**10 способов мошенничества в интернете**



Человек так устроен, что ему всегда кажется: плохое может произойти с кем угодно, но только не с ним. И махинации в Сети здесь не исключение. Даже тот, кто однажды попал на удочку аферистов, все равно уверен: теперь-то он осторожен и больше этого никогда не произойдет. Но мошенники очень изобретательны, и потому люди снова и снова попадаются в расставленные ловушки.

**1. «Проверка реквизитов»**

Кажется, что никто в здравом уме не станет сообщать мошеннику информацию о своем банковском счете или реквизиты своей карты. Но мошенники все равно обманом получают доступ к чужим деньгам.

Очень популярной схемой является телефонный звонок от «сотрудника банка». Клиента могут попросить назвать реквизиты банковской карты («для проверки») или подтвердить зачисление денег на счет при помощи смс-пароля. Правда, после подтверждения оказывается, что сумма, указанная в сообщении, была не зачислена, а списана со счета клиента!

Под любым предлогом мошенники могут попросить человека предоставить данные о сроке окончания действия карты и CVV-код. Дальше – дело техники: этой картой можно расплачиваться в Сети.

**2. «Подтверждение перевода»**

Эта схема, как правило, используется псевдопокупателями, промышляющими в интернете. Мошенник звонит продавцу, интересуется товаром и предлагает выслать деньги на карту.

Дальше схема такая: мошенник говорит, что отправил деньги, но продавцу нужно подтвердить перевод, поскольку деньги идут из другой платежной системы. Продавца просят подъехать к банкомату и дают ему подробные инструкции, что и как делать. И нередки случаи, когда под предлогом подтверждения перевода невнимательный продавец, получающий инструкции от мошенника в режиме реального времени, отправлял ему все деньги со свой карты.

**3. Фишинг.**

Цель фишинга - получить ваши секретные данные: пароли доступа, PIN-код кредитной карты и т.д. Вам может прийти е-мейл или смс-сообщение «от банка» о взломе аккаунта, о закрытии вашей карты или об опасном вирусе. И для того, чтобы избежать всех этих напастей, предлагают прислать свои пароли.

Совет однозначный: никогда и никому не сообщайте свои пароли, PIN-коды и прочую секретную информацию. Помните: сотрудники банков никогда не просят назвать им эти данные.

**4. Ловушки от продавцов**

Немало мошенничеств связано с популярными досками объявлений в интернете. Схемы от продавцов стары как мир – просто удивительно, как люди умудряются раз за разом на них попадаться.

Итак, продавец перед отправкой товара почтой просит аванс, а то и вовсе 100%-ную предоплату. После получения денег исчезает навсегда: не выходит на связь, отключает телефон, удаляет аккаунт.

Вторая популярная схема заключается в том, что покупателю отправляется бракованный товар. Причем наложенный платеж не спасет, ведь немало товаров (запчасти, комплектующие и т.д.) нельзя проверить на наличие брака на почте.

**5. Гороскоп на заказ**

В интернете есть масса объявлений, предлагающих заказать персональный гороскоп. Выслать его обещают быстро и бесплатно, но для этого нужно заполнить стандартную анкету: имя, фамилия, дата рождения, электронный адрес.

После заполнения анкеты любителю астрологии приходит письмо с условием: чтобы получить заказ, надо отправить по указанному номеру смс-сообщение с определенным набором цифр. Надо ли говорить, что сразу после отправки со счета клиента списывается определенная сумма?

После этого есть два варианта развития событий: либо заказчику действительно тут же высылают гороскоп (правда, такая скорость вряд ли может говорить о его уникальности), либо ничего не присылают. Но в любом случае это обман.

Кроме того, в качестве бесплатного бонуса на почтовый ящик заказчика еще долго будут приходить «заманчивые предложения».

**6. Любителям фриланса**

Искусством наживаться на безработных отечественные мошенники овладели задолго до появления интернета. А теперь просто перенесли сюда свои незамысловатые схемы.

Итак, аферист размещает объявление о том, что требуется, например, наборщик текстов. После заполнения анкеты, человек получает письмо из «издательства». Мол, работа заключается в перепечатке рукописных текстов. Но для того, чтобы этот текст получить, нужно заплатить определенную сумму. Сумма чаще всего символическая: 20-50 грн. Видимо, мошенники понимают, что здесь особо не разгуляешься. Но, как говорится, с миру по нитке…

Также в Сети есть различные биржи, где один человек может заказать работу другому. Немало обманов связано с тем, что заказчики не платят. Иногда мотивируют тем, что работа сделана некачественно, а иногда и вовсе без объяснений.

Избежать этого способа мошенничества с большой долей вероятности можно, изучив информацию о заказчике и отзывы. И если вы видите, что человек зарегистрировался неделю назад, а отзывов о нем либо нет, либо негативные, от сотрудничества лучше воздержаться или работать по частичной предоплате.

**7. Выиграй смартфон**

У интернет-магазинов сейчас тяжелые времена, но все же это не повод для надувательства. А здесь оно тоже встречается.

Например, интернет-магазин объявляет розыгрыш крутого смартфона. Но для участия в акции нужно купить какой-то товар – например, чехол для телефона или наушники – потому что розыгрыш проводится среди покупателей. Вполне возможно, что кому-то из покупателей «с улицы» и удавалось что-то когда-то выиграть, но мы таким данными не располагаем.

**8. «Бесплатное» скачивание**

Скачивать из интернета сейчас умеют все. Работы немного: найти через поисковик нужную программу, книгу или другой информационный продукт и нажать на большую кнопку «Скачать бесплатно». Но тут вас может ждать сюрприз: после нажатия кнопки выясняется, что вам нужно ввести номер телефона и нажать «Продолжить».

После этого перед юзером появляется следующая информация: для того, чтобы скачать программу бесплатно, нужно ответить на смс с каким-нибудь вопросом – в каком городе живете или сколько вам лет. Понятно, что смс вам выльется в круглую сумму.

Разновидность этого способа мошенничества может завести чуть дальше: скачать файл получилось, но смс придется отправить, чтобы разархивировать архив.

Тут важно помнить: отправляя смс-сообщение, вы рискуете потерять все деньги со счета. Так что делать этого не стоит.

**9. «Победитель» лотереи**

Наверное, трудно найти человека, которому хоть раз в жизни не пришло бы сообщение о том, что он выиграл в лотерею или победил в конкурсе. Но чтобы получить свой подарок, вы должны отправить небольшую сумму за пересылку. Естественно, после отправки денег никакого подарка «выигравший» не получает.

Если вы участвовали в конкурсе и действительно выиграли, подарок отправляют за счет компании. Ни о каких «деньгах наперед» не может быть и речи!

**10. Деньги за информацию**

Сейчас в интернете популярен такой способ заработка денег, как информационный бизнес. Ушлые авторы предлагают всевозможные методики – от «как удачно выйти замуж» до «как заработать миллион, не вставая с дивана».

А еще здесь продается масса чудодейственных средств, которые «помогут похудеть» за 2 дня или «накачать мышцы» за неделю.

Здравый смысл подсказывает, что вестись на это не нужно. Вполне возможно, что за ваши деньги вам пришлют какую-нибудь инструкцию или видеокурс. Но из них вы узнаете то, что знали и до этого: чтобы заработать реальные деньги, нужно работать, чтобы накачать мышцы – не вылезать из спортзала, а чтобы похудеть – меньше есть и больше двигаться.