УДК: 004.056.5+343.721

Волошина Д. О.
Остапенко-Боженова А.В.

СОЦІАЛЬНА СКЛАДОВА ІНТЕРНЕТ-ШАХРАЙСТВА

Вінницький національний технічний університет

Анотація

Робота присвячена дослідженню особливостей інтернет-шахрайств. Розглянуті основні методи шахрайств в мережі інтернет.

Ключові слова: інтернет, шахраї, обман, інтернет-шахрайство.

Abstract

The work is devoted to the study of the peculiarities of Internet fraud, their types. The main methods of fraud on the Internet were considered.

Keywords: internet, fraudsters, deception, internet fraud.

Вступ

Інтернет-шахрайство, яке, з одного боку, є результатом еволюції традиційного шахрайства, оскільки деякі його види зустрічаються в Інтернеті без будь-яких серйозних змін в методиці реалізації злочинного замислу; з іншого боку - це якісно нова група злочинів, оскільки при схожості методів реалізації, конкретні способи мають істотні відмінності [1].

Практично повна безкарність, анонімність шахраїв, велика кількість довірливих людей – все це стає причинами збільшення масштабів інтернет-шахрайства. Зловмисники вигадують нові схеми вимагання грошей з інтернет-користувачів.

Основна частина

Інтернет- чи мобільне- шахрайство – є способом здійснення злочину за допомогою сучасних технологій. Відповідно до частини першої статті 190 Кримінального кодексу України, шахрайство – це заволодіння чужим майном або набуття права на майно шляхом обману чи зловживання довірою [2]. Частиною третьою статті 190 Кримінального кодексу України передбачається, що шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки карається позбавленням волі на строк від трьох до восьми років [2].

Інтернет-злочини, як і багато інших комп'ютерно-мережевих злочинів, характеризується високою латентністю, по-перше, через складність розслідування, тому що найчастіше шахраї діють анонімно, а по-друге, іноді через дуже складну реалізацію шахрайських схем в Інтернеті досить важно зрозуміти хід їхніх думок та передбачити наступний крок [1].

Як і в традиційному шахрайстві, основна частина посягань направлена на невизначено широке коло потенційних жертв, а особливо на шантаж заради власної вигоди шахрая.

Однією з особливостей є також те, що для деяких способів інтернет-шахрайства характерна наявність додаткових вимог до особистості злочинця. Найчастіше мова йде про наявність спеціальних знань у певній сфері - сфері інформаційних технологій. Інтернет-шахраї зазвичай досить освічені люди у сфері інтернет-технологій, вони знаю великі кількість лазівок, за допомогою яких стає майже не можливо ідентифікувати їхню особистість.

У випадку з інтернет-шахрайством посягання відбувається виключно на право на майно, оскільки Інтернет є, скоріше, певним середовищем здатним до передачі виключно інформації. Таке середовище можна вважати матеріальним лише умовно, оскільки вона не має всі ознаки матеріальності. Таким чином, якщо злочинець, вчинивши шахрайство, викрав грошові кошти, шляхом переводу їх на свій таємний рахунок, то це, не буде розкраданням саме грошових коштів. Швидше навпаки, це повинно вважатися отриманням права на них, в тому числі права отримати ці гроші в матеріальній формі [3].

Виходячи з вище написаного найпоширеніші шахрайські схеми, що використовують методи соціальної інженерії, зображені на рис.1.

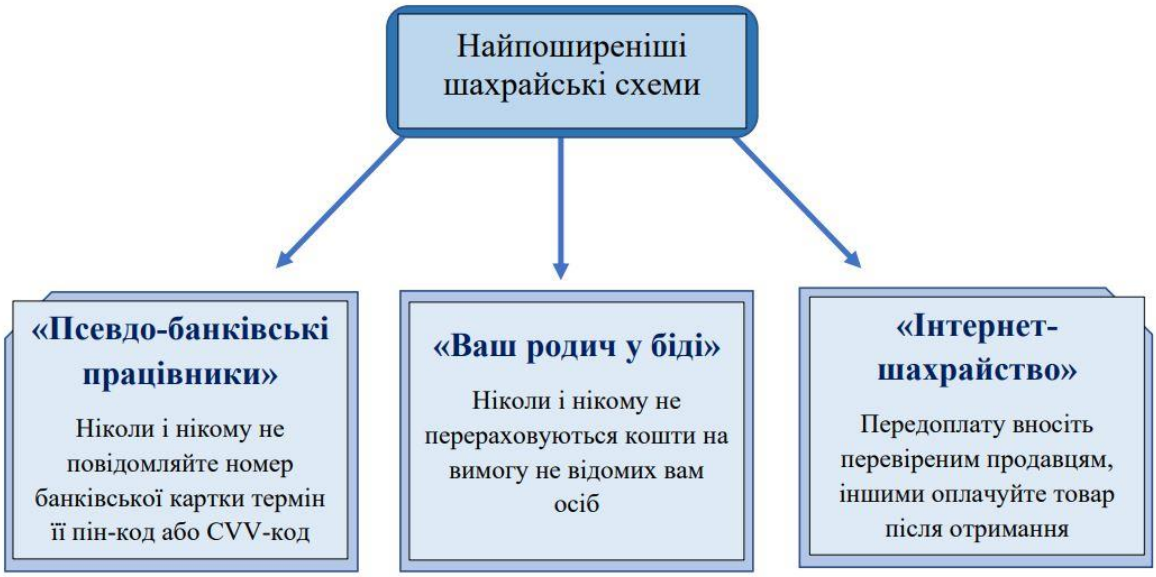

Рис. 1 Найпоширеніші шахрайські схеми

Шахраї є досить гарними психологами у сфері комунікації з довірливими людьми і знають, на які слабкі сторони людської особистості можна натиснути, щоб переконати жертву добровільно розлучитися з заощадженнями або персональними даними. Невігластво, жадібність, віра в «щасливий випадок», лінь, азарт, марнославство, несамостійність, забобони, звичка бути ввічливим і дотримуватися суспільних норм, ритуали і традиції, комплекси, невротичні стани: завдяки цим умовно негативним рисам люди потрапляють під вплив методів соціальної інженерії шахрая, іноді навіть не усвідомлюючи цього. Інтуїтивно шахраї використовують такий фактор, як навіювання, впливаючи на емоції і почуття, тобто на підсвідомість жертви, тим самим маніпулюючи поведінкою, розумом і волею людини [4].

Висновки

Отже, дослідивши питання інтернет-шахрайств можна виділити декілька важливих речей. Зараз такий вид шахрайств дуже розповсюджений тому що інтернет – це найкращий простір зловмисника для реалізації своїх незаконних схем та планів. Тому, потрібно обов'язково дотримуватись правил кібергігієни та безпеки в мережі. Пильність, увага та обізнаність в сфері інформаційних технологій та кібергігієни стають основними факторами захисту від інтернет-шахрайств.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Криміналістична профілактика економічних злочинів: науково-практичний посібник / Кол. авт.: С.В. Веліканов, А.Ф. Волобуєв, В.А. Журавель та ін. (За ред. д-ра юрид. наук, проф. В.А. Журавля) Харків: ''Харків юридичний'' , 2006. 236с.)
2. Кримінальний кодекс України : Кодекс України; Кодекс, Закон від 05.04.2001 № 2341-III // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2341-14 (дата звернення: 01.05.2022)
3. Тюлюкіна О.В. Протидія економічним злочинам, що вчиняються в кіберпросторі: магіст. робота. ст. юридичного факультету/ Тернопільський національний економічний університет, 2018. 122с.
4. Мотузка Л. І., Шпитяк В. А. Захист дітей від шкідливого впливу мережі інтернет: навчально методичний посібник. Срібне: Відділ освіти Срібнянської районної державної адміністрації Районний методичний кабінет, 2015. 25с.

Волошина Дана Олегівна – студентка групи 1КІТС-20б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: voloshynadana11@gmail.com

Остапенко-Боженова Аліна Василівна —. асистент кафедри Захисту Інформації, Факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: ostapenko-bozhenova_a_v@vntu.edu.ua

Voloshyna Dana Olehivna - student of group 1KITS-20b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: voloshynadana11@gmail.com

Ostapenko-Bozhenova Alina V. — assistant in Information Protection department Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: ostapenko-bozhenova_a_v@vntu.edu.ua