



Администрация  
Краснодарского края



# КИБЕР БЕЗОПАСНОСТЬ



## ФИНАНСОВОЕ КИБЕР МОШЕННИЧЕСТВО

## ФИНАНСОВОЕ

### КИБЕРМОШЕННИЧЕСТВО

— это преступная деятельность в сфере информационных технологий, целью которой является причинение материального или иного ущерба путем хищения личной информации пользователя.

Совершают эти преступления киберпреступники или хакеры, которые зарабатывают на этом деньги.

### ? КАКИЕ ДАННЫЕ НУЖНЫ МОШЕННИКАМ

- ✓ Ключом к деньгам на вашем счете могут стать реквизиты карты, включая срок действия, три цифры с оборота, а также пароли и коды из уведомлений банка.
- ✓ Либо логины и пароли от вашего онлайн-банка и других приложений; и личных кабинетов, к которым привязана платежная информация.
- ✓ Мошенники выманивают конфиденциальные данные с помощью социальной инженерии и фишинга (вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логики и паролям).
- ✓ Нередко они рассылают сообщения со ссылками на вредоносные программы или файлами, содержащими вирусы, с помощью которых киберпреступники надеются получить удаленный доступ к гаджетам и украсть секретные данные.

### ? КАК ЗАЩИТИТЬ УСТРОЙСТВА ОТ КИБЕРПРЕСТУПНИКОВ

#### СЛЕДУЙТЕ ГЛАВНЫМ ПРАВИЛАМ КИБЕРГИГИЕНЫ

##### Пользуйтесь антивирусами

Установите антивирусные программы на все гаджеты, которыми пользуетесь. Тогда мошенники не смогут завладеть данными с вашего устройства, даже если вы перейдете по вредоносной ссылке. Главное не забывать обновлять защитные системы.

##### Постоянно обновляйте систему

Злоумышленники всегда ищут уязвимости в программном обеспечении и приложениях, и производители регулярно выпускают обновления и усиливают антивирусную защиту. Поэтому важно всегда использовать последнюю версию программ. В настройках вашего гаджета найдите функцию автоматического обновления и включите ее. Взломать обновленное устройство гораздо сложнее.

##### Скачивайте только проверенные приложения

Загружайте приложения из проверенных источников. Перед загрузкой читайте комментарии других пользователей на профильных форумах, чтобы заранее узнать о возможных рисках использования программы. А также убедитесь, что она активно обновляется разработчиком — в официальных магазинах обычно указана дата последних изменений.

Если вы скачали какое-либо приложение, но совсем им не пользуетесь — лучше его удалить, тем самым снизив риск взлома вашего устройства.

##### Не устанавливайте программы по просьбе незнакомцев

Не только вредоносные приложения несут угрозу. Иногда мошенники используют легальные программы удаленного доступа, чтобы управлять устройством от вашего имени.

С помощью программ удаленного доступа преступники могут прочесть СМС от банка с секретными кодами и паролями, зайти в ваш онлайн-банк, перевести деньги или оформить кредит от вашего имени.

##### Изучайте настройки конфиденциальности

При установке приложений обращайтесь внимание на настройки конфиденциальности. Действительно ли так уж необходимо делиться с программой списком ваших контактов или геолокацией?

Разрешайте доступ только в том случае, если это действительно необходимо. Например, местоположение нужно для приложения такси, но едва ли важно календарю задач. Если вас не устраивают требования прав доступа, выберите другое приложение.

Когда в программе обновляется пользовательское соглашение, не спешите сразу принимать условия — сперва внимательно их изучите.

##### Выбирайте сложные пароли

Пароль должен состоять не менее чем из восьми символов: цифр, строчных и заглавных букв, специальных символов. Лучше не использовать популярные слова и общеизвестные сокращения. Никаких дат рождения, имен и фамилий. Пароли должны быть разными для каждого аккаунта — не повторяйтесь. И каждый раз вводите пароль заново вручную — не сохраняйте его для автоматического ввода.

По возможности настройте двойную идентификацию, тогда помимо ввода пароля система будет каждый раз запрашивать подтверждение входа с помощью кода, который мгновенно приходит в СМС, push-уведомлении или на электронный адрес.

