Erasmus+

GoDIGITAL

Разширен текст

SPOŁECZNA AKADEMIA NAUK
UNIVERSITY OF SOCIAL SCIENCES

EUnipartners

PF PUBLICA FIDES

Emphasys CENTRE

2.2 РАЗШИРЕН ТЕКСТ

2.2.1 ТЕМА 1: ИНТЕРНЕТ БЕЗОПАСНОСТ

Интернет може да бъде сравнен с океан. Океанът може да бъде много опасно място: хората могат да се изгубят или да се удавят, опитвайки се да се любуват на морето или да изследват неговата омайваща необятност. Майката на снимката обаче не забранява на децата си контакта с морето. Вместо това тя им позволява да се доближат до водата и ги учи как да й се радват, като им обяснява някои правила за безопасно „използване“ на морето. В началото тя застава до тях и ги съветва, така че те постепенно придобиват самостоятелност за да могат по-късно да се радват на водата.

Ето по този начин би трябвало да мислим и за използването на Интернет. Трябва да идентифицираме потенциалните опасности от широко разпространение на Интернет и да придобием знания и начини за избягване на всички възможни рискове. След това е необходимо да се запознаят младите ученици с възприемането на добри практики във връзка с безопасното използване на Интернет.

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

Рисковете в Интернет са много. Ние очертаваме десет (10) от най-големите рискове:

1. Интернет пристрастяване и отчуждение на потребителите от реалния свят
2. Неподходящо и обидно съдържание
3. Нежелани съобщения (спам)
4. Интернет тормоз
5. Онлайн изкушения на потребителя – детска порнография, онлайн хазарт, насилствени игри и други вредни интернет дейности
6. Нарушаване на личното пространство на потребителя
7. Дезинформация, разпространявана по Интернет (фалшиви новини, градски легенди, онлайн шеги)
8. Прихващане на лични данни чрез „фишинг“ и „фарминг“
9. Зловреден софтуер, който заразява компютрите
10. Физическо състояние в резултат на продължителна употреба на компютри

Ние считаме, че в днешно време теоретичните познания не са достатъчни за един учител. Необходими са и познание и практически знания. Поради тази причина в следващите параграфи ще бъдат разработени някои технически въпроси, по такъв начин, че потребителите и учителите в частност да бъдат податливи, но и да реагират на възможните онлайн рискове за да могат да защитят и обучат своите ученици от най-ранна възраст.

2.2.1.1 Как да избягваме лоши сайтове

Преди да започнем с представянето на начините за избягване на „лоши“ уеб сайтове, трябва да отговорим на въпроса: какво се счита за „лош“ сайт? Като „лош“ сайт обикновено се счита всеки уебсайт, съдържащ материали, които попадат в категории от 1 до 8, представени във въведението по-горе.

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

Някои начини за избягване на тези категории уебсайтове:

- **Използване на Интернет филтри**

Има много интернет филтри, които могат да бъдат закупени или изтеглени и които не позволяват на потребителя или членовете на семейството му да отварят всякакви съмнителни сайтове. Тези филтри работят, като предотвратяват достъпа на потребителите до сайтове, които се считат за съмнителни от гледна точка на безопасността им или които представляват неподходящо или NSFW (не безопасно за работа) съдържание. Много родители използват тези филтри, за да се уверят, че децата им използват само сайтове, които са подходящи за възрастта им, но и хора от всички възрасти, както и учители, могат да ги използват, за да се уверят, че търсенето им в мрежата винаги е безопасно.

- **Използване на филтрите на търсачките**

Много търсачки дават на потребителите на интернет възможността да изберат „по-безопасно“ търсене при използване на техните услуги. Например, Google предлага „безопасно филтриране при търсене“. Това важи за всяко търсене на изображения и видео, както и за новини и общо търсене на съдържание.

- **Не предполагйте адреса на уебсайт**

Това вероятно е начин номер едно, по който хората попадат на неприятности. Има много сайтове, които използват уеб адреси подобни на популярни и безопасни уебсайтове и когато хората се опитват да напишат по спомен адреса на сайт, които искат да посетят, те в крайна сметка попадат на грешен сайт.

- **Никога влизайте в сайт, които изглежда съмнителен**

Когато имате съмнения, не влизайте в сайта. Ако описанието на сайта, името или URL адресът му изглеждат по някакъв начин „изключени“, можете да намери друг сайт, който е по-надежден, особено когато използвате сайта за проучване.

2.2.1.2 Въведение в зловредния софтуер – Как да го избягвате

Риск номер 9 във въведението се отнася до зловредния софтуер. Това е е термин, който се използва за злонамерен софтуер, който е предназначен да нанася щети или да извършва нежелани действия на компютърна система. Примерите за зловреден софтуер са : вируси, червеи, троянски коне, шпионски софтуер и измамен софтуер.

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

Следва кратко описание на на всеки един от тези типове зловреден софтуер, така че учителят да се запознае с терминологията и особено с начина, по който всеки един тях работи.

- **Компютърни вируси**

Компютърен вирус е малка софтуерна програма, която се разпространява от един компютър на друг и пречи на работата на компютъра. Компютърен вирус може да повреди или изтрие данни на компютър, да използва електронната поща, за да разпространи вируса на други компютри или дори да изтрие всичко от твърдия диск. Компютърните вируси често се разпространяват чрез прикачени файлове в имейл съобщения или чрез съобщения в реално време. Следователно потребителят никога не трябва да отваря прикачен файл за имейл, освен ако знае кой е изпратил съобщението. Вирусите могат да бъдат прикрити като прикачени файлове със забавни изображения, поздравителни картички или аудио и видео файлове. Компютърните вируси също се разпространяват чрез изтеглене от Интернет. Те могат да бъдат скрити в пиратски софтуер или в други файлове или програми, които някой може да изтегли.

- **Компютърни червеи**

Червей е компютърен код, който се разпространява без взаимодействие с потребителя. Повечето червеи започват като прикачени файлове към имейл, които заразяват компютъра, когато се отворят. Червеят сканира заразения компютър за файлове, като адресни книги или временни уеб страници, които съдържат имейл адреси. Червеят използва адресите за изпращане на заразени имейл съобщения и често имитира (или подправя) адресното поле „От“ в последващи имейл съобщения, така че тези заразени съобщения изглежда да са от някой, когото познавате. След това червеите се разпространяват автоматично чрез имейл съобщения, мрежи или слабости на операционната система, често затрудняващи тази система, още преди да е известна причината. Червеите не винаги са разрушителни за компютрите, но обикновено причиняват проблеми с работата и стабилносттз на компютъра и мрежата.

- **Троянски коне**

Троянски кон е злонамерена софтуерна програма, която се крие вътре в други програми. Той влиза в компютър, скрит вътре в оригиналната програма, като например скрийнсейвър. Тогава поставя код в операционната система, който позволява на хакер да получи достъп до заразения компютър. Троянските коне

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

обикновено не се разпространяват сами. Те се разпространяват от вируси, червеи или изтеглен софтуер.

- **Шпионски софтуер**

Шпионският софтуер може да се инсталира на компютър без знанието на потребителите. Тези програми могат да променят конфигурацията на компютъра или да събират рекламни данни и лична информация. Шпионският софтуер може да проследява историята на търсене в Интернет и също така може да пренасочва уеб браузъра към уебсайт, различен от този, на който потребителят възнамерява да отиде .

- **Изманен софтуер**

Измамната софтуерна програма за сигурност се опитва да накара потребителя да мисли, че неговият / нейният компютър е заразен от вирус и обикновено го/я подтиква да изтегли или купи продукт, който премахва вируса. Имената на тези продукти често съдържат думи като Antivirus, Shield, Security, Protection или Fixer. Това ги прави да звучат като легитимни. Те често се стартират веднага след като някой ги изтегли или след последващо стартиране на компютъра. Измамният софтуер може да попречи на приложения като Internet Explorer да се отварят. Той може също да показва, че важни файлове на Windows са заразени.

За да избегне всички тези видове зловреден софтуер, потребителят трябва да се запознае с някои техники като:

- Инсталиране на качествени антивирусни програми
- Инсталиране защита от шпионски софтуер в реално време
- Поддържане актуален анти-злонамерен софтуер
- Извършване на всекидневни сканирания
- Декативиране на автоматичното стартиране
- Дективиране на визуализациите на изображения в Outlook
- Избягване да отваряте линкове или прикачени файлове от имейли
- Умно сърфиране
- Използване на хардуерна защитна стена
- Поставяне на DNS защита

Въпреки това зловредния софтуер може да бъде предотвратен само с интелигентно онлайн поведение. Най-големият фактор за предотвратяване на злонамерена програма на компютър е самият потребител. Потребителите на компютри не се нуждаят от експертни знания или специално обучение. Те просто се нуждаят от бдителност, за да избегнат изтеглянето и инсталирането, колкото и да е изкушаващо, на всичко, което не разбират или на което се доверяват, от следните източници:

- **От уебсайт:** Ако не сте сигурни, напуснете сайта и проучете софтуера, който ви се иска да инсталирате. Ако е наред, винаги можете да се върнете на сайта и да го инсталирате. Ако не е наред, ще избегнете главоболие от зловреден софтуер.
- **От имейл:** . Не се доверявайте на нищо, свързано със спам съобщения. Подхождайте към имейли от хора, които познавате с внимание, когато съобщението

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

съдържа връзки или прикачени файлове. Ако това, което се иска да прегледате или инсталирате, изглежда съмнително, не го правете.

- **От физически носител:** Ваши приятели, семейство и сътрудници могат несъзнателно да ви дадат диск или флаш устройство със заразен файл в него. Не приемайте сляпо тези файлове; сканирайте ги със софтуер за сигурност. Ако въпреки това все още не сте сигурни, не приемайте файловете.
- **От изкачащи прозорци:** Някои изскачащи прозорци или кутии ще се опитат да ви насочат към изтегляне на софтуер или приемане на безплатно „системно сканиране“ от някакъв тип. Често тези изскачащи прозорци използват плашещи тактики, за да повярвате, че имате нужда от това, което предлагат, за да сте в безопасност. Затворете изскачащия прозорец, без да натиснете върху нещо вътре (включително X в ъгъла). Затворете прозореца чрез Windows Task Manager (натиснете Ctrl-Alt-Delete).
- **От друг софтуер:** Някои програми се опитват да инсталират зловреден софтуер като част от собствения процес на инсталиране. Когато инсталирате софтуер, обърнете голямо внимание на полетата за съобщения, преди да натиснете бутона Напред, ОК или Съгласен съм. Сканирайте потребителското споразумение за всичко, за което се предполага, че зловреден софтуер може да е част от инсталацията. Ако не сте сигурни, анулирайте инсталацията, проверете програмата и стартирайте инсталацията отново, ако прецените, че е безопасна.
- **От нелегално споделяне на файлове:** Контролът върху качеството на нелегалния софтуер е малък, затова е лесно за атакуващият да наимеува зловредния софтуер като популярен филм, албум или програма, за да ви изкуши да го изтеглите.

2.2.1.3. Как да премахнате злонамерен софтуер

Ако подозирате, че е налице зловреден софтуер или просто искате да бъдете внимателни има няколко стеъпки, които да предприемаете

а) Архивирайте всички файлове и други данни

Файловете и данните са от решаващо значение. Затова в момента, в който разберете, че вашият компютър е заразен със зловреден софтуер трябва да архивирата всички файлове и други данни преди зловредния софтуер да

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

достигне до тях и да ги повреди. Освен това подобно архивиране ще ви помогне бързо да си ги върнете обратно.

b) Прекъснете връзката с интернет

Следващото най-добро действие е да прекъснете връзката на компютъра с Интернет за да предотвратите по нататъшни щети, тъй като Интернет е мястото за разпространение на зловредния софтуер. И всеки момент, в който потребителят остава свързан с интернет, особено след заразяване с зловреден софтуер, положението му ще се влоши.

c) Сканирайте компютъра в безопасен режим

Превключете на безопасен режим и сканирайте компютъра. Без задълбаване в технически подробности, безопасен режим е ограничен режим, който позволява да се стартират само сигурни приложения, като по този начин се намалява риска от разпространение на зловреден софтуер в други части на компютъра. В най-добрия случай подобно почистване може да подобри работата на компютъра. Друга проста, но ефективна мярка би била почистването на временните и изтеглените файлове.

d) Използвайте инструмент за премахване на зловреден софтуер

Ако все още нямате изтглете линцензирана прогрма срещу зловреден софтуер. След това я инсталирайте и стартирайте. Програми като тези са предназначени да търсят и елиминират всеки злонамерен софтуер на устройството.

След като устройството е вече чисто е добре да промените паролите, не само на компютъра или мобилното устройство, но също и за имейла си, за профилите си в социалните медии, за любимите ви сайтове за пазаруване и за онлайн банкиране и фактуриране.

Премахването на зловреден софтуер не е лека задача и понякога не можем да се справим сами. Ето защо е най-добре да оставите на експерти да се справят със ситуацията, ако смятате, че не можете сам да решите проблема.

2.2.1.4 Подсигуряване на интернет профили

Паролите са като ключове от личния ви онлайн дом. Трябва да направите всичко, което можете за да попречим на други хора да получат достъп до паролата ви. Можете допълнително да защитите своите профили като използвате допълнителни методи за установяване. Някои основни съвети са:

- Затворете профилите, които не използвате от дълго време
- Създавайте силни пароли (т.е. направте паролата си цяло изречение)
- Уникален профил – уникална парола
- Напишето го и го пазете
- Променяйте често своите пароли
- Заключване на вход (силно

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

удостоверяване)

- Проверявайте активността във вашия профил
- Актуализирайте профила си
- Посочете вашите доверени контакти

Повече идеи за безопасността на интернет можете да намерите в предложената допълнителна литература.

Препратки

https://www.lifewire.com/avoid-dangerous-websites-3481594

https://support.microsoft.com/uz-latn-uz/help/129972/how-to-prevent-and-remove-viruses-and-other-malware

https://www.malwarebytes.com/malware/

https://antivirus.comodo.com/security/how-to-get-rid-of-malware.php

https://www.wikihow.com/Keep-Online-Accounts-Secure

https://www.bullguard.com/bullguard-security-center/internet-security/security-tips/safe-online-accounts.aspx

https://www.pcworld.com/article/210891/malware.html

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543