**Правила финансовой безопасности в Интернете**

Наши персональные и финансовые данные – мишень для мошенников, орудующих не только в реальном мире, но достающих нас по телефону или в Интернете. Как уберечь личные финансы и семейный бюджет от выкачивания кровных средств со счетов?

В Интернет-магазинах можно наткнуться на несколько разновидностей мошенничества. В основном, деньги с вашей карты Интернет-мошенники пытаются украсть многими способами, например:

1) заражением вашего компьютера. Неважно, используете вы настольный компьютер, ноутбук, смартфон или планшет – заразить их можно через уязвимости операционной системы или установленных вами программ;

2) кражей данных прямо в форме оплаты – некоторые крупные сайты и Интернет-магазины взламывают, вставляя туда платежную форму, из которой данные карты,

3) социальной инженерией – взломав профили ваших друзей или создав привлекательные поддельные профили, мошенники пытаются заставить вас перевести им деньги, переписываясь с вами по электронной почте, в Skype и социальных сетях;

4) спамом и скамом – вам предлагают какие-то товары или услуги по привлекательно низкой цене, но качество не гарантировано;

5) фишингом – вас приманивают на поддельные сообщения от вашего банка или крупного Интернет-портала по электронной почте, в социальных сетях. Перейдете и поверите – данные уже у мошенников, и они могут снять с вашей банковской карты деньги далеко за пределами страны.

**Прокуратура г. Норильска подготовила советы на каждый день, которые помогут уберечь вас от данных видов мошенничества и сберечь ваши деньги:**

**1. Думайте о защите вашего Интернет-устройства**

Неважно, новый или старый у вас компьютер или нет; неважно, что вы думаете про использование антивирусов; неважно, ходите ли вы на сомнительные сайты или нет… Важно, понимаете ли вы, что любая система уязвима перед теми, кто жаждет ее взломать и нажиться на этом. Столкнуться с «грязью» в Интернете проще, чем на улице – и ваши деньги могут внезапно подвергнуться опасности, если ваш любимый сайт взломают или повредят защиту вашего устройства, или если вы просто зайдете в Интернет по бесплатному публичному Wi-Fi (он может оказаться приманкой мошенников). Помните об этом и используйте несколько уровней защиты – дополнительные пароли и программы для повышения безопасности – везде могут таиться угрозы. Дополнительно поможет проверка всех сайтов, на которые вас завлекают, на предмет фальсификации, специальным модулем антивируса. Мало ли чего вы там подхватите, если решите углубиться…

**2. Переводите деньги только друзьям, с кем есть не только контакт в сети**

В последние пару лет участились взломы профилей соцсетей (ВКонтакте, Одноклассники) и других программ для общения (Skype, WhatsApp, Viber), которые мошенники используют для того, чтобы втереться в доверие к постоянным контактам взломанного. Когда друг или родственник просит помочь ему деньгами, не выходя на связь по другим каналам – заподозрите неладное. В финансовой безопасности важно «перебдеть, чем недобдеть».

**3. Покупайте только у продавцов, которым есть основания верить**

Много историй ходит про то, что в китайских Интернет-магазинах и в отечественных сервисах бесплатных объявлений покупатели получают кирпичи по цене iPhone… Для этого нужно платить через сервисы защищенной сделки. Или всё же делать крупные покупки только у проверенных продавцов с высоким рейтингом.

**4. Если вы в Интернете через мобильное устройство – регулярно проверяйте баланс счета**

Проверяйте состояние своего счета у мобильного оператора после посещения сомнительных сайтов, предлагавших бесплатные загрузки «шокирующих» видео, неприличных картинок и взломанных программ. Может быть, вас против вашей воли «подписали» на ежедневные платежи, которые могут обнулить вам счет. Когда счет исчерпается, отключат от связи вас быстро, а добиться возврата денег придется долго.

**5. Платите в Сети только специальной банковской картой**

Если вы заведете дополнительную карту для Интернет-платежей, вы обезопасите основную сумму на своем счету. Вы можете перекидывать нужную сумму через Интернет-банк или мобильный банк на счет нужной карты всякий раз, когда собираетесь платить.

**6. Не сообщайте данные своей карты никому**

Как только вам приходит сообщение «У вас заблокированы деньги. Перезвоните по номеру 8-800…» – нужно насторожиться и посмотреть в Интернете, что пишут про этот номер. Скорее всего, он не связан с вашим банком, а зарегистрирован на подставную компанию. И по этому номеру вас ожидают вопросы жуликов, умело втирающихся в доверие, про номер и срок действия вашей карты.

**7. Постарайтесь не ставить нелегельные программы на компьютер, смартфон и планшет**

Если вы используете приложения Интернет-банков на своем планшете или «умном» телефоне, проверяйте происхождение новых программ, которые ставятся на ваше устройство. Считать SMS-сообщение с помощью взломанной программы гораздо проще, чем подглядывать за жертвами. А «подсмотреть», что вы вводите с клавиатуры, гораздо легче на обычном компьютере, если функцией «прослушки» обладает незаметная шпионская программа.

Защитить [семейный бюджет](https://www.keepsoft.ru/hbk.php?a=blogpost_622&url=https://www.keepsoft.ru/hbk/) от посягательств непросто. Но постарайтесь! И помните, что в случае воровства денег с банковской карты вы защищены законодательно. Как только вы узнали про неладное, в течение суток постарайтесь обратиться в ваш банк и зарегистрировать заявление (по телефону, через онлайн-банк или лично). После чего банк проведет свое расследование и выясняет, мошеннические это были действия или сознательные ваши. С заявлением о хищении денежных средств с вашей карты вы также можете обратиться в территориальный отдел полиции ОМВД России по г. Норильску.