Головне територіальне управління юстиції в Івано-Франківській області

Інтернет - шахрайство

Івано-Франківськ
травень, 2015

Шахрайство є одним із найпоширеніших злочинів, що характеризується вчиненням злочинного діяння проти власності.

Одним із видів шахрайства є Інтернет – шахрайство, яке можна визначити як - заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою, вчинене в (або з використанням) всесвітньої комп'ютерної мережі, що надає доступ до різноманітних інформаційних ресурсів.

Найбільш популярними способами обману через Internet є:

онлайн-аукціони: це не доставка купленого товару після сплати за нього покупцем грошей. Тобто, покупець обирає товар, заповнює анкету, яка створює ілюзію справжності угоди, сплачує вартість обраного товару плюс доставку, але товару він не отримує. Існує зворотна ситуація, коли замовляється товар чи послуга через Інтернет по фальшивій кредитній карті;

фальшиві рахунки на оплату з Інтернет-магазинів - підроблені рахунки, що розсилаються по e-mail, містять посилання на шкідливі програми. Одержувач, який відкрив рахунок, негайно стає жертвою зловмисних дій;

шахрайський Інтернет - магазин: шахрай відкриває такий магазин, за вигідними цінами пропонує товар, отримує передоплату, а після цього зникає, привласнивши гроші;

фішинг: вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказування або обміну валюти, Інтернет-магазинів. Шахраї використовують різні виверти, які найчастіше змушують користувачів самостійно розкрити конфіденційні дані - наприклад, посилаючи електронні листи із пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на веб-сайт в Інтернет, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів;

крадіжка послуг - правопорушення з отримання несанкціонованого доступу до будь-якої системи, щоб безкоштовно скористатись її послугами;

підроблені сайти благодійних фондів: Інтернет злочинці - неперевершені майстри викликати жалість і грати на людських трагедіях. Особливо актуальними такі методи відбирання грошових коштів стають у святковий сезон, коли відвідувачі мережі більш охоче розлучаються з грошима;

"гарячі" путівки: туристична фірма пропонує "демпінгові" ціни на висококласні тури, а насправді продає дуже дешеві пакети послуг, які зовсім не відповідають описам і фотографіям на сайті;

фінансові піраміди: це організація, членство в якій набувається за умови внесення певних платежів, внесків чи іншої оплати і дозволяє отримувати прибуток членам організації в залежності від кількості залучених ними учасників. Як правило, організатори фінансової піраміди обіцяють високі прибутки, які неможливо підтримувати тривалий час, а погашення зобов'язань піраміди перед усіма учасниками є практично неможливим;

пропозиції щодо працевлаштування: «роботодавець» пропонує роботу та надсилає чіткі інструкції щодо її виконання, а також, наприкінці листа вказує, що приступити до роботи ви зможете, тільки оплативши яку-небудь послугу, наприклад, атестат Webmoney;

злам webmoney гаманців: отримання електронного листа з повідомленням приблизно наступного змісту: «Шановний користувач webmoney, я, вивчаючи систему захисту електронних гаманців, встановив, що вона має значний недолік. Мною був створений гаманець, переславши гроші на який ви отримуєте їх у два рази більше». Далі пропонується номер гаманця на якій слід направити кошти та інформація про строки їх повернення. Для більшого введення в оману, зловмисники часто в зворотній адресі вказують якщо не справжні електронні адреса адміністрації Webmoney, то, принаймні, зовні схожий на останній;

лист від виробника операційної системи: на електрону адресу приходить лист від імені виробника вашої операційної системи (наприклад – Microsoft.com). Зміст листа короткий, здебільшого, про захист ваших прав та вашого комп'ютера, та адресує вас на файл, що додається до листа. При спробі відкрити файл на моніторі з'являється вікно в якому міститься текст про необхідність надіслання СМС на короткий номер для отримання «ключа активації»;

повідомлення від друга: на сторінку користувача соціальної мережі приходить повідомлення від імені його знайомого (друга), при цьому зміст таких повідомлень дуже варіативний – від прохання відправити СМС для підвищення індивідуального рейтингу, до повідомлення про те, що ваша сторінка була зламана, ви розсилаєте «спам» та вам необхідно відправити СМС (чи перевести електроні кошти) для поновлення вашої сторінки та ін.;

Інтернет-кардинг - використання даних з чужої банківської картки для здійснення різних операцій у мережі з метою отримання грошей.

Деякі поради, щоб не стати жертвою Інтернет - шахраїв:

1. Не довіряйте усій інформації, що розміщена в Інтернеті.
2. Ніколи не здійснюйте операцій по картках за допомогою електронних платіжних систем у магазинах, яким не довіряєте або які бачите вперше. Особливо, якщо на них немає логотипів платіжних систем, та інших організацій, які борються із шахраями.
3. У разі покупки товарів через мережу Інтернет, рекомендується здійснювати переказ коштів лише на банківські рахунки або розраховуватись зі службою доставки. Також, рекомендується завести спеціальну картку саме для Інтернет-розрахунків.
4. Подбайте, щоб завжди був включений ваш брандмауер і регулярно оновлюйте операційну систему, антивірусні та інші програми.
5. Остерігайтесь електронної пошти чи миттєвих повідомлень з невідомого джерела, особливо якщо вони містять якісь посилання або запит про особисту інформацію, наприклад підтвердження пароля.
6. Вводіть паролі, які важко вгадати. Періодично змінюйте їх та не використовуйте один пароль для різних облікових записів.
7. Надавайте банківські дані чи дані про свою кредитну картку лише надійним і захищеним веб-сайтам.
8. Часто й уважно перевіряйте виписки з банківського рахунку і те, які операції було здійснено з вашою кредитною карткою. Виявивши незнайому вам операцію, негайно зв'яжіться з банком.
9. Регулярно перевіряйте стан свого рахунку як у платіжній системі, так і на картці. Якщо у вашому банку є послуга СМС-повідомлення – обов'язково підключіть її, тому що це найшвидший спосіб одержати інформацію про здійснення операцій із вашими коштами.
10. Переконайтеся, що ви правильно вписали адресу веб-сайту, особливо якщо це сайт фінансової установи. Лише через одну помилку можна потрапити на сайт шахраїв.
11. Будьте обережні, послуговуючись незахищеним бездротовим з'єднанням (Wi-Fi), оскільки шахраї можуть вкрасти ваші дані і переадресувати вас на фальшивий сайт.
12. На запитання «Запам'ятати цей пароль?» відповідайте «ні», оскільки троянські програми можуть збирати ваші збережені паролі.