Кузьміна А. - курсант 1 курсу факультету підготовки фахівців для органів досудового розслідування;
Мирошниченко В.О. – науковий керівник, професор кафедри економічної та інформаційної безпеки, кандидат технічних наук, доцент (Дніпропетровський державний університет внутрішніх справ)

ФІНАНСОВЕ ШАХРАЙСТВО В СОЦІАЛЬНИХ МЕРЕЖАХ

Привабливість інтернет-магазинів важко недооцінити: багатий вибір, демократична ціна, доставка до дверей. У сучасних магазинах соціальної мережі можна знайти все, що завгодно за ціною нижче, ніж у звичайних магазинах. Ми настільки довірливі, тому можемо купувати в Інтернеті, але часто стаємо неуважними, чим і користуються шахраї. За інерцією довіряємо всім магазинам незалежно від його пізнаваності і наявності відгуків.

Зазвичай схема така: створюється один сайт, на якому викладаються товари однієї номенклатурної ознаки. Наприклад, дитяче взуття певної торгової марки. Ціна на запропоновані товари зазвичай нижче середньо ринкової. На такому сайті немає ні відгуків, ні привабливого дизайну. Тільки небагато інформації і, можливо, фільтр для зручного пошуку. Контактні дані заповнені теж дуже бідно.

Працюють такі інтернет-магазини найчастіше по 100% передоплаті. Покупець вибирає товар і потім оплачує його. Після чого протягом зазначеного терміну очікує відправку товару. Звичайно ніхто замовлення нікуди відправляти не буде. Зателефонувавши за вказаним телефоном, покупець виявить, що він не обслуговується, або просто не беруть слухавку.

Буває так, що в умовах передбачена можливість оплати за фактом отримання товару. У цьому випадку після оформлення замовлення, покупцеві на контактний E-mail або телефон приходить повідомлення, що в разі передоплати доставка безкоштовна (або інформація про інші вигоди). При цьому часто для оплати скидається не банківські реквізити, а номер електронного гаманця і після отримання грошей псевдопродавець зникає.

Також широко розповсюджені в Інтернеті схеми шахрайства з роботою. Варіантів маса, а найпоширеніші такі:

1. Пропонують виконати роботу, наприклад, написати текст, створити картинку, змонтувати відео. Отримують результат і не оплачують його.

2. Пропонують високий стабільний дохід за декілька годин, наприклад, розміщення реклами. Після тижнів старанної праці працівник отримує замість обіцяних коштів кілька сотень гривень. Це пояснюють по-різному: тільки почав, далі буде більше, не дотримана будь-яка умова, мало переходів по посиланнях і так далі. Так триває до того, поки людина не зрозуміє, що його обманюють.

3. Пропонують роботу з хорошою оплатою, але спочатку потрібно

зробити страховий внесок на той випадок, якщо ви не виконаєте роботу в строк та замовник не отримає результат. Те ж саме відбувається і зі збором ручок на дому. Потрібно заплатити за ручки, які вам надішлють за вказаною адресою. Звичайно ж, нічого ніхто надсилати не буде. Зробите внесок, і ваш дуже товариський і доброзичливий роботодавець вмить зникне.

Є й інший варіант обману. Шахрай дзвонить людині, яка є клієнтом будь-якого банку, і повідомляє, що у неї є заборгованість по кредиту і почала нараховуватися пеня. На що чує відповідь, що ніякого кредиту немає і, мабуть, помилка. Тоді дуже ввічливий «співробітник банку» просить уточнити особисті дані, щоб перевірити наявність заборгованості. А перелякана помилковим боргом людина, не замислюючись, повідомляє все, що у неї просять. Після чого з її рахунку зникають всі гроші. Пропозицій, під якими просять повідомити особисті дані, може бути дуже багато і звучать вони дуже правдоподібно. Навіть якщо карту, рахунок, аккаунт заблокують, клієнт завжди може зняти блокування при особистому візиті у відділення банку.

Щоб не бути обдуреними в Інтернет, можна порадити наступне:

- Не сприймати будь-яку отриману інформацію, як істину в останній інстанції. Перш ніж реагувати, треба задуматися, чи схоже це на правду. Ставте під сумнів навіть повідомлення в соціальних мережах, які ви отримали від друзів. Їх акаунт могли зламати.
- Не вірити обіцянкам величезної вигоди. Це стосується пропозицій заробити мільйони, віддавши пару тисяч гривень, і сенсаційних знижок. Всі знижки – це добре продуманий маркетинговий хід. Жоден продавець не стане віддавати товар нижче собівартості.
- Розголошувати особисті дані без реальної потреби. Досвідчені шахраї навіть мінімум інформації можуть перетворити на власну вигоду.
- Не реагувати на повідомлення і дзвінки з незнайомих номерів на фінансові пропозиції. Шахраї викликають сильні емоції для того, щоб було легше виманити жадані гроші.
- Бути пильними. Навряд чи можна перерахувати всі способи, як можуть обманювати в Інтернеті. Тільки уважність і недовіра до тих, хто просить, переконує і пропонує, зможе по-справжньому вберегти від шахраїв.

Варто відзначити, що шахрайство в Інтернеті – це діяльність, якою часто займаються люди, які володіють певними навичками. Наприклад, талановиті програмісти, хакери, колишні співробітники банків. Тобто їм для зняття грошей потрібно отримати мінімум інформації. Тому не варто особливо покладатися на те, що логін, пароль, підтвердження на телефон або пін-код вас по-справжньому убезпечать. Вони рятують від шахраїв-аматорів, а від профі вбереже тільки уважність. У випадку Інтернет - шахрайства завжди необхідно звернутися до спеціального відділу у структурі МВС України, який займається злочинами в Інтернет просторі [1].

Використані джерела:

1. Офіційний сайт кіберполіції України. - [Електронний ресурс]. − URL: https://cyberpolice.gov.ua.