УДК 343.53
DOI: 10.31733/15-03-2024/2/303-304

Оксана БРИСКОВСЬКА
провідний науковий співробітник
наукової лабораторії з проблем
протидії злочинності ННІ №1
Національної академії
внутрішніх справ,
кандидат юридичних наук,
старший науковий співробітник

ПРОТИДІЯ ІНТЕРНЕТ-ШАХРАЙСТВУ – В НИЗЦІ ПРІОРИТЕТНИХ ЗАВДАНЬ ПОЛІТИКИ ДЕРЖАВИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Нині, для онлайн-шахрайської діяльності зловмисників, війна відкрила нові «горизонти та можливості», користуючись вразливим емоційним станом співвітчизників, маніпулюючи почуттями людей які перебувають у розпачі та гніві, будують шахрайські схеми, пристосовуючись до ситуації [1, с. 174].

86% від загальної кількості випадків платіжного шахрайства за 2022 рік відбулися в мережі Інтернет [2]. Беручі до уваги обставини, станом на зараз, в яких живуть громадяни України під час війни, онлайн шахраї тільки урізноманітили інструменти та схеми вчинення кримінальних правопорушень. Використовуючи проти людей їхню збентеженість емоційний стан, тривожність, безграмотність у користуванні Інтернетом. Нині більше 70% українців не мають впевненості у своїй здатності розпізнати ознаки онлайн-шахрайства. Менша половина мешканців України перевіряє у повідомленнях безпомилковість назви логотипу компанії і електронну адресу відправника[3]. 7 із 10 українців переймаються, що їх рідні чи друзі можуть з легкістю відреагувати на шахрайське повідомлення, а 68% українців самі не впевнені у своїх можливостях щодо спроможності розпізнати онлайн-шахрайство [3].

Інтернет-шахраї зламують акаунти громадян, роблять сайти, подібні до вебресурсів державних установ, відомих банків, магазинів, розраховуючи на безпечність та неуважність користувачів інтернету. Вчиняють онлайн-шахрайство з продажу товарів і послуг, коли підроблені вебсайти і соціальні мережі можуть використовувати для реалізації неіснуючих товарів або послуг, після чого гроші отримують від покупців, але товари не доставляються [4]. Наприклад, в Київський області, житель п.м.т. Коцюбинського використовуючи один із месенджерів розміщував оголошення з надання послуг щодо пасажирських перевезень за кордон на території України. Наразі поліцейські встановили 62 громадянина, яким зловмисник заподіяв шкоду на приблизну суму у 100 000 гривень [5]. Найбільш розвинути онлайн шахрайство з продажу неіснуючих товарів і послуг у прифронтових областях від якого потерпають наші захисники шахраї під виглядом продавця публікують оголошення з продажу автівок, тактичного екіпірування та багато чого іншого, що є актуальним для наших військових [4]. Зловмисники також проводять неіснуючі інтернет-аукціони з фальшивими ставками, сьогодні, набирає розмаху криптовалютне шахрайство. Онлай-шахраї реалізують інформацію яка наявна в соціальних мережах, тиснучи на родинні зв'язки, використовуючи довіру для виманювання грошей застосовуючи різні форми впливу.

Шахрайські повідомлення, відомі також як фішингові повідомлення, це вид шахрайства, в якому зловмисники намагаються отримати особисті дані осіб, фінансову інформацію або зламати їх облікові записи, шляхом надсилання підроблених електронних листів, повідомлень у соціальних мережах, смс або дзвінків. Основною метою фішингу є зловживання довірою громадян. Шахраї можуть використовувати різні підступні методи, щоб змусити їх розкрити конфіденційну інформацію, наприклад, зловмисники можуть стверджувати, що вони представники банку, онлайнсервісу або іншої довіреної організації. Фальшиві повідомлення, електронні листи або смс, зловмисники здатні відправляти від офіційних органів представляючись представниками правоохоронних органів, уряду або міжнародних організацій. Вони можуть стверджувати, що особа стала жертвою злочину або

повинна сплатити штраф [6].

Протидія різновидам інтернет-шахрайства є важливим завданням сучасного суспільства. Забезпечення безперервної просвітницької роботи, охоплюючи всі соціально-демографічні верстви населення, через засоби масової інформації (телебачення, радіо, пресу, соціальні мережі, сайти, повідомлення в різних месенджерах тощо), бесіди, лекції (колективам, працівникам на підприємствах, в установах, організаціях, студентам у вишах, учням у школі, пенсіонерам, соціально незахищеним верствам населення за місцем проживання і т. ін.) з метою своєчасного інформування про нові види інтернет-шахрайства в умовах воєнного стану [7].

При проведенні такої просвітницької роботи необхідно пояснювати алгоритм дій особи яка стала жертвою злочинних дій онлайн-шахраїв. Наприклад, якщо особа перерахувала кошти на банківський або телефонний рахунок, то цей процес можна зупинити негайно звернувшись до банку з просьбою скасувати платіж та заблокувати банківську картку. Не зволікаючи звернутися в поліцію зателефонувавши за номером «102», або на «гарячу лінію» управління з боротьби кіберзлочинністю надавши свій номер телефону та номер з якого телефонував зловмисник, а також номери банківських рахунків з яких були перераховані кошти та номери рахунків на які ці кошти надіслані.

Особам які потерпіли від онлайн-шахрайства необхідно зібрати всю інформацію, щодо такої події, яка б підтвердила факт вчинення даного кримінального правопорушення. Це можуть бути: активні посилання на веб сайт, знімки з екрану з різних соціальних мереж, квитанції про оплату, виписки з банку про проведений платіж. Також доцільно запросити у банку квитанції списання грошових коштів.

Якщо кошти переведено через платіжну систему на рахунок інтернет-магазину, необхідно негайно повідомити:

службу підтримки відповідної платіжної системи;

адміністратора вебсайту щодо факту вчинення шахрайських дій для блокування сторінки цієї особи.

Звернувшись до адміністрації сайту або технічної підтримки соціальної мережі, платформи купівлі-продажу товарів, повідомити про втрату доступу до акаунту та поінформувати, що натрапили на шахрая.

Отже, За виявленням будь якого онлайн-шахрайства необхідно не зволікати, а заблокувати банківську картку скориставшись додатком або зв'язатися з банком. Зібрати докази (повідомлення, листування, скріншоти підроблених веб сайтів) та повідомити про шахрайство у поліцію.

Нині виникла необхідність у безперервній просвітницькій роботі через усі засоби масової інформації щодо протидії інтернет-шахрайству. Необхідно постійно оновлювати інформацію про риси онлайн-шахрайств, ситуації-пастки, які створюють зловмисники для ошукання довірливих осіб, про способи вчинення інтернет-шахрайств, видів та особливостей поведінки онлайн-злочинців.

1. Брисковська О.М., Гелемей М.О. Особливості вчинення шахрайства в мережі інтернет в умовах воєнного стану *Київський часопис права* № 3, 2023. С. 174 –180. DOI https://doi.org/10.32782/klj/2023.3.25

2. Шахрайство в Інтернеті, як вберегтися? URL : https://www.ukrinform.ua/rubric-society/3759836-sahrajstvo-v-interneti-ak-vberegtisa.html

3. А. Якобчук Половина українців потрапили на гачок шахраїв у мережі URL : https://slovoproslovo.info/ polovina-ukraintsiv-potrapili-na-gachok-shahraiv-u-merezhi

4. Як протидіяти онлайн-шахрайству: стало відомо, скільки звернень реєструється щоденно на Донеччині URL : https://dn.gov.ua/news/yak-protidiyati-onlajn-shahrajstvu-stalo-vidomo-skilki-zvernen-reyestruyetsya-shchodenno-na-donechchini

5. Фіктивні послуги перевезення: поліцейські Київщини повідомили про підозру чоловікові, який ошукав громадян майже на 100 тисяч гривень URL : https://cyberpolice.gov.ua/news/fiktyvni-poslugy-perevezennya-policzejski-kyyivshhyny-povidomyly-pro-pidozru-cholovikovi-yakyj-oshukav-gromadyan-majzhe-na--tysyach-gryven-5139/

6. Протидія зростанню інтернет-шахрайств URL : https://koda.gov.ua/wp-content/uploads/2023/05/zahyst.pdf

7. Брисковська О.М. Окремі види фінансового шахрайства з використанням мережі інтернет в умовах воєнного стану. *Злочинність і протидія їй в умовах війни: глобальний, регіональний та національний виміри* : матеріали наук.-практ. конф. (Вінниця, 12 квіт. 2023 р.) МВС України, Харків. Нац. ун-т внутр. справ, Кримінол. асоц. України, Наук. парк «Наука та безпека». ХНУВС, 2023. С. 46–49.