Пять важных правил,
как не стать жертвой преступников в социальных сетях

Взлом аккаунта, спам, вымогательство, «липовые» интернет-магазины, хищения с банковских карт – подсказываем, как избежать этих и других опасностей.

В тройку самых популярных соцсетей входят Вконтакте (70,4% опрошенных), Instagram (43,6%) и Facebook (29,1%). Незначительно от лидеров отстает социальная сеть Одноклассники (27,9%), а вот аудитория Twitter и Linkedin, согласно социальному опросу, в разы меньше - 10,3% и 3,2%, соответственно.

Социальные сети «лишают» нас одиночества и скуки – там всегда есть с кем поговорить, можно обсудить только что вышедший фильм, похвастаться подарком, купить практически все, что угодно, но иногда и попасть в беду.

Около 20% пользователей заявляют о том, что сталкивались с проблемами безопасности данных в социальных сетях. Чаще всего, это проблемы кражи пароля (26%) и взлома аккаунта (69,2%). При этом, чуть более 23% опрошенных отметили, что при взломе мошенник выдавал себя за них и пытался выманить деньги у их друзей. Однако имеют место и другие проблемы, например, кража пароля от электронной почты, к которой привязан аккаунт в социальной сети (15,6%), и кража денежных средств с банковской карты, также привязанной к аккаунту (3,5%).

Несмотря на то, что продажа товаров и услуг в социальных сетях является несанкционированной, более половины опрошенных заявили о том, что делают там покупки регулярно или периодически, и лишь 18% пользователей считают это небезопасным.

По законодательству любая, будь то онлайн или офлайн, покупка должна сопровождаться выдачей кассового чека или публичной офертой. Однако более 40% респондентов отметили, что чек при покупке товара в социальных сетях им выдан не был.

По данным опроса около 4% пользователей сталкивались с мошенничеством при осуществлении покупок в соцсетях лично, чуть менее 37% заявили, что такие проблемы возникали у их знакомых.

Подобные жалобы на мошеннические паблики, выдающие себя за интернет-магазины поступают и на Горячую линию Рунета *(Рунет – русскоязычный Интернет)*, составляя около 20% обращений, касающихся проблем, возникших в социальных сетях.

Примеры обращений на Горячую линию Рунета,
раздел «Социальные сети»

1. Спам-рассылка, мошенники

«Присылают такой текст: Здравствуйте! Рады сообщить, что вы победили в конкурсе, и выиграли iPhone 6! Свяжитесь с менеджером (страница в соцсети), и получите ваш приз в ближайшее время! Доставка бесплатная! После обращения к менеджеру тот присылает 2 фотографии, на которых указаны реквизиты для перевода 425 рублей, как за доставку».

2. Мошеннические интернет-магазины

«Группа мошенников. Отправила предоплату в размере 4800 руб. за вещи. С того момента мне никто не отвечает. Списалась с несколькими девушками из числа состоящих в группе, они тоже стали жертвами этой группы. Вот ссылка девушки, которая руководит группой (ссылка на страницу в соцсети)».

3. Единичные мошенники. Продажа товаров\услуг

«В пятницу заказала у девушки через интернет обувь. Диалог был прекрасен поначалу,все рассказывала, как оплатить ,через что оплатить, я оплатила по ее требованиям 50% суммы покупки,в понедельник, сказали, будет отчет ,что мне по почте отправит посылку, и покажет фотографию чека, я написала в понедельник личное сообщение этой девушке, отправили мне или нет обувь, мне не ответили, и заблокировали... я так думаю, меня обманули....»

4. Взлом аккаунта

«Взломали мою подругу и требуют деньги у ее друзей».

5. Мошеннический паблик

«В социальной сети (адрес паблика в соцсети) создан паблик под названием «Бесплатный», где люди за репост их записей получают бесплатные подарки. На днях мне пришло сообщение от менеджера сайта о том, что я выиграла телефон и мне предоставили выбор – телефон или денежный эквивалент. Я выбрала деньги, меня попросили создать киви кошелек и оплатить комиссию от суммы телефона в размере 1200 рублей. После того, как я это сделала, деньги на счет мне не поступили, на что менеджер этой группы сказал, что в киви произошел сбой и они отправят мне деньги еще раз с возмещением комиссии. Деньги, естественно, мне не поступили, а человек, который мне писал, неохотно отвечает и пишет полную ерунду, что ждите, комиссия вам вернется».

6. Противоправный контент

«Здравствуйте, организация Фонд «Безопасный дом» просит вас

разобраться с противоправным контентом, размещенным в социальной сети (адрес соцсети) по указанной ссылке. В ходе изучения контента возникло подозрение, что указанный человек под прикрытием тренингов по пик-апу и др. вовлекает женщин и несовершеннолетних лиц в проституцию, а также совершает сексуальное насилие над женщинами, размещая фото и видео в социальные сети и YouTube».

Помочь справиться со всеми этими проблемами призваны официальные службы поддержки пользователей социальных сетей. Однако не все знают, куда именно нужно обратиться. Около 5% пользователей, у которых возникали проблемы, не смогли найти необходимые контакты. По мнению 28% опрошенных, многие пользователи, попавшие в беду, просто не могут разобраться с техникой подачи заявления.

Зная об этом, мошенники пользуются ситуацией, создавая «фейковые» службы поддержки, стараясь выманить у и без того обиженных, пользователей персональные данные. Поэтому многие предпочитают решать проблемы самостоятельно, опасаясь кражи (15,9%) и разглашения своих персональных данных (19%).

В связи с этим, авторитет служб поддержки в глазах пользователей невысок. За помощью к ним обращались около 32% опрошенных, а вот решить проблему самостоятельно старался практически каждый второй. Но сомневаться в эффективности служб поддержки не стоит. Около 63% обратившихся, сумели решить свою проблему.

Столкнуться в социальных сетях возможно не только с мошенниками, но и с более опасными преступниками.

Случай с похищением сына известного российского предпринимателя показал, что бездумное распространение сведений о себе в социальных сетях может дорого обойтись вам или вашим родным. Возможно, вы не являетесь известным бизнесменом, но стать жертвой преступников, которые из поста «ВКонтакте» знают, что с 1 по 15 числа вы всей семьей будете «греться на солнышке в Египте» вполне возможно.

Отсюда следуют правила:

- Меньше конкретных данных о своей жизни.
- Не публикуйте информацию, по которой можно определить ваш домашний адрес и время, когда там никого не бывает.
- Не размещайте в общем доступе посты о дорогостоящих покупках или сделках, в результате которых можно сделать вывод о наличии у вас крупной суммы денег или ценностей, которые можно перепродать.
- Не описывайте свой постоянный маршрут, пролегающий между домом и работой – нападения с целью ограбления не всегда бывают случайными.

- Если очень хочется поделиться радостью от начинающегося отпуска, добавьте к сообщению приписку о включенной охранной сигнализации (даже если это не правда) – это наверняка отпугнет «продвинутых» любителей легкой наживы.

Для того чтобы обезопасить себя от интернет-мошенников рекомендуется соблюдать пять важных правил:

1) создать уникальный надежный пароль,
2) не разглашать персональные данные,
3) контролировать личную информацию,
4) не осуществлять покупки в социальных сетях,
5) в случае покупки товара не осуществлять предоплату.

Список официальных служб поддержки пользователей в социальных сетях:

ВКонтакте:
- Задать вопрос
- Помощь по сайту
- Популярные вопросы

Фейсбук:
- Справочный центр
- Помощь по смене пароля
- Помощь по возврату аккаунта
- Сообщить о нарушениях

Одноклассники:
- Служба поддержки
- Форма подачи жалобы

Инстаграм:
- Справочный центр

Твиттер:
- Справочный центр
- Сообщить о нарушениях

Linkedin:
- Служба поддержки

Также обязательно оставьте заявление на Горячей линии Рунета. Потому что ваше обращение может быть не единичным случаем, а массовым мошенничеством. Тогда вы поможете не только себе, но и многим другим пользователям Интернет.