|  |  |
| --- | --- |
| C:\Users\PermyakovaEN\Desktop\ЗПП\15.03.2017 - ВСЕМИРНЫЙ ДЕНЬ ПРАВ ПОТРЕБИТЕЛЕЙ\imgpreview.jpg | ***Как не попасться мошенникам в Интернете*** |

**Выбирайте безопасные сайты**

Будьте внимательны, не переходите по ссылкам из электронных писем и СМС от неизвестных отправителей. Даже если сообщение пришло от знакомого Вам человека или организации, есть вероятность, что у мошенников появился доступ к их аккаунтам, и они хотят получить доступ и к Вашим данным.

Всегда проверяйте адресную строку браузера. Иногда можно попасть на фишинговый сайт (сайт мошенников) при переходе с одной страницы известного Вам портала на другую.

Делайте покупки только на сайтах, которые обеспечивают безопасное соединение. Адрес такого ресурса начинается с https://. В адресной строке есть значок в виде закрытого замка.

Еще лучше - проверять сертификат безопасности сайта. Для этого нажмите на значок замка и в открывшемся окне выберите «Просмотр сертификатов». Убедитесь, что сертификат выдан именно тому сайту, на котором вы находитесь, и срок его действия еще не закончился.

Выбирайте известные интернет-магазины и сервисы. Изучите отзывы о них от других пользователей. Лучше всего посмотреть отзывы на нескольких независимых сайтах. Добросовестный продавец всегда предоставляет информацию о себе: полное наименование, регистрационные данные, телефон, адрес и прочие контактные данные.

Также следует удостовериться, что продавец является зарегистрированным индивидуальным предпринимателем или юридическим лицом. Это можно сделать, сравнив сведения, указанные на сайте продавца со сведениями, приведенными на сайте Федеральной налоговой службы: [https://egrul.nalog.ru](https://egrul.nalog.ru/).

**Используйте систему безопасных платежей**

Когда переходите на страницу оплаты, ищите логотипы программ MasterCard SecureCode, Verified by Visa и Mir Accept. Эти программы с помощью технологии 3D-Secure дополнительно защищают Вас во время покупок в Интернете.

Если онлайн-магазин поддерживает эту технологию, после ввода реквизитов карты он перенаправит Вас на безопасную интернет-страницу банка. Для подтверждения покупки банк отправит СМС с одноразовым паролем на номер мобильного телефона, привязанный к карте или счету. Никому не сообщайте этот код - просто введите его в специальное поле на странице оплаты.

**Заведите отдельную карту для покупок в Интернете**

Если Вы часто делаете покупки или оплачиваете услуги в Интернете, например, телефонную связь или штрафы, безопаснее использовать для этого отдельную карту. Вносите на нее лишь ту сумму, которую собираетесь потратить, и установите лимит по количеству операций в сутки. Некоторые банки позволяют создать виртуальные карты, которые действительны только для одной онлайн-покупки.

**Никому не сообщайте персональную информацию**

Чаще всего в краже средств со счета виноваты вовсе не банки, платежные системы или онлайн-магазины, а сами доверчивые пользователи.

Мошенники знают множество уловок, чтобы втереться к Вам в доверие, и Ваша задача на эти уловки не попасться. Никогда не сообщайте посторонним данные своей карты, персональные данные и коды из СМС.

Никому не говорите Ваш ПИН-код и код проверки подлинности карты (CVV2/CVC2/ППК2) - последние три цифры на ее оборотной стороне. Даже сотрудники банка не вправе требовать от Вас эти данные. Если кто-либо пытается их узнать, будьте уверены - это мошенники.

Таких же правил следует придерживаться и при пользовании интернет-кошельком: никогда и никому не сообщайте логин и пароль от своего аккаунта.

**Подключите СМС-оповещения об операциях по карте**

В этом случае Вы сразу же узнаете о платеже, которого Вы не совершали, и сможете быстро отреагировать: заблокировать карту и опротестовать операцию.