СОЦИАЛНИ МРЕЖИ В ИНТЕРНЕТ – УДОБСТВА И РИСКОВЕ

гл. ас. Илияна Чакърова

ПУ “Паисий Хилендарски” – филиал Смолян
pet_iliana@yahoo.com

***Резюме**: Ежедневното използване на социалните мрежи в Интернет ни дава възможност да извършим своевременно някои свои професионални дейности и контакти, преквалификации, финансови разплащания, лични online-срещи и други комуникации. В настоящата статия се разглеждат някои удобства, както и най-често срещаните опасности и рискове при работа в съществуващите социални мрежи.*

***Ключови думи**: online-обучение, интернет търговия, злоупотреба с лични данни.*

1. Увод

„Социалната мрежа е социална структура от индивиди (или организации), свързани в специфични за дадена мрежа типове отношения като приятелство (роднинство), идеи, виждания, традиции, финансови отношения, хипервръзки и други.“ [9]

*“**Социални мрежи*** – сайтове, които позволяват създаване на персонален профил, след което се осъществяват контакти, дискусии и споделяне на информация с приятели, семейство, колеги. Такива са известните социални мрежи ***Facebook***, ***Twitter***, ***MySpace***, ***YouTube***, ***Flickr***,…” ***Инвитро България*** и много други, и „Понастоящем социалните медии се развиват много динамично, нараства популярността им, появяват се приложения в нови области, следователно представеният списък не претендира за изчерпателност.“ [1]

Социалните мрежи според типа информация, която съдържат са:

- за ***online-обучение***;
- за ***интернет търговия***;
- за споделяне на ***контакти***;
- за споделяне на ***предпочитания*** (хипервръзки към интересни статии, новини, музика, видео, снимки и др.);
- за споделяне на ***авторско съдържание*** (картинки, музика, видео, статии и др.);
- за споделяне на ***лична информация***;
- за ***реклама*** на продукт или услуга, и др.

Социалните мрежи са добра възможност за хората, които искат да популяризират дейността си чрез фирмения си интернет сайт или блог, да привлекат бързо и безплатно определен брой посетители на страниците си. Мобилността на съвременния човек налага като необходимост (а в много случаи се явява и удобство) участието му в различни ***групи*** на избраните от него социалните мрежи.

Да не забравяме за възможната опасност, която носи фактът, че всяка социална мрежа, в която участваме, съхранява лична информация и доста данни за нас (име, адрес, телефон, e-mail, снимки, музика, текстове, лични съобщения и др.), които трябва да обработва съгласно условията, които ние сте приели при регистрацията си.

2. Удобства

2.1. ***Online-обучение:*** Ежедневното лавинообразно нарастване на научна информация изисква и съответстващ темп на нарастване ефективността на образователния процес. Тенденцията към информационна глобализация, благодарение на комуникационните възможности на създадените мултимедийни продукти, предполага и образованост, основана върху новите информационни технологии.

Начинът на представяне на информацията в повечето случаи е определящ за нейното възприемане и въздействие. Човешкият опит показва, че най-добрият начин за постигане на такъв ефект е допълването на това представяне с нагледни пособия. Представената по такъв начин информация е привлекателна и по-лесна за възприемане и осмисляне. Поради това мултимедията е широко използвана за създаване на съвременни обучаващи системи. Мултимедийната технология е много близка до човешките способности за възприемане на действителността и без съмнение представлява значителен напредък в областта на компютризираното представяне на информацията.

Нагледността стимулира актуалното online-обучение, насърчава логическото и практическо мислене при обучаваните. Въвежданият нов учебен материал чрез набор на ***3D***-модели, картинен, снимков, графичен (схеми, диаграми) и атрибутивен (таблици) материал, повишава любознателността, стимулира за активност при ученето, води до рефлексивно равнище на овладяване, дискутиране на неговото значение и търсене на приложението му в практиката. Чрез нагледното обучение, логическото и критическо мислене стимулират творчески процес на възприемане, осмисляне и усвояване на понятия и факти. Така сложният теоретичен материал става когнитивен (познаваем) за обучаваните и се затваря кръгът, в който те активно участват: ***възприемане – синтезиране – усвояване на информацията***.

“В някои развити страни свързват реформата в образованието с изисквания към завършващите основната му степен да са запознати с приложенията на споменатите (*по-горе*) блогове, подкасти, ***Wikipedia*** и ***Twitter*** като източници на информация и форми на комуникация …”. [1]

Online-обучението се провежда под ръководството на квалифициран инструктор и е максимално гъвкаво и адаптивно към:

- учащи хора, които едновременно с това и работят;
- майки, отглеждащи децата си;
- хора, живеещите в населени места, отдалечени от висшето училище /обучаващата организация;
- хора в неравностойно положение;
- групи със специфични образователни потребности.

Тази форма на обучение е равнопоставена на редовната форма по отношение на съдържанието на учебните планове и издаваната диплома от висшето училище. Чрез информационните технологии всеки обучаем получава постоянен достъп до качените на конкретен интернет сайт учебните материали, предварително разработени в съответствие с учебните програми, които отговарят на държавните образователни изисквания за придобиване на съответната степен за професионална квалификация.

След като се регистрира плащането на съответната такса, обучаваният получава право (чрез парола) за достъп до съществената част на образователния интернет сайт. Там са разположени всички учебни материали, изпитни тестове и задачи за упражнения, в съответствие с одобрените от МОМН учебни програми. От електронните учебни материали обучаемият се самоподготвя и чрез предвидените тестове се самооценява. Когато системата покаже за даден обучаем недостатъчна успеваемост (например под 50 %) при първо решаване на теста, той получава втори и последен шанс да се самоизпита.

Всеки тест се решава за определено време и ако обучаемият не може да се справи, системата автоматично прекъсва процеса на самоизпитване.

Методиката на online-обучението повишава активността на обучавания в собственото му учене и развитие, като го поставя на централно място в системата на обучение, за разлика от традиционните схеми, ориентирани към преподавателя. Методически насочваното саморазвитие, освен по-ефективен учебен процес и по-висока мотивация, формира и набор от качества за самостоятелно вземане на решение. За целта през целия курс обучаваният може да ползва подкрепата както на инструктора-наставник, така и на другите обучаеми – негови колеги, на обучена за целта администрация, на специално

изготвени учебни материали и други удобства на електронната платформа, която предоставя широки възможности за виртуална комуникация. [7]

2.2. ***Интернет търговия:*** През последните над десет години сме свидетели на т.нар. пазаруване по Интернет, т.е. стотици хиляди различни корпорации, големи и малки фирми, или просто хора, искащи да продадат нещо, предлагат online стоки и услуги. Този вид пазаруване наподобява на традиционната търговия – има същите елементи, същите участници и същата функционалност. [5]

При интернет търговията (***електронната търговия***) мястото за пазаруване се явява самият ***web-сайт***. Хората го посещават, разглеждат продуктите в каталог, само че електронен, харесват една или друга стока или услуга и когато решат да закупят нещо – те го правят. [2, 3]

Предимствата на този начин на пазаруване са няколко. Клиентите правят всичко това от вкъщи, без да ходят до магазина. Друго удобство за тях е, че не се налага да правят покупката си в рамките на работното време на магазина. За „продавача“ това означава постоянно работно време на неговия “магазин” и без допълнителен персонал „зад щанда“. Най-голямото удобство за търговеца е, че той не търси клиенти, а клиентите доста активно търсят него – търговеца. При тази ситуация търговците не молят клиента за покупка, а отговарят на неговите въпроси и се стараят да задоволят изискванията му. Това им дава голямо психологическо предимство и възможност за по-ефективна работа. [6]

При електронната търговия начинът за приемане на поръчки е попълване от клиентите на електронен формуляр (***online form***). Тази електронна бланка най-често изисква отбелязване на списък от желаните стоки с посочена цена и обща стойност, попълване на адресна информация за доставката и издаването на фактурата, както и начина на плащане и доставка. При традиционната търговия, клиентът плаща избраните стоки и може да ги вземе със себе си или да остави на продавача адрес, на който да му ги доставят. Така е и в електронния магазин – клиентът докато „пазарува“ си избира определени стоки, „купува ги“ чрез ***online form*** и напуска сайта. [10]

В България има изградена както законова база (***Закон за електронната търговия***, обн. – **ДВ**, бр. 82 от 2009 г., в сила от 16.10.2009 г.), така и проекти (напр. ***БАЕТ*** – Българската Асоциация за Електронна търговия [14]), свързани с развитието на електронната търговия, като се счита, че този тип отношения ще заемат все повече място, още повече като се има предвид, че в страната ни има много добре развито електронно банкиране, което е сред основните фактори за повишаване на електронните търговски отношения.

3. Рискове

Потенциалните рискове в съществуващите социални мрежи са свързани предимно с незаконното използване на лична информация от трети страни, които биха могли например да намерят начин да копират и обобщават потребителски профили, да събират лична финансова информация или да копират лична информация и да я използват за свои цели.

Като използваме социални мрежи, ние ставаме по-забележими, оттук и рискуваме да споделим неща от живота си с хора, с които не бихме желали да направим това в реалния живот.

3.1. *Термини, използвани като основна информация при работа в социални мрежи:*

Физическо лице – лице, до което се отнасят личните данни. Всички ние сме такива лица.

Лични данни – информация, свързана с даден човек (например имена, ЕГН, адрес, номер на банкова сметка, телефонен номер, e-mail, снимки и др.). Те се използват често в ежедневния живот, например при регистрация в обществен регистър, абониране за услуга (конвенционална или online), откриване на банкова сметка, постъпване в болнично заведение и др.

Чувствителни данни – специална категория лични данни, включваща информация за расов или етнически произход, политически идеи, религиозни или философски убеждения, членство в профсъюзи, както и данни, свързани със здравословното състояние и половия живот. Обработката на чувствителни данни е предмет на по-строги правила. Те могат да бъдат събирани на „opt-in“ принцип (трябва да дадете изрично съгласие за обработването на тези данни) и с тях трябва да се работи внимателно.

Данни за трафик – описват съобщителни дейности в обществените мрежи (например мобилни мрежи, интернет). Данните за трафика често се отнасят до маршрута, продължителността, времето или обема на комуникацията. Съхраняването и използването на подобни данни от интернет доставчиците на услуги е позволено само с цел изготвяне на сметки. При определени обстоятелства и в съответствие със законодателствата във всяка страна-членка на ЕС националните правоохранителни органи (обикновено полицията) могат да използват данните за трафика за разкриване на тежки престъпления.

Администратор на данни – лице или организация, което определя как се обработват данните (например използване, съхраняване или изтриване) и за какви цели, както в публичния, така и в частния сектор (например спортен клуб, администриращ данните за своите членове) и др.

Обработващ лични данни – лице, което обработва (например използва, съхранява или изтрива) лични данни от името на администратора.

Cookies („Бисквитки“) – скрита информация, която се обменя между потребител на интернет и web-сървър и се съхранява в компютъра на потребителя. Те често се използват за наблюдение на дейността на потребителите в интернет. Web-браузърите обикновено позволяват да се забрани използването на „бисквитки“ (Cookies) или те да се изтриват.

3.1. *Най-често срещаните опасности при работа в социални мрежи:*

Кражба на самоличност – отнася се до всички видове престъпления, при които някой незаконно придобива и използва личните данни на друго лице по начин, който включва измама или заблуда, обикновено с цел извличане на икономическа изгода. В повечето случаи кражбата на самоличност се извършва по метода на „фишинга“ (phishing) (метод за извършване на измама с кредитни карти, кражба на самоличност и/или обикновена кражба. „Фишинг“-атаките (phishing) използват електронни писма с фалшив подател и подправени web-сайтове, създадени с цел да подведат потребителите да разкрият лични финансови данни, като например номера на кредитни карти или потребителски имена и пароли за online-банкиране). [15, 16]

Кибер тормоз – агресивно тормозещо поведение, което е умишлено, повтаря се във времето и включва неуравновесено използване на интернет, мобилен телефон или друг вид цифрови технологии. Сред формите на тормоз са: изпращане на текстови съобщения, електронни писма или съобщения в реално време с обидно съдържание; публикуване на неприлични снимки или съобщения за други лица в блогове, профили или web-сайтове; разпространяване на слухове или лъжи за някой друг под чуждо име (откраднатa самоличност); телефонен тормоз; обидни устни съобщения.

Кибер преследване – заплашително поведение от страна на лице, което постоянно се свързва с жертвата с помощта на електронни средства (електронна поща, програма за съобщения в реално време и др.).

Радиочестотна идентификация (RFID) – технология, която позволява автоматична идентификация и улавяне на данни от разстояние чрез използване на радиочестоти. Тя позволява прикрепването с помощта на микрочип на уникален идентификатор и носител на информация, към всякакъв обект, животно или дори човек и прочитането на тази информация чрез безжично устройство. RFID може да застраши неприкосновеността на личния живот – технологията за радиочестотна идентификация може да се използва за събиране на информация, пряко или косвено свързана с дадено лице и поради това считана за лична информация. Радиочестотните идентификатори могат да съхраняват лични данни, като тези в паспортите или медицинските картони. Технологията може да се използва за издирване или проследяване на движението на хора или за изготвяне на профили на човешко поведение.

Спам – може да се дефинира като нежелани електронни съобщения, които се разпространяват в големи количества. Терминът „нежелателен“ е много субективен. Типичен пример са електронни или текстови съобщения със съдържание, свързано с продажба на фармацевтични продукти, съмнителни финансови транзакции, порнография и др. В повечето случаи спамът се разпространява с цел подвеждане на хората да похарчат пари за нещо или да разкрият лична информация с цел икономическа изгода за подбудителя.

Законодателството на ЕС защитава нашия личен живот и права върху интелектуална собственост, както и тези на хората, които споменаваме във нашия блог или в социална мрежа.

Законодателството на ЕС защитава личните данни на всички граждани и по правило гарантира, че личните ни данни не могат да бъдат използвани без нашето предварително съгласие [16]. (За допълнителна информация относно нашето национално законодателство, включително за прилагането на директивата за запазване на данни, може да се свържем с ***българския национален телекомуникационен регулатор*** [13] или ***българския национален орган за защита на данните*** [12]).

Но трябва да се има предвид, че винаги съществува риск от злоупотреба с нещата, които споделяме в интернет – профили, блогове, снимки, видео-клипове, съобщения.

При работа в социални мрежи е възможна защита на нашия личен живот и намаляване на риска от кражба на самоличността ни. Някои лесни начини за това са:

- внимателно да прочетем условията на социалната мрежа, към която искаме да се присъединим. Да решим кой е възможно да има достъп до профила ни и да определим на кого да дадем това право на достъп;
- преди да споделим в която и да е социална мрежа лични материали, внимателно да помислим какво разкриват те за нас. Тяхното публикуване може да има сериозни последици за нашия личен и професионален живот;
- да използваме настройките за неприкосновеност на личния ни живот, за да повишим нивото на online-защита, т.е. да ограничим достъпа до нашето online-съдържание, например като използваме настройките за неприкосновеност на сайта, да защитим с парола нашия блог, за да контролираме кой може да го разглежда, или да блокираме достъпа до нашите фотоалбуми в сайтове на социални мрежи за всички, освен за определен кръг от нашите приятели. Отговорността е наша. След като веднъж качим нещо или го изпратим на друг човек, то престава да бъде лично и други могат да го използват по начини, които не сме предвидили;
- внимателно да преглеждаме всяка реклама за „безплатни“ продукти. Да не бързаме и да не се поддаваме на изкушението веднага да отговорим на

привлекателната оферта, а да се уверим, че напълно разбираме всички нейни условия.

4. Заключение

За разлика от използването им в България, в чужбина социалните мрежи са обект на особено уважение от страна на повечето големи и известни корпорации, които търсят различни методи за да попадат на първа страница, особено на водещите социални мрежи. Тези корпорации отдавна са разбрали силата на социалните мрежи и ползите, които могат да извличат от тях.

Въпреки че социалните мрежи предоставят безплатно ценни възможности, за нашата безопасност в Интернет, ние трябва да знаем те как работят и какви рискове крие тяхното използване.

Добрата вест е, че днес повечето доставчици на online-услуги обръщат сериозно внимание на безопасността и сигурността на клиентите си при работа им в Интернет. [13, 15, 16]

Литература

1. Врагов Г., М. Станева, Р. Овчарова, Приложение на социалните медии в образованието, Сборник с доклади на международна конференция "Образованието в информационното общество", Пловдив, 2010.
2. Денев, Д., Педагогически основи на съвременните образователни технологии – (Кратка е-Методика)
3. Къминг, Т., Малкото "е" на големия бизнес, Бизнес планиране за интернет търговия, изд. Класика и Стил ООД, С., 2006.
4. Марчевски, Ив., Международни маркетингови проучвания, Стопански свят, бр. 60//2002.
5. http://www-it.fmi.uni-sofia.bg/courses/BonI/chapter2.html
6. http://www.tuj.asenevtsi.com/Informatica2/I079.htm
7. http://www.tuj.asenevtsi.com/Informatica2/I081.htm
8. http://www.nsi.bg/IKT/IKT.htm
9. http://bg.wikipedia.org
10. http://www.adam-europe.eu/prj/5928/prj/MENUET_course_e-Commerce_bg.pdf
11. http://epp.eurostat.ec.europa.eu/portal/page/portal/eurostat/home
12. http://ec.europa.eu/justice/data-protection/index_en.htm
13. http://erg.eu.int/links/index_en.htm
14. http://www.baet.bg/
15. http://www.baet.net/
16. http://www.crc.bg/

INTERNET SOCIAL NETWORKS – BENEFITS AND RISKS

assistant professor Iliyana Chakarova

PU “Paisii Hilendarski” – branch Smolyan, pet_iliana@yahoo.com

Abstract: *Every-day use of social networks gives us the opportunity to perform various tasks such as:*
– perform job-related activities;
- create professional contacts;
- acquire new qualifications;
- make financial transactions and payments online;
- arrange personal appointments and other communication;
In the current article we discuss some of the major benefits as well as the risks of using social networks online.