# Интернет престъпления

Живка Военкинова

***Abstrac. Internet crime****: Presented are the most popular Internet crimes.They discuss the measures to be taken against cybercrime. Justify the necessity of preventing and combating Internet crime and the usefulness of the formation of knowledge and skills of students to deal with criminal situations.*

***Key words:*** *internet, crimes, fraud, studenti, prevention.*

## ВЪВЕДЕНИЕ

Модерните технологии в съвременния свят улесняват дейността на хората и ежедневни им живот. Заедно с това се извършват множество престъпления поради, които могат да възникнат различни проблеми.

Ежедневно сме свидетели на много измами, които се извършват, чрез интернет, за които потърпевшите изобщо не подозират и научават за тях понякога чак след години. В много от случаите извършителите не могат да бъдат открити, което допълнително усложнява нещата.

Поради това, считаме, че е необходимо студентите от ШУ „Еп. Константин Преславски", специалност „Социална педагогика" /бакалавърска и магистърска степен/, които не са специалисти в областта на компютърните технологии, да бъдат специално запознати с проблемите, които произтичат от интернет измамите.

## ИЗЛОЖЕНИЕ

Почти във всяко домакинство съществуват компютри и членовете и от най-големия до най- малкия ежедневно ползват интернет.

„Под престъпление в кибернетичното пространство „компютърно престъпление", „свързано с компютърните престъпления" или „престъпления в сферата на високите технологии" следва да се разбира престъпни деяния, извършени посредством използване на електронни съобщителни мрежи и информационни системи или срещу такива мрежи или системи" [2,с.1]. Престъпленията са три категории:

- измама или фалшификация;
- извършени посредством електронни съобщителни мрежи;
- извършени посредством информационни мрежи;
- публикувани в електронна медия на незаконно съдържание:
  - детска порнография;
  - материали за подбуждане на расова омраза и др.;
- престъпления характерни единствено за електронната мрежа:
  - атаки срещу информационни системи;
  - отказ на услуга;
  - чужд достъп, т.е. хакерство и др.

Регулацията на компютърните измами в Република България се извършва чрез:

- структурите на Министерство на вътрешните работи и прокуратурата;
- в Наказателния кодекс съществува глава „Компютърни престъпления"
- проект „Кибер тероризмът като нова заплаха за сигурността" - финансиран от НАТО;
- проект „Правосъдие в дигиталната ера" - укрепване на капацитета на магистратите на България и Румъния при разследване, обвинения, и осъждания в случаи включващи кибер престъпления с финансовата подкрепа на Европейската комисия;
- анализ на ситуация в превенцията и борбата с компютърните престъпления в България, и Румъния;

- обучения за борба с компютърни престъпления - обучени са 150 съдии, прокурори и следователи от България [2,с.1].

Я. Колев [3,с.1] началникът на сектор „Компютърни престъпления" в ГДБОП, посочва, че законодателството за разследване на тези престъпления дава много възможности. За да се съберат достатъчно доказателства и разследването да е качествено се гарантира запазване на данните от интернет доставчиците до над 6 месеца. Според него последната мода в тези престъпления е свързана с кражба на сертификати и онлайн банкирането, таргетират се групи с интереси в областта на търговията, получената информация се подава на по-големи онлайн пазари. Той подчертава, че е достатъчно да бъдат сигнализирани за престъпления, но не скрива, че не е възможно да следят всичко.

Препоръчва хигиена на интернет общуването като мярка за защита на личните данни от посегателства в мрежата, хората да не предоставят личните си данни на когото и да било, защото не е изключено те да бъдат използвани неправилно.

Европейската комисия за борба с компютърните престъпления [4,с.1] посочва, че всеки ден около 1 милиард души стават жертви на компютърни престъпления. Извършителите са невидими за хората и остават ненаказани.

Европейският център по киберпространство към Европейския съюз ще предупреждава страните от Европейския съюз за сериозни заплахи, ще идентифицира престъпни мрежи и ще оказва помощ по време на разследване.

Кибер престъпността в Европейския съюз най- често включва следното:

- кражби на самоличност в интернет;
- компютърни измами;
- измами с кредитни карти;
- сексуална експлоатация на деца;
- присвояване на профили в интернет;
- атаки срещу публични или частни интернет системи.

Всеки ден след хакерски атаки се блокират около 600 000 профила във Facebook.

Само за 2011г. загубите в световен мащаб, които са причинени от компютърни измами са над 85 до 291 мил. евро. Следователно, прокурори и съдии могат да задават към този център въпроси от технически и криминален характер.

Мерките, които се предприемат срещу кибер престъпленията ще доведат да следното:

- повишаване доверието към електронното банкиране;
- повишаване доверието в онлаин резервациите;
- ще се увеличи спестяването на милиони евро.

За превенция и борба с интернет престъпленията МВР [5,с.1] стартира официален сайт www.cyberkrime.bg , чрез който в реално време учениците могат да подават сигнали. Я. Колев ще управлява административно този сайт. По идея на учениците от Софийската професионална гимназия по електроника „Джон Атанасов" е създаден лицензираният софтуер, който е осигурен от Асоциация на полицейските началници.

Целта на създаване на сайта е да се намалят престъпленията от или срещу деца, предпазване от престъпления в Интернет и формиране на отговорно поведение в мрежата. Учениците предлагат на специалистите от МВР сами да формират „Интернет патрули", чрез които да откриват с помощта на сърфиране във виртуалното пространство, сайтове с незаконно съдържание и да подават сигнали в ГДБОП.

Страницата е създадена по следният начин и менюто за навигация включва следното:

- информация на английски и български език;
- Наказателен кодекс;

- Закон за закрила на детето;
- Конвенция за престъпления в кибернетичното пространство;
- Правила за безопасна работа на учениците в Интернет и училищната мрежа;
- съвети към родителите;
- съвети към децата;
- сигнализиране;
- Фишинг;
- компютърен жаргон;
- Форум.

С. Бачева [6,с.1] посочва, че през 2015г. и в България вече са разпространени 10- те най- популярни измами по Интернет и те са следните:

- търговски измами - безброй видове, чрез които предлагат стоки за продажба, но на много ниски цени;
- „pump-and-dump" схеми- чрез различни канали се разпространяват фалшиви информации за компании или за някакви акции;
- клик-измами /clik-throygh-frauds/ nare`en o]e "феномен на нашето време"- търговци плащат на различни големи сайтове да публикуват рекламен банер и в зависимост от броя на кликванията върху банера, търговецът плаща на сървиз-провайдър определена сума в края на месеца, конкурентите му могат да кликат върху банера много пъти, т.е. правят „кухи" посещения и в края на месеца трябва да плати огромни суми без да е привлякъл очакваните клиенти;
- мними търгове - от името на компании с много добра репутация на пазара се организират недействителни търгове, чрез фалшиви интернет страници като те на знаят за това и много хора изгарят с пари;
- екскроу измами - напр. „За да е сигурно, че като продадете стока на друго лице то ще ви плати парите /или обратно - за да си получите стоката като дадете парите/ всичко трябва да мине през мен";
- фишинг - под формата на спам от името на някоя финансова институция се изпраща съобщение като изискването е човек да даде лични данни, номера на сметки, кредитни карти и проч.;
- фарминг - използване на слабостите на съвременната техника, на начините, по който работи Интернет - използва се за кражба на самоличност, банкови данни и други;
- гугъл бомби - несъзнателно или съзнателно свързване на определен сайт в Интернет с дадена ключова дума и търсачката да изкарва на преден план точно този сайт- например ако са напише думата „провал" да излезе сайт към българското правителство;
- нигерийски измами - получава се известие например, че някоя известна личност е починала или убита като е оставила няколко милиона долара , които трябва да се скрият след това се предлага човек да си посочи банковата сметка за да му преведат огромна сума, от която ще получи % за услугата, а след това веднага се изисква да им се направи превод за административни такси, мита и проч.;
- кражба на банкови сертификати - троянски кон се въвежда в компютъра на дадена компания като след това се изтегля информацията и се използва за престъпления, дори и чрез електронно банкиране.

Според някои изследователи [6, с.1] във Фейсбук жените малко превъзхождат останалите със своето присъствие и отношение към него. Жертви на опити за финансови измами стават над 30% от потребителите на Интернет. Най-често срещана е, т. нар. „нигерийска измама" като напоследък тя има нова модификация , която започва с ухажване на жените и предложение за брак, които са много примамливи, и обещаващи светло бъдеще. Целта им е да измъкнат различни суми пари като започнат от ухажването до края всичко трае около месец. Обикновено

освен снимката, на която се вижда много привлекателен мъж нищо друго не се споменава за място работа, фирма или нещо, което да може да се провери. В крайна сметка „много влюбеният мъж" съобщава, че банката временно му е блокирала по неизвестни причини сметката и за да пристигне при нея тя трябва да му преведе сумата за самолетен билет. В зависимост от финансовото състояние на жената варират исканите суми, но не са редки случаите, когато ги уговарят да инвестират в неговия или на негови познати бизнес. Конкретно име и адрес се дава, когато жената е наивна и се поддаде на обещанията. Изискването е да се изпрати сумата, чрез Western Union и др. подобни начини.

Съветите при съмнение за измама в подобни случаи са следните:

- веднага да се затвори страницата;
- да се проследи IP адреса на измамника;
- нищо повече да не се споделя с измамника;
- нищо да не се изпраща на измамника;
- да не се дават лични данни и данни за достъп в мрежата;
- да не се дават данни за дебитни и кредитни карти;
- винаги да се излиза от системата и от конкретните сайтове, да не се оставя отворено за хакерски атаки;
- да не се запомнят пароли за вход;
- да се използват различни пароли за всяка регистрация;
- да се проверяват всички данни, които са известни за измамниците независимо колко са оскъдни [7,с.2].

Инцидентите в Интернет, т. е. измамите в електронната поща, които днес най-много се обсъждат са и най- обезпокояващи [8,с.1].

Измамите в Интернет имат следните характеристики:

- получателят не познава източника на електронното писмо;
- получените писма звучат официално;
- за увеличаване на безпокойството писмата звучат трагично;
- често предупреждават за злонамерен софтуер, който ще унищожи хардуера;
- всяват страх у хората;
- съдържат граматични и правописни грешки;
- информацията в тях е противоречива;
- не предоставят адрес, който може да се провери в Интернет, а включват молба да се изпрати писмо в електронната поща на всички, които познаваме и др.

Г. Константинова и Д. Димова [1,с.1] посочват, че изтеглените с чужди лични данни бързи кредити са хит на годината. Финансовите институции, които предлагат бързи пари само за 10 мин. е явление ново за нашия пазар поради, което прокуратурата призовава хората да бъдат нащрек. От съда предупреждават, че ако измамените по някакъв начин успеят да докажат, че те не са теглили кредити и не се наложи да ги погасяват в бъдеще ако решат да теглят кредити определено ще имат проблеми, защото имената им ще са влезли в регистъра на лошите длъжници.

## ЗАКЛЮЧЕНИЕ

Заключението, което може да се направи е, че измамниците са навсякъде около нас и са готови, както да извършат престъпления, така и да замесят в тях и нас самите без да подозираме за това. Студентите от специалност „Социална педагогика" се запознават с посочените интернет измами както по време на лекционните курсове, така и по време на семинарните упражнения при обучението по информационни технологии. Получените знания и формираните практически умения могат да им послужат при професионалната реализация, и в личен план за предпазване от подобни измами, и престъпления.

**ЛИТЕРАТУРА**

[1] Константинова, Г. и Д. Димитрова, SOS! Нов вид измама , пазете си личните данни, Марица, Пловдив, 2015,1.

[2] www.netlaw.bg//-bg/?S=198i=9- Компютърни престъпления.

[3] www.temanews.com/index.php?p=tema&ind=227said=7923- Шефът на сектор „Компютърни престъпления" е ГДБОП Явор Колев: Наказанията за проникване в чужд имейл са малки.

[4] www.europa.eu/news/justice/120328_bg.htm - Европейска комисия. Борба с компютърни престъпления.

[5] tchnews.bg/article -6716.htm l - МВР стартира сайт за превенция и борба с интернет престъпленията.

[6] e-vestnik.bg - Бачева, С., 10-те най-популярни измами по Интернет вече и в България.

[7] dariknews.bg- Нов вид финансови измами по Интернет свързани с онлайн ухажване и обещания за брак.

[8] znannieto.net - Измамите в интернет.

**За контакти:**

Проф. д-р Живка Енчева Военкинова, Катедра "Социална педагогика", Шуменски университет "Еп. Константин Преславски", тел.: 0893336809, e-mail: jivkavo@abv.bg