Не храните деньги на этой карте – перед совершением покупки просто переведите на нее ту сумму, которую собираетесь потратить. Для этих целей можно использовать виртуальные карты, которые генерируются через мобильное приложение банка и привязаны к основному счету, но имеют отдельный номер и срок действия.

4. 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.

5. НЕ УСТАНАВЛИВАЙТЕ ПРОГРАММЫ ПО ПРОСЬБЕ НЕЗНАКОМЦЕВ. Мошенники могут использовать легальные программы удаленного доступа, чтобы управлять устройством от вашего имени.

6. ВЫБИРАЙТЕ СЛОЖНЫЕ ПАРОЛИ. Пароль должен состоять не менее чем из восьми символов: цифр, строчных и заглавных букв, специальных символов. Пароли должны быть разными для каждого аккаунта. Каждый раз вводите пароль заново вручную, не сохраняйте его для автоматического ввода.

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

КАК ПРОТИВОСТОЯТЬ ТЕЛЕФОННЫМ МОШЕННИКАМ?

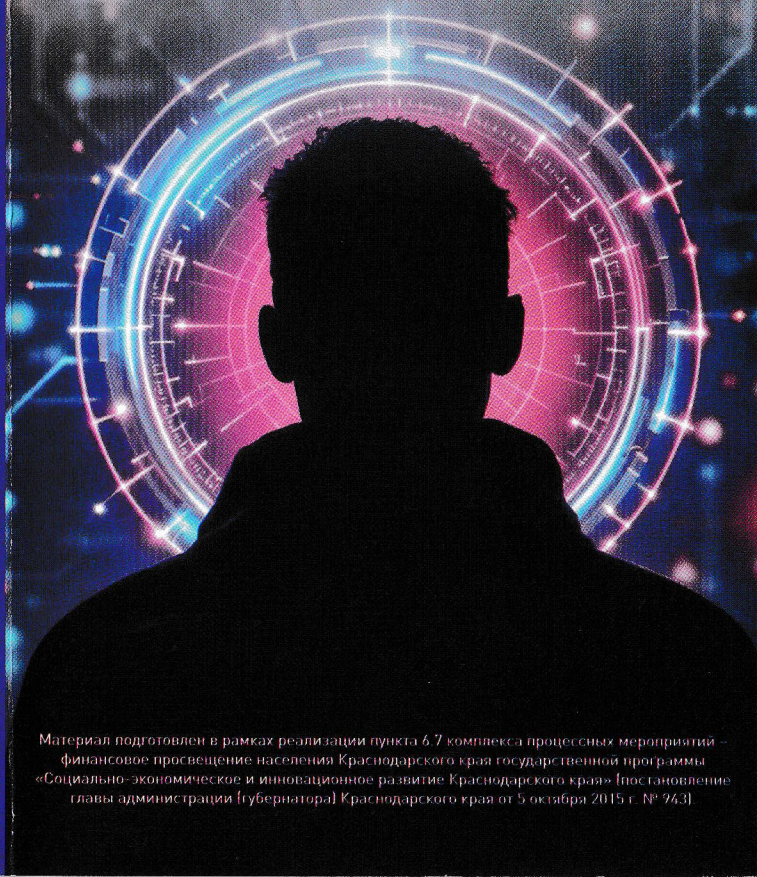
- **НЕ ОТВЕЧАЙТЕ** на звонки с незнакомых номеров, особенно зарегистрированных в другом регионе.
- **ПРЕРВИТЕ РАЗГОВОР,** если он касается финансовых вопросов.
- **НЕ ТОРОПИТЕСЬ,** принимая финансовое решение.
- **ПРОВЕРЬТЕ ИНФОРМАЦИЮ** в интернете или обратитесь за помощью к близким родственникам.
- **САМОСТОЯТЕЛЬНО ПОЗВОНИТЕ** близкому человеку/в банк/в организацию.
- **НЕ ПЕРЕЗВАНИВАЙТЕ** по незнакомым номерам.
- **НЕ СООБЩАЙТЕ** коды подтверждения из SMS, пароли, ПИН-коды, CVV-коды банковских карт и другие конфиденциальные данные посторонним людям.

САМОЕ АКТУАЛЬНОЕ ЗДЕСЬ!

Администрация Краснодарского края

Министерство экономики Краснодарского края

КИБЕР-БЕЗОПАСНОСТЬ



Материал подготовлен в рамках реализации пункта 6.7 комплекса процессных мероприятий – финансовое просвещение населения Краснодарского края государственной программы «Социально-экономическое и инновационное развитие Краснодарского края» (постановление главы администрации (губернатора) Краснодарского края от 5 октября 2015 г. № 943)

ФИНАНСОВОЕ КИБЕРМОШЕННИЧЕСТВО

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

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, 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 – логинам и паролям). Нередко они рассылают сообщения со ссылками на вредоносные программы или файлами, содержащими вирусы, с помощью которых кибер-преступники надеются получить удаленный доступ к устройствам и украсть секретные данные.

ПОПУЛЯРНЫЕ СПОСОБЫ КИБЕРМОШЕННИЧЕСТВА

ДИПФЕЙКИ. С помощью нейросети мошенники создают реалистичное видеоизображение человека. Затем сгенерированный образ рассылают его друзьям или родным через мессенджеры или социальные сети. В коротком фальшивом видеоролике виртуальный герой, голос которого иногда сложно отличить от голоса прототипа, рассказывает якобы о своей проблеме (болезнь, ДТП, увольнение) и просит перевести деньги на определенный счет. Чтобы создать цифровую копию конкретного человека, злоумышленники используют фото и видео, а также запись голоса, полученные, в основном, в результате взлома его аккаунта в социальных сетях или мессенджерах.

ФИШИНГ с использованием искусственного интеллекта. Фейковые электронные письма и сообщения предназначены для того, чтобы заставить вас раскрыть вашу личную информацию и пароли.

СОЦИАЛЬНЫЕ СЕТИ И ЧАТ-БОТЫ. Программы, которые маскируются под реальных людей, также могут обманом заставить вас раскрыть информацию.

РАССЫЛКА «ПОЛЕЗНЫХ ФАЙЛОВ». Злоумышленники рассылают файлы с вирусами в социальных сетях и мессенджерах, чтобы похитить деньги пользователей.

Они маскируют их под «полезные» файлы – например, бесплатные электронные книги или антивирусные программы. Однако, если человек скачает и откроет такой файл, то мошенники получат полный дистанционный контроль над его устройством. Это позволит злоумышленникам читать входящие СМС-сообщения, просматривать журнал звонков и управлять любыми функциями смартфона.

КАК ЗАЩИТИТЬ УСТРОЙСТВА ОТ КИБЕРПРЕСТУПНИКОВ?

1. ПОЛЬЗУЙТЕСЬ АНТИВИРУСАМИ. Установите антивирусные программы на все устройства, которыми пользуетесь.

2. ПРОВЕРЯЙТЕ АДРЕС САЙТА. Осуществляйте онлайн-оплату только если сайт использует протокол HTTPS и имеет действующий сертификат безопасности (изображение замка в адресной строке). Иконка замка слева от адреса сайта должна быть зеленой или серой (в зависимости от браузера), а при нажатии на нее должен отображаться действующий SSL-сертификат.

3. ЗАВЕДИТЕ ОТДЕЛЬНУЮ КАРТУ. Для онлайн-шопинга лучше не использовать обычную карту (в том числе зарплатную) – лучше выпустить отдельную. Если мошенники получат к ней доступ, то смогут завладеть только теми средствами, которые на ней находятся.