Как защитить свои гаджеты от мошенников

Киберпреступники постоянно охотятся на чужие личные данные. Атакуют телефоны, планшеты и компьютеры с помощью вредоносных программ, выманивают секретную информацию у банковских клиентов уловками социальной инженерии. Рассказываем, как защитить свою конфиденциальность и дать отпор злоумышленникам.

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.

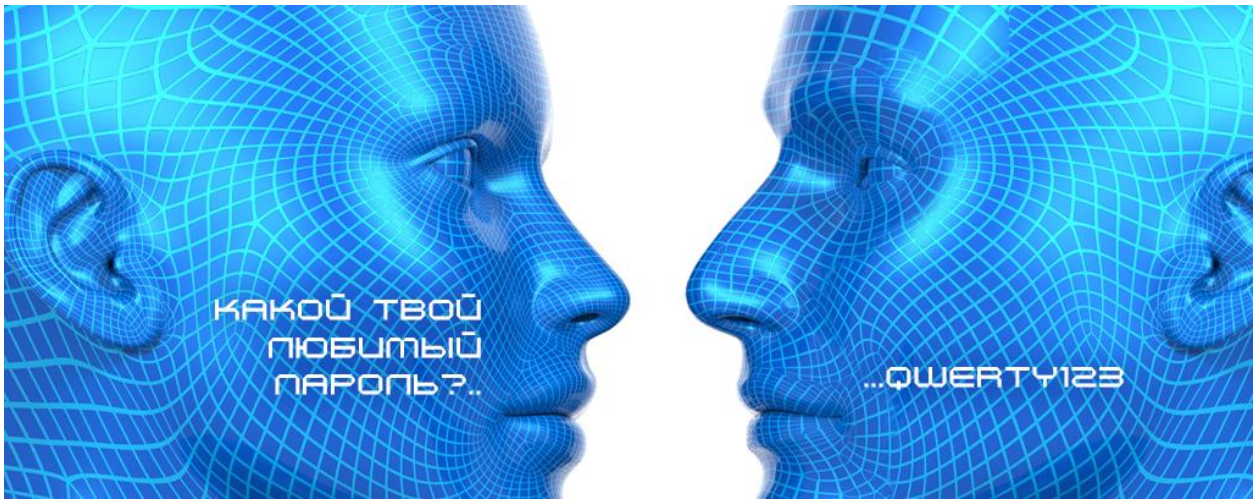
«Все началось с того, что я решила продать холодильник в интернете. Разместила объявление на популярном сайте, и буквально через пять минут звонит покупатель. Говорит, что работает в компании, которая занимается скупкой старых холодильников. Они их ремонтируют и перепродают, а непригодные для ремонта идут на детали. Мол, их очень интересует модель моего холодильника и они готовы прямо сейчас перевести предоплату…»

Будьте бдительны, не наступайте на чужие грабли!

Мошенники выманивают конфиденциальные данные с помощью социальной инженерии и фишинга.Нередко они рассылают сообщения со ссылками на вредоносные программы или файлами, содержащими вирусы. С помощью них киберпреступники надеются получить удаленный доступ к гаджетам и украсть с них секретные данные.

Банк ничего не компенсирует, если человек сам сообщил мошенникам конфиденциальную информацию или добровольно установил шпионскую программу.

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.

«Каждый месяц бывший муж переводит мне на карту алименты. Как-то вечером мы созвонились и он сказал, что перевел четыре тысячи. Мне сразу же пришло смс от банка о том, что деньги поступили. Ночью я получила еще одно уведомление от банка, о том, что моя карта заблокирована. Чтобы отменить блокировку, нужно было пройти по ссылке из сообщения…»

Будьте бдительны, не наступайте на чужие грабли!

Подробнее о том, как распознать сомнительную ссылку и обезопасить свои деньги и данные, читайте в тексте «Фишинг: что это такое и как от него защититься».

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. Например, для телефонов и планшетов на базе iOS – из AppStore, для Android – из Google Play. 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.

«Решила подзаработать в декрете и стала искать в интернете удаленку. Разместила резюме на популярном сайте вакансий. Скоро позвонила девушка и сказала, что ищет операторов колл-центра в свой магазин по продаже косметики. Предложила хорошую зарплату и работать всего три часа в день. Как раз то, что мне нужно. Стали обсуждать детали, она попросила скачать на телефон несколько программ для работы…»

Будьте бдительны, не наступайте на чужие грабли!

Если вы скачали какое-либо приложение, но совсем им не пользуетесь – лучше его удалить. Вдруг у него слабая киберзащита? Снизите 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.

«Только что столкнулся с ситуацией, звонок на телефон, человек представился сотрудником банка и рассказал, что к моему счету подключился сторонний телефон и попытался перевести деньги, эта попытка заблокирована...»

Будьте бдительны, не наступайте на чужие грабли!

С помощью программ удаленного доступа преступники могут прочитать 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 обращайте 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.

Как обезопасить данные на случай пропажи телефона?

Эти риски стоит продумать заранее. Выполните три шага:

1. **Включите блокировку**

Для защиты устройства включите автоматическую блокировку экрана. Используйте пароль, отпечаток пальца или Face ID – функцию распознавания лица владельца.

2. **Настройте отслеживание**

Установите программу, позволяющую дистанционно отслеживать местоположение устройства. В случае кражи или потери вы сможете видеть, где находится ваш гаджет, подключиться к нему и даже удаленно стереть с него всю информацию. К примеру, в устройствах на базе с Android есть функция поиска телефона Google Find My Device, в девайсах Samsung – схожая опция Samsung Find My Mobile, на платформе iOS – Find My iPhone. Обязательно заранее активируйте их в настройках гаджета.

3. **Создавайте резервные копии**

Регулярно делайте «бэкап» – резервное копирование ваших данных. Эта опция позволяет сохранять конфигурацию настроек вашего устройства, все приложения и другую информацию. Это поможет быстрее восстановить данные с потерянного или украденного телефона и перенести их на новый.

Что делать, если телефон украли?

Если вы лишились телефона с номером, который привязан к вашему банковскому счету, действуйте, как при потере карты. Звоните в банк на горячую линию или бегите в его отделение и просите блокировать все карты, мобильный и онлайн-банк.

После этого на всякий случай позвоните на свой номер: возможно, телефон кто-то нашел и готов вам его вернуть.

Если же гаджет своровали, напишите в полиции заявление о краже. Возьмите заверенную копию этого заявления – оно может понадобиться в банке, если преступники успеют взломать телефон и онлайн-банк и украсть деньги со счетов.

Как быть, если мошенники взломали украденный телефон и вывели деньги со счетов?

В этом случае вы можете рассчитывать на компенсацию только при двух условиях:

1. Вы не нарушали правил безопасности. Например, не сообщали мошенникам конфиденциальные данные карты, логины и пароли от онлайн-банка, ваше устройство на момент кражи было защищено паролем, как и все приложения, к которым привязана платежная информация.
2. Вы вовремя оспорили списание – не позднее следующего дня после того, как получили от банка уведомление об операции, которую не совершали.

Чтобы возместить потери, как можно скорее пишите в банк заявление, что операции прошли без вашего согласия, просите провести внутреннее расследование и вернуть деньги. Подчеркните, что вы соблюдали правила кибергигиены. И приложите копию заявления о краже телефона, которое вы составили в полиции.

Если на вас оформили кредит, то отдельным заявлением требуйте у банка признать договор недействительным. Просите отложить начало выплат по кредиту до завершения расследования. В случаях, когда банк не соглашается на отсрочку платежей, лучше их вносить, чтобы не испортить свою кредитную историю. Когда договор аннулируют, вы сможете потребовать, чтобы вам вернули уплаченное.

Если вы соблюдали все требования безопасности, но банк не прислушивается к вашим доводам, жалуйтесь на него в интернет-приемную Банка России.

Подробнее о том, как обезопаситься от киберпреступников, читайте в тексте «Как уберечь себя и близких от финансового мошенничества».

Истории о других схемах, с помощью которых аферисты крадут данные и деньги, и советы, как вовремя распознать обман, вы найдете в разделе «Грабли».

Источник:
Официальный сайт Банка России
по финансовой грамотности
Fincult.info