Микитчик Андрій Васильович,
доцент кафедри кримінології та кримінально-виконавчого права Національної академії внутрішніх справ, кандидат юридичних наук

КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА СПОСОБІВ УЧИНЕННЯ КІБЕРШАХРАЙСТВА В УКРАЇНІ

Анотація. Досліджуються та аналізуються найбільш розповсюджені види та способи кібершахрайства під час карантинних обмежень в Україні та пропонуються дієві заходи запобігання.

Ключові слова: шахрайство, злочинність, кіберзлочинність, карантин, кримінальне провадження.

Summary. The most common types and methods of cyber fraud during quarantine restrictions in Ukraine are explored and analyzed, and effective prevention measures are proposed.

Keywords: fraud, crime, cybercrime, quarantine, criminal proceedings.

На сьогоднішній день під час карантину в Україні значно підвищився рівень шахрайства в Інтернеті, водночас в цілому рівень злочинності зменшився, також за онлайн-шахрайство, пов'язане з коронавірусом, відкрито 41 кримінальне провадження. [1]

Співробітники кіберполіції спільно зі слідчими провели заходи з виявлення осіб, які використовують пандемією коронавірусу для вчинення шахрайських дій, займаються нелегальною торгівлею засобами індивідуального захисту, медичними виробами та здійснюють протиправну діяльність у кіберпросторі. Загалом проведено 56 санкціонованих обшуків спільно зі слідчими підрозділами Національної поліції під процесуальним керівництвом прокуратури, у Вінницькій, Дніпропетровській, Запорізькій, Івано-Франківській, Львівській, Миколаївській, Одеській, Полтавській, Рівненській, Тернопільській та Чернігівській.

Кіберполіція України заблокувала 157 інтернет-посилань, що використовувались шахраями з метою «наживи» під час пандемії. Також слідчими було виявлено 267 фактів щодо розміщення в інтернеті неправдивої чи провокаційної інформації щодо пандемії коронавірусу. Наразі вже ідентифіковано 152 особи, які цю інформацію розповсюджували [2].

Вважаємо за доцільне проаналізувати найбільш розповсюджені схеми кібершахрайств в Україні під час карантину

1. Фейковий продаж дезинфікуючих засобів, ліків, вакцини, тестів, медичних масок, рукавичок, «антикоронавірусного варення», «дезинфікуючих свічок» тощо. Товари, які рекламуються, можуть бути підробленими або взагалі неіснуючими. Головне – не поспішайте з передоплатою. Робіть її тільки перевіреним продавцям!

2. Виявлення коронавіруса «на районі» Віруси-крадії маскуються під мобільні додатки, які наче вміють у реальному часі відстежувати спалахи коронавірусу на вашій вулиці, місті, країні. Після встановлення такої програми збій відбувається у вашому телефоні або комп'ютері. Файли на пристрої блокуються. Далі злочинці вимагають викуп

3. Шахрайські онлайн-сервіси (курси, розваги, доставка тощо) Онлайн-курси з додаткового заробітку в Інтернет, курси з вивчення іноземних мов, підписки на онлайн-кінотеатри та бібліотеки, онлайн-фітнес та тренування, мобільні застосунки для доставки їжі, ліків та алкоголю, онлайн-консультації сімейного лікаря, психо-вірусолога тощо.

4. Шкідливі посилання на сайти «відстеження COVID-19» Електронною поштою або месенджером від шахраїв надходить інформація про поширення COVID-19 з посиланням на сайт «авторитетної» організації, де є онлайн-карта поширення захворення (наприклад, сайт ВООЗ), а насправді – посилання на фішинговий сайт, який викрадає логіни та паролі.

5. Фішингові сайти оплати комунальних послуг За час карантину значно зросла кількість громадян, що почали сплачувати комунальні послуги онлайн. Відповідно побільшало і шахрайських (фішингових) сайтів, які «працюють» під виглядом платіжних онлайнсервісів, а насправді – викрадають гроші або карткові реквізити.

6. «Вашого близького родича відправили на обсервацію з коронавірусом» Це адаптація під COVID-19 загальновідомої схеми «Ваш родич у неприємній життєвій ситуації». Тепер нічні дзвонарі повідомляють самоізольованим людям, що їхній син, донька чи онук відправлені на обсервацію. Далі шахраї від імені лікарів пропонують спробувати дорогу сироватку та диктують номер картки, на яку потрібно перерахувати кошти.

7. Перевірка даних по кредитам під час карантину Шахраї телефонують громадянам від імені банків або мікрофінансових організацій під легендою «Перевірка даних, щоб уникнути штрафів за невчасну сплату кредитів під час карантину». А насправді – виманюють карткові реквізити, банківські SMS-коди та інформацію для віддаленої ідентифікації у банку.

8. «Пенсійне посвідченя недійсне» – дзвінки з «ПФУ» «Пенсійне посвідчення на час карантину буде недійсним», – кажуть шахраї, телефонуючі і так не нажарт наляканим коронавірусом пенсіонерам. І коли спантеличена жертва «підвисає», пропонують негайно переказати заощадження на нову картку, начебто відкриту на ім'я пенсіонера.

9. Шахрайство у туристичній індустрії Для тих, хто ще до початку пандемії купив путівки, квитки на літак, забронював готель тощо, але не встиг відпочити через спалах коронавірусу та усесвітній

карантин і зараз шукає можливість повернути свої гроші – саме для них відкрилася безліч шахрайських сервісів з «повернення коштів».

10. BEC-атаки: «У нас змінився банківский рахунок» Шахрай під виглядом постачальника звертається телефоном або електронною поштою до співробітника компанії, який відповідальний за оплату товарів, та повідомляє про зміну банківських реквізитів у зв'язку зі спалахом коронавірусу та надає для оплати свої власні реквізити.

11. Вербовка мулів. Мулам приготуватися! Злочинці використовують поточну кризу, вербуючи грошових «мулів» для різних брудних схем з відмивання грошей. Шахраї створили фіктивну організацію Vasty Health Care Foundation і вербують «відмивальників» під прикриттям боротьби з коронавірусом... Схема активно «працює» закордоном, але готуватися потрібно вже і нам[3]

Отже, діяльність щодо запобігання кібешахрайствам має включати в себе заходи віктимологічної профілактики - підвищення рівня цифрової грамотності населення і сприяння в просуванні індивідуальних засобів захисту особистої інформації. Актуальними є поглиблені виктимологічні кримінологічні дослідження кіберзлочинності, спрямовані на виявлення об'єктивних закономірностей, детермінант кіберзлочинності, характеристик окремих типів особистості кіберзлочинців, а також різних аспектів забезпечення кібербезпеки. Таким чином, проведений аналіз дає підстави зробити висновок про те, що проблема запобігання кіберзлочинності є багатогранною і лежить не тільки у законодавчій сфері, а і в технічній і технологічній.

Список використаних джерел

1. Продовження та пом'якшення карантину обговорили на нараді в Офісі Президента. URL: https://www.president.gov.ua/news/prodovzhennya-ta-pomyakshennya-karantinu-obgovorili-na-narad-60757.

2. Кіберполіція викрила мережу шахраїв, які ошукали близько 1000 осіб. URL: https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-merezhu-shaxrajiv-yaki-oshukali-blizko-1000-osib/.

3. Інтерактивна графіка: КОРОНАШАХРАЙСТВО Кіберзагрози під час карантину. URL: https://www.ema.com.ua/wp content/uploads/2020/03/covid-19-infographics.pdf#view=fit.