

# ІНТЕРНЕТ-ШАХРАЙСТВА ТА СПОСОБИ ЇХ УНИКНЕННЯ

*Беліцький О. С., студ. (гр. КП-01, ФПМ КПІ ім. Ігоря Сікорського);  
Полукаров Ю. О., к.т.н., доц. (каф. ОППЦБ, КПІ ім. Ігоря Сікорського)*

**Анотація.** 2020 рік став переломним у сфері інтернет послуг. Торгівля їжею та її доставка, придбання ліків, одягу, взуття, оплата комунальних платежів та багато іншого наразі можна зробити через інтернет. Однак, разом з цим стрімкого розвитку набуло явище онлайн шахрайства. У даній роботі висвітлено основні види онлайн-шахрайства та наведено рекомендації – як не стати жертвою сучасних аферистів.

**Ключові слова:** шахрайство в інтернеті, онлайн шахрайство, види шахрайства онлайн, безпека в інтернеті.

**Abstract.** 2020 was a turning point in the field of Internet services. Food trade and delivery, the purchase of medicines, clothing, footwear, utility bills and much more can now be done online. However, at the same time, the phenomenon of online fraud has developed rapidly. This paper highlights the main types of online fraud and provides recommendations – how not to fall victim to modern scams.

**Keywords:** Internet fraud, online fraud, types of fraud online, security on the Internet.

**Вступ.** На сьогодні, з розвитком комп'ютерних технологій та всесвітньої мережі Інтернет, актуальною є проблема безпеки. «Попереджений – значить озброєний», – відомий вислів, який доречно згадати, перш ніж переходити до висвітлення даного матеріалу.

Для початку визначимо, що таке шахрайство. Шахрайство – це свідоме намагання заволодіння чужим майном або придбання права на майно, шляхом обману чи зловживання довірою [1]. Відповідно, жертви шахрайства, у даному випадку – це особи, які хотіли отримати ту чи іншу послугу або товар, віддаючи свої гроші, майно та інформацію онлайн-махінаторам. У цьому полягає специфіка шахрайства – все нібито робиться добровільно та за власного бажання.

У кримінальному кодексі передбачено два способи шахрайства [1]:

- обман;
- зловживання довірою.

**Аналіз стану питання.** На даний час неможливо перерахувати всі відомі схеми шахрайства, адже з кожним днем їх стає дедалі більше. Це зумовлено технологічним «кібер» прогресом та поколінням, яке не уявляє своє життя без цих історичних нововведень. Зростання населення в містах, брак робочих місць, жага легких грошей, масова поява людей з феноменом «хіккі» (японський термін, яким характеризують людей, що відмовляються від соціального життя і прагнуть до соціальної ізоляції, внаслідок дії різних особистих і соціальних факторів) – основні причини розвитку інтернет-шахрайства.

**Мета роботи.** Охарактеризувати основні види інтернет-шахрайства та

розробити рекомендації для запобігання потрапляння в пастки інтернет-аферистів.

**Методики, матеріали і результати досліджень.** Інтернет – це мережа, що об'єднує комп'ютери по всій Земній кулі, дозволяючи отримувати інформацію, спілкуватися, обмінюватись файлами, вести торгівлю тощо. Інтернет з'явився лише у 1969 році, але зараз, лише через 52 роки, ми вже не можемо уявити своє життя без нього. Спілкуватися, навчатися, робити покупки можна, не виходячи з дому. Це відкриває великий світ можливостей, який, нажаль, має не лише позитивні риси. Однією з проблем, яка з'явилася з розвитком Інтернет мереж – онлайн-шахрайство.

Виділимо декілька основних різновидів онлайн-махінацій [2]:

- з «передплатою»;
- з «призами»;
- «надзвичайна ситуація»;
- онлайн-шопінг;
- онлайн-знайомства;
- «квитанція».

Нижче наведемо пояснення сутності всіх видів шахрайства даного переліку.

**Шахрайство з «передплатою».** Сюди можна віднести такі ситуації, коли Вас попросять внести кошти авансом для отримання тієї чи іншої послуги або товару. Пропонують працевлаштування чи навчання, але кошти потрібно відправити заздалегідь кошти. Сюди також можна віднести махінації з орендою майна: ви наче щось орендуєте, а такого майна не існує взагалі [3].

**Шахрайство з «призами».** Ви начебто «виграли» автомобіль, поїздку на Гаваї чи ящик косметики. Зазвичай на екрані, при перегляді якомось сайту, спливають вікна, на які не спішіть натискати. Безкоштовний сир – лише у мишоловці. Найімовірніше Вас попросять або надіслати гроші на якийсь рахунок, щоб нібито брати участь у розіграші або просто через посилання зможуть проникнути у Ваш комп'ютер, причому Ви, навряд чи про це дізнаєтесь.

**Шахрайство про «надзвичайну ситуацію».** Такий вид шахрайства був популярний у 2017-2019 роках. Напевне Ви зіштовхувались з СМС-ми, у яких був стандартний текст «Мамо, будь ласка, терміново надійшли мені грошей на цей номер телефону, дуже треба, я в біді!». Тут схема та сама: Вас просять надіслати особисті дані, бо банк заблокував Вашу карту, але банк взагалі тут ні до чого, або щось, на кшталт, повідомлень «Привіт, я твій друг дитинства, допоможи, скинь на карту (\*номер карти\*) таку суму, я беру участь у шоу, потрібна твоя допомога!» [4].

**Шахрайство при онлайн шопінгу.** Часто це переплітається зі схемами шахрайства з передплатою, але також Вас можуть попросити надіслати кошти за товар, знижка на який, виглядає дуже привабливою, але, зазвичай, після переказу коштів Ви не побачите ані товару, ані можливості зв'язатися з

«продавцем».

**Шахрайство в онлайн знайомствах.** Дедалі більше з'являється історій про нібито щасливі подружжя, які познайомилися в Інтернеті. Насправді, індустрія онлайн-знайомств більш «розвинута», ніж Ви можете собі уявити. Торгівля особистими фотографіями, особистою інформацією, навіть веб-проституція та багато іншого – це далеко не повний перелік «товарів та послуг» на просторах цього сегменту інтернету. Тут варто бути особливо уважним. Найчастіше і найбанальніше – Ви певний час спілкуєтесь з людиною, якій поступово починаєте довіряти, і, яка одного «прекрасного» дня, просить Вас скинути гроші на якусь вигадану потребу [3].

**Шахрайство з «квитанціями».** Особливо уважними потрібно бути, коли Ви отримуєте квитанції, тому що вони можуть бути підробленими. Вас можуть попросити повернути кошти, ніби помилилися рахунком, або квитанція виявилася на більшу суму, ніж домовлялися, і Вас попросять повернути різницю між вказаною і договірною сумою. Тут все потрібно перевіряти по декілька разів. Ніколи не поспішайте, а за необхідністю зверніться до компетентної людини (співробітник банку, де Ви обслуговуєтесь, або знайомий-фінансист), яка допоможе, переконатися, що з квитанцією усе гаразд [4].

Після ознайомлення з основними видами шахрайства в Інтернеті надамо рекомендації – як не потрапити до пастки аферистів.

**Рекомендації як не стати жертвою онлайн-шахраїв [5].**

- остерігайтеся фейкових інтернет-магазинів, сторінок у соціальних мережах та сайтів-двійників;
- не довіряйте підозрілим повідомленням про шалені виграші та спадки від закордонних родичів, про яких Ви раніше навіть ніколи не чули;
- ні в якому разі не вказуйте свої персональні дані на неперевірених сайтах і сервісах;
- не розголошуйте дані банківських карток (ключове слово, термін дії та CVV-код);
- не варто реагувати на листи, яких Ви не очікували або не знаєте їх джерел;
- здійснюйте передплату лише у перевірених інтернет-магазинах (або, принаймні, на незначну суму);
- рор-уп вікна з оголошеннями продажі акційних товарів або вакансій – не те місце, де Ви знайдете, що Вам потрібно;
- не користуйтеся підозрілими сервісами;

**Висновки.** Резюмуючи все вищесказане, стає зрозуміло, що безпека в Інтернеті – це особиста справа кожного. Навіть злагоджені дії державних структур не спроможні гарантувати онлайн безпеку, якщо Ви не будете дотримуватись вищевказаних правил та рекомендацій. Якщо ж Ви, все ж таки, стали жертвою онлайн шахраїв, негайно звертайтеся до поліції та/або до суду.

## Література

1. Кримінальний кодекс України: № 270-VI від 15.04.2008. Чинний зі змінами. Перевірено 08.07.2019. Ст.190. URL : [https://kodeksy.com.ua/kriminal\\_nij\\_kodeks\\_ukraini/statja-190.htm](https://kodeksy.com.ua/kriminal_nij_kodeks_ukraini/statja-190.htm).
2. Вчені нотатки Таврійського національного університету ім. В. І. Вернадського. Серія «Юридичні науки». Том 26(65) 2013. №1. С. 278-283.
3. Очімовська Т. Новые уловки интернет-мошенников. Електронний ресурс: URL: [http://smi.liga.net/articles/2013-02-12/8306060-novye\\_ulovki\\_internet\\_moshennikov.htm](http://smi.liga.net/articles/2013-02-12/8306060-novye_ulovki_internet_moshennikov.htm).
4. Коршикова Т.В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки: дис. докт. філ.: Національна академія внутрішніх справ. Київ. 2021. 255 с. – Електронний ресурс. URL: <http://elar.naiu.kiev.ua/jspui/handle/123456789/18989>.
5. Тюлюкіна О.В. Протидія економічним злочинам, що вчиняються в кіберпросторі: магіс. роб. студ.: Тернопільський національний економічний університет. Тернопіль. 2018. 122 с. – Електронний ресурс. URL: [http://dspace.wunu.edu.ua/bitstream/316497/32689/1/%D0%9C%D0%B0%D0%B3\\_%D0%A2%D1%8E%D0%BB%D1%8E%D0%BA%D1%96%D0%BD%D0%B0.pdf](http://dspace.wunu.edu.ua/bitstream/316497/32689/1/%D0%9C%D0%B0%D0%B3_%D0%A2%D1%8E%D0%BB%D1%8E%D0%BA%D1%96%D0%BD%D0%B0.pdf)