Знать, где ловушка, - это первый шаг к тому, чтобы избежать ее.

Фрэнк Херберт

ПАМЯТКА
«Виртуальные ловушки»

Правила безопасного обращения с финансами и персональными данными в Интернете.

1. Регулярно обновляйте антивирусную программу на домашнем компьютере.
2. Не сообщайте реквизиты банковской карты неизвестным.
3. Будьте бдительны при вводе паролей и личных данных на сайтах, при переходе по незнакомым ссылкам.
4. Не вводите данные банковской карты с компьютеров общественного пользования.
5. Не открывайте подозрительные ссылки из писем и sms от незнакомых отправителей.
6. Помните, что ни один из платежных сервисов не требует оплаты комиссии от получателя перевода.
7. Ни в коем случае не верьте в возможность легкого заработка в сети Интернет и не поддавайтесь на уловки сайтов -„лохотронов”.
8. Получайте максимально полную и достоверную информацию о продавце или интернет-магазине перед покупкой товара и не приобретайте товары в социальных сетях

Ответственность за мошенничество в сети Интернет

В случае, если Вы были обмануты интернет-магазином, юридическое лицо обязано возместить Вам неосновательное обогащение (ст. 1102 Гражданского кодекса РФ), а также понесенные Вами убытки в полном объеме, в том числе компенсацию морального вреда (до трех тысяч рублей, в среднем) (ст. 15 Закона о защите прав потребителей). Также деятельность магазина может быть приостановлена Прокуратурой.

За мошенничество в сети Интернет, совершенное физическими лицами, предусмотрена реальная уголовная ответственность по статье 159 Уголовного кодекса Российской Федерации. Минимальное наказание за мошенничество составляет штраф до ста двадцати тысяч рублей, максимальное наказание, в зависимости от конкретного состава мошенничества, может доходить до лишения свободы на срок до шести лет (часть 3 статьи 159 УК РФ).

Помните, что лучше не становиться жертвой интернет-мошенника вовсе и быть бдительными, так как в случае, если Вы все же стали жертвой мошенника, защита своих прав и возврат денежных средств займет определенное количество времени (от одного до трех месяцев, в среднем).

Расскажите друзьям!

Виды виртуального мошенничества

Фишинг (англ. phishing) – вид интернет мошенничества, целью которого является сбор информации (персональных данных, паролей) пользователя. На электронную почту приходит письмо с уведомлением о том, что Вам необходимо срочно обновить (передать) свои персональные данные в какой-либо системе. Сообщения фишеров часто содержат угрозы, типа блокировки аккаунта, счета и т.д.

Фарминг (англ. pharming) – более продвинутая версия фишинга, заключающаяся в переводе пользователей на фальшивый веб-сайт и краже конфиденциальной информации. «Нигерийские письма» (англ. «Nigerianscam») – электронное письмо с просьбой о помощи в переводе крупной денежной суммы.

Аукционы по типу "Скандинавского аукциона". На таком аукционе товар выставляется по очень низкой цене участники делают минимальные ставки и за каждую ставку с них снимается определенная сумма. Аукцион заканчивается в случае, если в течении определенного времени не будет подано ни одной заявки. После этого товар продается участнику, предложившему последнюю ставку.

«Финансовые пирамиды» - Вы будете получать доход от привлечения новых партнеров в данную организацию. И когда приход новых участников прекращается - финансовая пирамида закрывается и забирает все деньги, которые были инвестированы.

«Попрошайничество в интернете». На сайтах или социальных сетях размещаются объявления с просьбами помочь больному ребенку или сироте. В объявлении, как правило, указываются все данные для связи и лицевой счет, на который нужно переводить денежную сумму. Вы перечисляете деньги, надеясь, что спасаете жизнь ребенку. Но на самом деле, вы просто пополняете счет какому-то мошеннику.

«Легкий заработок». Заходя на любой сайт можно увидеть много предложений заработать хорошие деньги без всяких знаний и умений, достаточно только вложить 10 долларов, а через несколько недель получишь 1000. Обычно такие «вкладчики» уходят ни с чем.

SMS-мошенничество. Вас просят отправить смс на какой-либо номер, указывая, что это либо бесплатно, либо стоит немного. После того, как человек отправляет смс, со счета его мобильного телефона списывается сумма денег в десятки раз превышающая заявленную стоимость отправки смс.