

ОРЛОВ РОМАН РУСЛАНОВИЧ

Магістр Харківського національного університету внутрішніх справ, старший інспектор 2-го відділу (протидії різновидам онлайн шахрайств) управління протидії кіберзлочинам у м. Києві Департаменту кіберполіції НП України,

ОКУШКО АНДРІЙ ВАСИЛЬОВИЧ

Кандидат юридичних наук, заступник начальника – начальник 2-го відділу (протидії різновидам онлайн шахрайств) управління протидії кіберзлочинам у м. Києві Департаменту кіберполіції НП України.

**РІЗНОВИДИ ОНЛАЙН ШАХРАЙСТВ ТА МЕТОДИ ПРОТИДІЇ
ЗЛОЧИНАМ У МЕРЕЖІ ІНТЕРНЕТ**

Сучасний світ відзначається стрімким розвитком інтернет-технологій, що дозволяє нам здійснювати онлайн-покупки, спілкуватися з друзями, отримувати освіту та вирішувати безліч інших завдань зручно та швидко. Проте разом із цим росте й загроза онлайн шахрайства, яка впливає на життя громадян та стан безпеки в цифровому просторі. Україна, як і багато інших країн, стикається із серйозною проблемою цього виду злочинності.

Стан онлайн шахрайства в Україні є предметом серйозної турботи та дослідження, оскільки ця проблема має потужний вплив на різні сфери суспільного життя. Зловмисники, використовуючи різноманітні методи та технології, вчиняють різні види кібершахрайства, яке може призвести до серйозних фінансових втрат, порушень конфіденційності та інших негативних наслідків. Онлайн шахрайства в Україні мають серйозний вплив на різні сфери життя, включаючи громадян, бізнес і суспільство загалом. Для громадян це може загрожувати:

Фінансовими втратами, а саме громадяни України стають жертвами онлайн шахраїв, які можуть вивести гроші з їх банківських рахунків, шахрайством через електронну комерцію, фейковими інвестиціями тощо. Це

може призвести до серйозних фінансових труднощів; Порушення приватності, а саме використання соціального інженерінгу та інших методів шахрайства може призвести до витоку конфіденційної інформації громадян, включаючи особисті дані та ідентифікаційну інформацію; Психологічний вплив, а саме жертви шахраїв можуть відчувати стрес, тривогу та невпевненість у власних діях. Вони можуть втратити довіру до інтернету та електронних технологій.

Для суспільства загалом, це може загрожувати економічними наслідками, а саме загальні фінансові втрати внаслідок онлайн шахрайства можуть негативно вплинути на економіку країни, включаючи зменшення інвестицій та економічний розвиток; Загроза національній безпеці, а саме кібершахраї мають потенціал завдати шкоди національній безпеці, використовуючи кібератаки та шпигунство; Спад віри в інтернет, а саме зростання кількості онлайн шахрайств може призвести до втрати довіри до інтернету та електронних послуг, що може вплинути на розвиток цифрової сфери суспільства.

На період військового часу, і в повсякденному житті, найрозповсюдженішими видами онлайн шахрайства є:

1. Фішинг - це вид шахрайства, коли атакувачі намагаються отримати конфіденційну інформацію, таку як паролі або фінансові дані, представляючи себе як надійний джерело, часто шляхом електронних листів або веб-сайтів.
2. Соціальний інженерінг - шахраї використовують маніпуляцію та психологічні техніки, щоб отримати інформацію від потенційних жертв, таких як військовослужбовці та члени їхніх родин.
3. Мальвара та віруси - ворожі програми (мальвара) використовуються для отримання доступу до інформації на комп'ютерах або мережах. Вони можуть поширювати шкідливі віруси, шпигунське програмне забезпечення та інші загрози.
4. Фейкові новини та дезінформація - вороги можуть розповсюджувати дезінформацію, що може призвести до паніки або внутрішньої дестабілізації в умовах військового конфлікту.

5. Кібершпигунство - військовослужбовці можуть стати метою шпигунства через витік інформації, яка може завдати шкоди національній безпеці.

Бути обізнаними щодо видів шахрайств є замалим для протидії даним злочинам, потрібно знати головні методи боротьби з онлайн шахрайствами, а саме:

1. Захист інформації - важливо застосовувати міцне шифрування для захисту конфіденційної інформації та регулярно оновлювати системи безпеки.
2. Освіта і тренування - проводити навчання для військовослужбовців та персоналу щодо впізнавання та запобігання онлайн шахрайству.
3. Моніторинг мережі - слід постійно моніторити мережі на наявність шкідливого програмного забезпечення та незвичайні активності.
4. Співпраця з іншими організаціями - важливо співпрацювати з іншими агентствами, в тому числі іншими військовими підрозділами та кібербезпечними партнерами.
5. Створення кризового плану - розробити план відповіді на кібератаки та інші подібні загрози.

Це лише загальний огляд і не враховує всіх можливих аспектів боротьби з онлайн шахрайством в умовах військового стану та в повсякденному житті. Деталізація та розробка конкретних стратегій залежать від конкретної ситуації та потреб.

Узагальнюючи, протидія онлайн шахрайству - це завдання, яке вимагає поєднання технічних рішень, освіти та співпраці між всіма суб'єктами. Лише шляхом об'єднаних зусиль ми можемо забезпечити більш якісну кібербезпеку, захист інтересів громадян і підприємств у цифровому світі.