

**Чтобы снизить риск быть обманутым в сети «Интернет», рекомендуем следовать следующим правилам:**

1. **Не доверяйте** непроверенным сайтам знакомств, заработка, азартных игр, лотерей, тотализаторам.

2. Если на сайте нет юридического адреса, контактных телефонов, обратной связи, то **не предоставляйте** свои персональные данные, банковские сведения.

3. **Не направляйте** SMS-сообщения на короткие номера, указанные в инструкции по разблокировке и защите от вирусов.

4. **Создавайте** сложные пароли там, где есть доступ к Вашим данным и денежным средствам, **пользуйтесь** обновляемой проверенной антивирусной программой.

5. При совершении покупок в сети «Интернет» предварительно **ознакомьтесь** с информацией о магазине, отзывами о его работе, инструкцией по возврату и обмену товара. Обратите внимание на дату создания сайта по дате регистрации домена.

Проверить данные об организации можно на сайте Федеральной налоговой службы России, используя ИНН и ОГРН. Помимо этого, следует с помощью поиска посмотреть «черный список интернет – магазинов».

6. Будьте **аккуратны и внимательны** при работе с электронными кошельками и банками-клиентами на сомнительных сайтах, а также при проведении операций на чужих компьютерах.



**Прокуратура Кировской области**  
610000 г. Киров, ул. Володарского, д. 98  
«Телефон доверия»: 8(8332) 38-11-53  
E-mail: [prokuror@oblast.kirov.ru](mailto:prokuror@oblast.kirov.ru)

**Общероссийская  
общественная организация  
АССОЦИАЦИЯ ЮРИСТОВ РОССИИ**  
**Кировское региональное отделение**  
г. Киров, ул. Дерендяева, 23, к.108  
тел./факс (8332) 64-98-11  
E-mail: [info@alrf43.ru](mailto:info@alrf43.ru)

*Прокуратура Кировской области*

\*\*\*

*Кировское региональное отделение  
Общероссийской общественной  
организации*

*«Ассоциация юристов России»*



**Будьте бдительны!  
Мошенничество  
в Интернете**



Киров

2019

## **Мошенничество в сети «Интернете»**

Жертвами мошенников в сети «Интернет» становятся не только начинающие пользователи, но и юридически грамотные люди.

Основными признаками того, что Вас пытаются обмануть, являются очень заманчивые и привлекательные предложения, такие как: высокий заработок в «Интернете» за час работы, низкие цены в интернет – магазинах.

Должно насторожить любое виртуальное мероприятие, которое требует вложения денежных средств, предоплаты.

При покупке товаровстораживающими факторами являются отсутствие возможности курьерской доставки и самовывоза товара, отсутствие у продавца или магазина «истории», неточности или несоответствия в описании товаров, излишняя назойливость продавца или менеджера.

## **Распространенные способы мошенничества в сети «Интернет»**

**Создание лотерей, конкурсов, других мероприятий**, где необходима регистрация участников с указанием полных персональных данных, используемых впоследствии для совершения хищения. При этом лотерейные билеты можно купить прямо на сайте. Организаторы создают страницу под видом официальной государственной лотереи или сайт – дублер (клон), где за небольшую плату идет продажа онлайн – билетов.

## **Сайты знакомств**

Здесь более 80% анкет являются фейковыми, от их имени пишут владельцы сайта. Провоцируя воспользоваться платными услугами. Впоследствии отключить платную услугу весьма проблематично. Такие сайты никогда не имеют открытой для посетителей страницы с адресами, контактами, наименованием юридического лица.

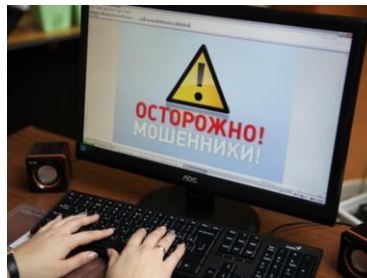
Также достаточно распространены случаи, когда мошенник ведет длительную переписку, в ходе которой поступает просьба о перечислении денежных средств для приобретения авиабилета, на покупку подарка, оплату услуг по доставке товара, в том числе с указанием сайта транспортной компании, о финансовой помощи в сложной ситуации и др.

## **Предложение заработка в сети «Интернет»**

Это сайты о предоставлении рабочих вакансий, когда необходимо внести первоначальное вложение через «Интернет» в обмен на полную инструкцию по заработку.

## **Финансовые пирамиды**

Внесение денег ради прибыли, которая складывается из взносов последующих участников.



## **Социальные сети**

Происходит «взламывание» анкет в социальных сетях, и от имени «друзей» рассылаются сообщения о необходимости перечислить определенную сумму денег либо произвести голосование в каком-либо проекте.

## **Блокировка доступа к электронной почте, аккаунтам**

В данном случае указывается определенная сумма, которую необходимо внести для того, чтобы была произведена разблокировка. Как правило, после внесения денег разблокировка не происходит, а появляется новая инструкция, которая призывает внести деньги повторно.

## **Интернет-магазины мошенников с предоплатой за товар**

На таких Интернет – площадках товары продаются только по предоплате. Заказчик получает посылку с товаром ненадлежащего качества либо испорченным товаром, посылка может прийти пустой или вообще не направляться покупателю.

## **Вирусы, блокирующие работу компьютера**

Для устранения блокировки мошенники предлагают направить SMS на указанный номер, в результате списываются денежные средства со счета либо с телефона.

## **Фишинг**

Для фишинга мошенники создают копию популярного сайта или приложения и активно её распространяют. Предлоги для перехода по ссылке могут быть самыми разными: от уведомлений о посетителях страницы до угроз распространения личных сведений.