card information.

Fraudulent purchases: Fraudsters purchase goods or services with stolen card information. Usually such purchases are made frequently or in large quantities.

Skimming method: data is copied from the card at ATMs or payment terminals using special equipment.

Fraud in the use of payment systems: Creating fake accounts: Fraudsters open fake electronic payment accounts and make illegal payments or transfers from other people's accounts. Reverse payment schemes: Once a payment is made, fraudsters attempt to unreasonably cancel or charge back it. For example, after using a service or product, they make a false claim for a refund. Fake payment messages: Via email or SMS: Fraudsters send users a message that says a payment has been made or is late, asking them to access a fake link to update their details or confirm the payment. Fraudulent payment acceptance: Fraudsters use the payment system to alert the user that an incorrect payment has been made and prompt them to pay again. Cheating through online games and apps: Virtual currency theft: Virtual currencies or bonuses used in games and mobile applications can be stolen by fraudsters or obtained through fraudulent payment methods. Fraud with in-app purchases: Children or inexperienced users are tricked into making high-priced purchases through fake apps.

Online shopping and money transfer scams: Discovery Fees: Fraudsters sell fake products or services on online trading platforms and accept an upfront payment, but then do not provide any products or services. Manipulation of money transfers: Fraudsters usually contact companies via email and pretend that they have changed their payment details, resulting in the money being transferred to the fraudster's account.

Social networks allow the rapid dissemination of information on a global scale at the same time, but the accuracy and reliability of this information is often not checked. False and manipulative messages, including fake news, spread rapidly on social networks. These messages can change people's views, create misconceptions and stereotypes. Especially on political and social issues, the spread of misinformation can have serious consequences, such as election manipulation, influencing public opinion, and causing riots[2].

Psychological Effects and Low Self-Esteem

In social networks, users often compare themselves with others, which can lead to psychological problems. For example, constantly comparing yourself to others' perfect lives, images, or successes can lead to low self-esteem, stress, depression, or anxiety. Young people, especially comparing themselves with others, strive to conform to the "ideal" image in social networks, which can lead to negative psychological states.

Online Harassment and Cyberbullying

In social networks, many people express not only their thoughts, but also their personalities. But some may use this space to insult or harass others. Cyberbullying (online harassment) remains a significant problem not only among young people, but also among adults.

Extremism and Terrorism: Social media can also be used to spread extremist ideas. Networks serve as a platform to introduce people to radical ideas, encourage

[2] Carnegie Endowment for International Peace

them to join a particular group, and even promote violence. Their activities are a serious threat in many countries, because these ideas spread quickly among the youth.

Ways to Overcome Risks: Strengthen privacy policies: Social networks should strengthen privacy policies to protect users' personal information. It is important to set up user security features to limit access to personal data and improve how users manage their data[3].

Educating young people about online safety: Self-defense should be taught to use social media safely and avoid online bullying. In this way, a broader understanding of the dangers of social media and how to overcome them can be created. The topic of extremism and terrorism is a serious threat to society and a source of global concern. Although these concepts are related to each other, each of them has its own characteristics and can be analyzed in different aspects. Below is important information about these topics. What is extremism?

Everyone should contribute to the maintenance of security and peace. At the same time, it is important to protect young people from the threats of radicalization through education and online awareness.

Adabiyotlar ro‘yxati:

Boyd, D. (2014). It's Complicated: The Social Lives of Networked Teens. Yale University Press.

Shirky, C. (2011). Cognitive Surplus: Creativity and Generosity in a Connected Age. Penguin Press.

Zuckerberg, M. (2017). The Social Network: The Impact of Social Media on Society. Harvard University Press.

Boyd, D. (2017). "Social Media and the Risk of Cyberbullying: Understanding and Addressing Online Harassment." Journal of Adolescent Health, 60(4), 459-463.

Livingstone, S., &Helsper, E. (2007). "Gradations in Digital Inclusion: Children, Young People, and the Digital Divide." New Media & Society, 9(4), 671-696.

O'Keeffe, G. S., & Clarke-Pearson, K. (2011). "The Impact of Social Media on Children, Adolescents, and Families." Pediatrics, 127(4), 800-804.

Andrejevic, M. (2004). "The Work of Watching: Interactive Audiences and the Exploitation of Online Privacy." Media, Culture & Society, 26(1), 19-36.

Cyberbullying Research Center. (2020). Cyberbullying Facts and Statistics.

European Commission. (2019). The Impact of Social Media on Youth: A Review of the Literature. European Commission Directorate-General for Communication Networks, Content and Technology.

[3] https://us.norton.com/