**ПАМЯТКА**

«КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ?»

Мошенничество по российскому законодательству, согласно ст. 159 УК РФ, представляет собой неправомерное завладение чужими деньгами или имуществом с целью обращения его в свою пользу или в пользу третьих лиц, совершаемое с помощью обмана или злоупотребления доверием



Как не попасть на мошеннический сайт:

1. Обращайте внимание на адресную строку браузера: на сайте-клоне будет допущена ошибка.
2. Оплачивайте покупки только через сайты с защищенным соединением и значком платежной системы.
3. Внимательно изучите содержание сайта.
4. Добавьте в закладки сайты, которыми часто пользуетесь, чтобы не набирать адрес вручную.

Как не стать жертвами скимминга и траппинга:

1. Перед снятием денег в банкомате осмотрите его.
2. На картоприемнике не должно быть посторонних предметов, клавиатура не должна шататься.
3. Набирая ПИН-код, прикрывайте клавиатуру рукой. Делайте это даже во время расчетов картой в кафе.
4. Старайтесь пользоваться банкоматами внутри отделений банков. Их чаще проверяют и лучше охраняют.

Ряд рекомендаций по тому, как не стать жертвой мошенников:

1. Мошенники устанавливают поддельную клавиатуру поверх оригинальной, что позволяет им узнать ваш пин-код. Стоит также проверить картоприемник, где может быть спрятан скиммер – считыватель магнитной полосы. Если вы заметили на банкомате посторонний предмет, нужно сразу же сообщить об этом сотрудникам банка.
2. Пользоваться Wi-Fi в кафе и ресторане, конечно же, можно, но специалисты рекомендуют выходить в интернет только через проверенные каналы. Дело в том, что мошенники могут подключиться к сети и отслеживать всё, что вы вводите через клавиатуру. В том числе данные вашей карты.
3. Номер карты, CVV-код, код подтверждения из смс – это данные, которые у вас могут запросить во время стандартного платежа. Если, помимо этого, вас просят ввести номер телефона, пин-код или паспортные данные, лучше откажитесь от операции.
4. Не переходите по ссылкам в письмах о выигрыше денег, гаджета или другого приза. Скорее всего, по ссылке вы получите только вирус.
5. Не передавайте банковскую карту посторонним. Требуйте проведения операций с ней только в личном присутствии и старайтесь никогда не терять ее из виду.
6. Не делайте покупки и не вводите код CCV/CVC на сомнительных сайтах.
7. Никому не сообщайте пин-код от банковской карты, не пишите его на карте и храните отдельно. Набирая пин-код, всегда прикрывайте клавиатуру рукой. В том числе, при расчете в кафе и магазинах.