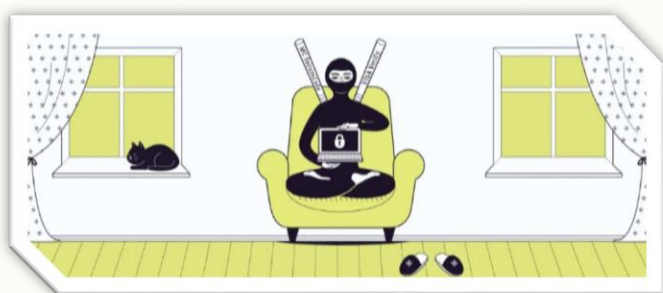


## БЕЗОПАСНЫЕ ПОКУПКИ В ИНТЕРНЕТЕ

Онлайн-шопинг быстрее и удобнее, чем походы по магазинам. Но и рисков больше: шанс встретить киберпреступников в разы выше, чем реальных грабителей. Делимся советами, как сделать покупки в сети максимально безопасными...

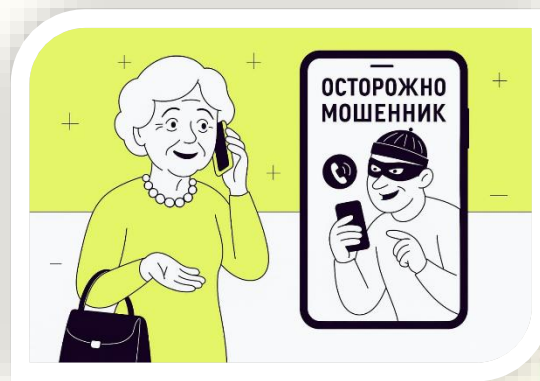
### 🐱 Где подстерегает опасность?



Риск возникает, как только на каком-то сайте или в приложении вы вводите данные банковской карты или электронного кошелька либо проводите оплату через мобильный или онлайн-банк

### 🔑 Как это работает?

Мошенники рассылают СМС, электронные письма, сообщения в мессенджерах и соцсетях с просьбой «подтвердить аккаунт» или «восстановить доступ к банковскому счету». Сообщения содержат ссылку на фишинговый сайт - сайт-двойник магазина, банка. Если вы не заметили подмены, то после ввода своего логина, пароля интернет-банка или реквизитов карты сразу переведете деньги мошенникам



### 👤 Как защититься?

#### 🔑 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.

### 🌿 **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

### 🌿 **Выбирайте безопасные сайты**

Не открывайте ссылки, которые прислали неизвестные отправители, не спешите переходить на сайт, даже если отправитель знаком

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

Всегда проверяйте адресную строку браузера, чтобы не 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

Выбирайте известные интернет-магазины и сервисы. Изучите отзывы о них от других пользователей. Добросовестный продавец всегда дает полную информацию о себе: телефон, адрес и прочие контактные данные

### 🌿 **Используйте систему безопасных платежей**

Когда переходите на страницу оплаты, ищите логотипы платежных систем. Эти программы дополнительно защищают вас во время покупок в интернете с помощью технологии 3D-Secure: после ввода реквизитов карты онлайн-магазин перенаправит вас на безопасную интернет-страницу банка. Для подтверждения покупки банк отправит уведомление с одноразовым паролем на номер мобильного телефона, привязанный к карте или счету

### 🌿 **Заведите отдельную карту для покупок в интернете**

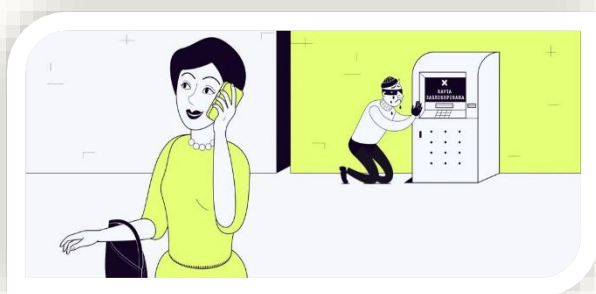
Если вы часто делаете покупки или оплачиваете услуги в интернете, безопаснее использовать для этого отдельную карту. Вносите на нее лишь ту сумму, которую собираетесь потратить, и установите лимит по количеству операций в сутки

✿ **Никому не сообщайте персональную информацию:**

- ◆ секретные реквизиты своей карты (последние 3 цифры на оборотной стороне карты)
- ◆ персональные данные
- ◆ коды из уведомлений от банка
- ◆ ПИН-код

**! ДАЖЕ СОТРУДНИКИ БАНКА НЕ ВПРАВЕ ТРЕБОВАТЬ ОТ ВАС ЭТИ ДАННЫЕ !**

✿ **Подключите оповещения об операциях по карте**



Так вы сразу узнаете о платеже или переводе, которые не совершали и успеете быстро отреагировать: заблокировать карту. Можно настроить уведомления о списаниях через мобильное приложение банка, подключить СМС-оповещения