

## Где подстерегает опасность?

Риск возникает во время покупок на сайтах и в приложениях, использования электронных кошельков, мобильного и интернет-банкинга.

Главное оружие киберпреступников – фишинг. Другими словами – выуживание конфиденциальных данных: паролей, реквизитов карты или счета для кражи денег с карты или из интернет-кошелька.

Воры играют на психологии: рассылают СМС, электронные письма и сообщения в чатах с просьбой, например, «подтвердить аккаунт» или «восстановить доступ к банковскому счету».

Сообщения содержат ссылку на специальный фишинговый сайт – сайт-двойник банка, госоргана или другой организации.

Если вы не заметили подмены, то после ввода своего логина, пароля интернетбанка или реквизитов карты сразу переведете деньги мошенникам.

## Как защититься от фишинга и других видов кибермошенничества?

### 1. Пользуйтесь только личными устройствами

Делайте покупки, заходите в свой интернет-банк или мобильный банк только с личного компьютера, планшета и смартфона.

Обязательно ставьте на них пароль.

### 2. Защититесь от вирусов

Обязательно поставьте антивирус на всех своих устройствах, включая мобильные, и регулярно обновляйте их. Хороший антивирусный пакет всегда включает защиту от фишинга и вирусных программ.

## 3. Выбирайте безопасные сайты

- Никогда не переходите по ссылкам из писем и СМС от неизвестных отправителей. Даже если сообщение пришло от знакомого вам человека или организации, не спешите открывать их. Возможно, у мошенников появился доступ к их аккаунтам и они хотят получить доступ и к вашим данным.

- Набирайте интернет-адрес банка вручную, а еще лучше – сохраняйте в закладках адреса ваших банков, госорганов и других организаций.

- Всегда проверяйте адресную строку браузера. Иногда можно попасть на фишинговый сайт 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 дает полную информацию о себе: телефон, адрес и прочие контактные данные.

## 4. 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.

## 5. 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.

## 6. 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.

## 7. 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.

### Что делать, если деньги все-таки украли?

#### Заблокируйте карту

Если с карты списали деньги без вашего ведома, позвоните в банк и заблокируйте карту. Так же нужно поступить, если вы потеряли карту или даже просто подозреваете, что ее данные стали известны посторонним людям.

#### Опротестуйте операцию

В тот же день, когда вы получили уведомление о незаконной операции (максимум – на следующий), обратитесь в отделение банка. Запросите выписку по счету и напишите заявление о несогласии с операцией, которую не совершали. Экземпляр заявления с отметкой банка, что оно принято, оставьте у себя.

Если банк докажет, что вы нарушили правила использования карты, то вернуть деньги не получится. Например, когда вы сами сообщили кому-то реквизиты своей карты, верификационный номер с ее оборотной стороны или ПИН-код.

#### Обратитесь в полицию

Расследованием преступлений в интернете занимается Бюро специальных технических мероприятий (БСТМ) МВД России. Подайте заявление в территориальное учреждение БСТМ. Можно просто написать заявление в отделение полиции по месту жительства. Чем

быстрее вы это сделаете, тем больше шансов найти преступников и вернуть деньги.

При подготовке буклета были использованы материалы сайта «Финансовая культура»:

<https://fincult.info/article/safe-shopping-on-the-internet/>

Составитель: М.А. Рыжкова, зав. центром правовой информации

Центр правовой информации

Адрес:

Курская область, г. Обоянь, ул. Ленина, 36

E-mail: [pcpioboyan2002@mail.ru](mailto:pcpioboyan2002@mail.ru)

Сайт: <http://мбиблиотека.рф/>

МКУК «Обоянская межпоселенческая библиотека»  
Центр правовой информации

**Безопасный  
онлайн-шопинг**



Обоянь, 2019