визнавати існування проблем, відкрито обговорювати їх та разом шукати шляхи безпечного та свідомого використання цифрових ресурсів молоддю.

Список використаних джерел

1. Лисенко І. О. Кібербулінг серед підлітків: психологічні аспекти та сучасні виклики. Київ, 2020. 120 с.
2. Кравченко Т. В. Вплив дистанційного навчання на психосоціальний розвиток учнів. Львів, 2021. 98 с.
3. Ковальчук О. В. Соціальні мережі та онлайн-маніпуляції: ризики для молоді. Харків, 2022. 135 с.
4. Петренко С. В. Форми та методи кібербулінгу: емпіричне дослідження. Одеса, 2021. 110 с.
5. Петрів С. В. Цифрова агресія та соціальні платформи: сучасні тенденції. Київ, 2022. 142 с.
6. Іваненко А. П. Використання молоді в інформаційних війнах: аналіз ризиків. Київ, 2023. 115 с.
7. Кримінальний кодекс України / Верховна Рада України. Київ, 2020.
8. Гончаренко М. О. Профілактика кібербулінгу та правове просвітництво серед учнів. Львів, 2021. 103 с.

Голікова Мілена Олексіївна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Резнік Ю. С., старший викладач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук

ВІКТИМОЛОГІЧНИЙ ПОРТРЕТ ТА МОДЕЛІ ПОВЕДІНКИ ЖЕРТВ КІБЕРЗЛОЧИНІВ

Розвиток інформаційних технологій не стоїть на місці і з кожним днем все глибше входить у всі сфери нашого життя. На сьогоднішній день навіть наймолодший українець має телефон

або планшет із доступом в Інтернет, має месенджери для зв'язку з батьками та доступ до різноманітних онлайн ігор. Не відстає і старше покоління. Зараз зустрічається все менше дідусів і бабусь із кнопковими телефонами, життя заполонили смартфони. Та чи безпечною для усіх є ця повальна цифровізація?

Безперечно, використання цифрових можливостей несе неабияку користь, але й небезпека існує. Згадайте, скільки разів вам доводилось отримувати повідомлення у телеграмі на кшталт «Моя дитина бере участь у конкурсі малюнка, проголосуй за неї за цим посиланням» або дзвінки із повідомлення про виграш, отримати який можливо всього-на-всього продиктувавши пароль з смс. Всі ці, безневинні на перший погляд, дії – ознаки кібератаки на вас та ваші пристрої. Так, це дрібниця у порівнянні з кібератаками на великі підприємства, критичну інфраструктуру або державні бази даних, але ці дрібниці несуть неабияку шкоду – втрачаються персональні дані, дані платіжних систем, відбувається крадіжка коштів або використання персональних даних для оформлення кредитів. Те, що здається дрібницею у масштабах країни, є трагедією для окремої людини.

Для початку розберемось, що таке «кіберзлочин». Відповідно до закону України «Про основні засади забезпечення кібербезпеки України» під поняттям «кіберзлочин (комп'ютерний злочин)» варто розуміти «суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України» [1]. У цьому ж законі знаходимо і значення поняття «кібератака», під якою розуміється «спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) у комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних

систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту» [1].

Незважаючи на те, що сам термін «кіберзлочин» розкрито лише у зазначеному вище законі України, злочинам з використанням кіберпростору присвячено цілий розділ у Кримінальному кодексі України. Йдеться про розділ XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку».

Ціллю будь-якої кібератаки є порушення конфіденційності, а також отримання доступу до інформації, зокрема персональної інформації користувача. Для кібератак часто використовується різноманітне шкідливе програмне забезпечення, яке умовно можна розділити на такі групи:

1. Backdoor – шкідливий програмний код, який встановлюється в систему, щоб надати зловмиснику віддалений доступ. Бекдори зазвичай дозволяють підключитися до комп'ютера з мінімальною аутентифікацією або зовсім без такої і виконувати команди в локальній системі.

2. Downloader – шкідливе програмне забезпечення, єдиною метою якого є завантаження іншого шкідливого програмного коду. Зазвичай встановлюють завантажувачі при першому доступі до системи.

3. Stealer – шкідливе програмне забезпечення, яке збирає інформацію на комп'ютері жертви і, як правило, відправляє її зловмисникові. Як приклад можна привести програми, що збирають хеші паролів, перехоплювачі й кейлогери. Дане ШПЗ використовується для отримання доступу до облікових записів інтернет додатків, таких як електронна пошта або інтернет-банкінг.

4. Rootkit – шкідливе програмне забезпечення, що приховує існування іншого коду. Руткіти зазвичай застосовуються в поєднанні з іншим ШПЗ, таким як бекдор, що дозволяє їм відкрити зловмисникові доступ до системи і ускладнити виявлення коду.

5. Вірус-вимагач (ransomware). Тип шкідливого програмного забезпечення, що блокує доступ до системи або унеможливлює роботу з файлами (часто за допомогою методів шифрування), після чого вимагає від жертви викуп для відновлення вихідного стану.

6. Keylogger – програмне забезпечення, що реєструє кожну дію користувача, наприклад з пристроїв вводу (рух комп'ютерної миші, натиснення кнопок клавіатури). Дозволяє заволодіти даними користувача, що були введені після його встановлення [2].

Однак усі перераховані вище способи кібератак стосуються в першу чергу комп'ютерних мереж та персональних комп'ютерів користувачів великих підприємств чи організацій. У випадку ж коли жертвою кіберзлочину є звичайний пересічний громадянин, найчастіше використовується «фішинг».

Фішингом називають атаку, метою якої є отримання доступу до конфіденційної інформації користувачів – логінів, паролів, платіжних даних тощо. Це досягається шляхом проведення масових розсилок електронних листів або повідомлень в соціальних мережах. Часто це робиться від імені відомих організацій, наприклад банків, або від імені знайомих користувачів. При цьому використовуються технічних засобів і засобів соціальної інженерії, які мають на меті введення в оману авторизованих користувачів і спонукання їх до розкриття персональних даних через створення копій сайтів, повідомлень подібних до легальних і знайомих користувачам.

Фішинг є одним із найпростіших способів отримання персональних даних, розрахований на персональну необережність та неуважність користувача. Фактично, такий «прямий фішинг» змушує користувача абсолютно свідомо ввести свої персональні дані та надати їх зловмисникам.

Беззаперечно, жертвою кіберзлочину може стати кожен, але все ж таки можливо виокремити певні віктимологічні ознаки потенційної жертви. Під віктимністю науковці розуміють уразливість членів суспільства перед злочинними посяганнями за певних ситуацій. Віктимність як явище – це властивість соціального суб'єкта наражатися на небезпеку злочинних посягань за певних обставин, ситуацій або внаслідок дій інших осіб [3, с. 8]. Таким чином, під віктимологічними ознаками варто розуміти такі собі дії, що вчиняє сама жертва, які полегшують можливість злочинцю вчинити злочин.

На мою думку, основними ознаками потенційної жертви кіберзлочину є: необережність, самовпевненість та наївність. Розглянемо кожну із наведених ознак окремо. Необережність користувача зазвичай проявляється у ігноруванні обов'язкових ознак, що вказували б на «реальне», а не «фішингове»

повідомлення. Наприклад, користувач отримує у месенджер повідомлення нібито від банку, але номер телефону – звичайний номер із кодом мобільного оператора, а посилання, на яке необхідно натиснути для того щоб перейти на сторінку банку, відрізняється від справжнього на одну-дві літери у адресі. Окрім того, зазвичай за такими посиланнями знаходяться сайти, на яких відсутній протокол безпеки, що вказує на його незахищеність.

Самовпевненість користувача зазвичай проявляється у випадках, коли користувач самостійно чинить дії із потенційно небезпечним контентом, вважаючи, що його проблема обійде стороною. Необережність часто проявляється при завантаженні файлів із сторонніх ресурсів, або самостійному введенні своїх особистих даних на ресурсах, що пропонують легкі гроші. У таких випадках користувач часто розуміє, що чинить неправильно, але вважає, що він жертвою не стане.

Наївність потенційної жертви кіберзлочину – найзручніша ознака для кіберзлочинця. Потенційній жертві обіцяють певну вигоду, або банально грають на її почуттях для того, щоб у подальшому отримати від неї необхідні дані. На наївності грають повідомлення щодо виграшу або державної допомоги, повідомлення щодо необхідності проголосувати у конкурсі чи пройти опитування.

Окрім того, якщо говорити про вік потенційної жертви, то більш вразливими є або наймолодші користувачі, або люди старшого покоління. Чому? Саме через необережність та певну наївність.

Так, на мою думку, люди похилого віку є більш вразливою ланкою суспільства. Наші люди старшого покоління не завжди обізнані в гаджетах. Вони живуть самі, або їх родичі далеко, та нема кому їм пояснити, як користуватися інтернетом та скільки в ньому потенційних злочинців. Приклад кіберзлочину, направленого на людей старшого віку, може бути повідомлення щодо надання такої собі послуги як Є-допомога. Довіра до назви, що вже не перший рік на слуху та викликає асоціації з державною допомогою, а також часта потреба у додаткових фінансах, спонукає потенційну жертву повірити у реальність такого повідомлення та вчинити всі дії, що необхідні злочинцю.

Іншою вразливою віковою групою є діти та молодші підлітки. Діти є наївними, їх легше вести в оману. Коли їм приходить повідомлення, наприклад, з акаунту їх друзів з

посиланням на ігрову валюту у популярних онлайн іграх (Roblox, Minecraft, Brawl Stars тощо), наївність та довіра не дозволяють їм запідозрити, що за цей акаунт був зламаний, а пропозицію щодо безкоштовної вигоди їм надає шахрай. Підлітки вже не такі наївні, тут більше грає зухвалість, віра в те, що вони будуть хитрішими. І навіть при наявності підозри щодо того, що посилання надійшло від шахрая, зухвалість спонукає перейти і подивитись, що буде далі.

Таким чином, відповідно до зазначеного вище, можна зробити наступні висновки. Найпопулярнішим кіберзлочином та методом кібершахрайства є «фішинг».

Віктимологічний портрет жертви кіберзлочину має такі ознаки: необережність, самовпевненість та наївність. А найбільш вразливими віковими групами є люди старшого покоління, діти та молодші підлітки.

Відповідальність за те, щоб не стати жертвою кіберзлочину лежить на кожному з нас особисто, тобто кожному треба слідкувати як і що він робить щоб не стати жертвою кіберзлочину. Загальні рекомендації залишаються незмінними: не переходити за невідомими посиланнями, перевіряти файли, які ви хочете завантажити, перевіряти протоколи безпеки на сайтах, на які заходити та не вводити особисті авторизаційні або платіжні дані на підозрілих сайтах. Краще тричі перевірити, аби потім не стати жертвою шахрая.

Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. Бикова Т. М., Гомон В. О., Голікова О. В. Розповсюдження шкідливого програмного забезпечення з метою отримання доступу до інформаційних систем. *Шкідливі програми як загроза об'єктам критичної інфраструктури в умовах кібервійни* : збірник матеріалів міжвідомчого круглого столу (Київ, 21 лют. 2023 р.). Київ : ІСТЕ СБУ, 2023. С. 24–28.

3. Головкін Б. М. Віктимність як основна категорія віктимології. *Журнал східноєвропейського права*. 2015. № 20. С. 6–13.