Фишинг: что это такое и как от него защититься

Николай получил электронное письмо от интернет-магазина, в котором часто делает покупки: «Подтвердите свой аккаунт, чтобы продолжать пользоваться бонусами». Николай перешел по ссылке из письма, заново ввел свои личные данные и данные банковской карты. Затем его попросили сделать «пробный платеж» на 1 рубль. В ходе оплаты надо было ввести трехзначный код с обратной стороны карты. Как только Николай ввел этот код, ему пришло сообщение от банка о списании со счета, но вовсе не 1 рубля, а 10 000 рублей. Разбираемся, как так получилось.

На самом деле письмо Николаю прислал не магазин, а кибермошенники. Они обманом выманили у Николая конфиденциальные данные, и он даже не заметил, как попался на их удочку. Этот вид мошенничества так и называется — **фишинг**. То есть рыбалка, ловля на крючок.

Обычно преступники сначала цепляют человека за живое: запугивают потерей денег или завлекают супервыгодой, пробуждают любопытство или сочувствие. Затем выманивают личные данные, реквизиты счета или карты. И в итоге списывают деньги с банковского счета.

Рассмотрим, какие ошибки допустил Николай и как он мог защититься от потери денег.

Ошибка № 1: не использовать антивирусную защиту

Николай считал пустой тратой денег покупку антивируса. Он решил, что гораздо проще и дешевле самому чистить почтовый ящик от спама.

Как устранить ошибку.

На все свои гаджеты — компьютер, ноутбук, планшет и смартфон — нужно установить антивирус. Хороший антивирусный пакет включает защиту от спама и фишинговых писем. Он сам распознает подозрительных адресатов.

Кроме того, антивирус защитит от программ, которые воруют данные карт, получают доступ к онлайн- и мобильным банкам, перехватывают СМС и push-сообщения с секретными кодами. Это еще опаснее, чем фишинг, — ваш счет могут обнулить, а вы об этом даже не сразу узнаете.

Важно регулярно обновлять защиту. Кибермошенники изобретают новые вирусы и способы фишинга буквально каждый день.

Ошибка № 2: переходить по ссылкам из сообщений от незнакомых адресатов

Николай решил, что получил письмо от онлайн-магазина — он увидел знакомое название и логотип в тексте письма. Но адрес отправителя он не проверил.

Как действуют преступники

Мошенники регистрируют адрес почты, похожий на адрес реального интернет-магазина, банка или другой легальной организации. Например, вместо настоящего адреса магазина «Супершоп» mail@supershop.ru используют mail@supersshope.ru.

Иногда обманщики даже не заморачиваются с похожим адресом, так как зачастую он скрыт от глаз пользователя. Просто указывают название магазина как имя отправителя — именно его и видит получатель. Подмену проверить легко, но не все обращают внимание на такие детали.

Мошенники заманивают людей на фишинговые сайты не только через электронную почту, но и через мессенджеры и социальные сети. Вам может прийти сообщение от знакомого, который предлагает перейти по ссылке. Но может оказаться, что его аккаунт взломали.

Иногда преступники даже не стараются мимикрировать под кого-то другого. Вместо этого они запускают свой собственный бизнес-проект. И создают видимость, что проводят викторины с гарантированным выигрышем, анкетирование за вознаграждение или рассылают видео для взрослых.

В текст письма или сообщения они добавляют ссылку, которая вместо обещанных викторин и видео ведет на фишинговый сайт. Его создают специально для этой аферы, чтобы собирать личные и платежные данные пользователей. В некоторых случаях при переходе по ссылке загружается вирус, который ворует данные с вашего устройства.

Обманщики подбирают тему письма, на которую получатель должен среагировать. Что-то пугающее: «Ваш аккаунт будет заблокирован», «Срочное сообщение от Службы безопасности». Или завлекающее: «Вам начислено 3000 бонусов», «Возврат платежа на 12 000 рублей». Или интригующее: «Привет! Шлю тебе фотки с последней вечеринки». Мошенники умеют играть на эмоциях.

Как избежать уловок мошенников

Всегда тщательно проверяйте адрес, с которого пришло письмо. Если он хотя бы одним символом отличается от привычного адреса магазина, банка, авиакомпании или другой реальной организации, такое письмо не стоит даже открывать. Если же адрес вам вообще не знаком и вы не ждете сообщений от новых адресатов, то можете смело его удалять.

Когда откроете письмо, обратите внимание на то, как оно написано и оформлено. Орфографические ошибки и ужасный дизайн — явный признак поддельного письма. Но в последнее время мошенники научились очень точно повторять фирменный стиль известных компаний. Так что стоит быть внимательным, даже если все выглядит идеально.

Если непонятную ссылку прислал друг или знакомый, лучше перезвонить и удостовериться, что это сообщение точно от него.

Ошибка № 3: не проверять адресную строку сайта

Николай заметил, что привычный дизайн интернет-магазина немного изменился, но это его не насторожило. Внимательно изучить адресную строку браузера ему и в голову не пришло.

Что нужно проверять при переходе на сайт

Адрес. Лучше всего сохранять адреса банков, госорганов, любимых интернет-магазинов и других онлайн-сервисов в закладках. Можно вбивать адрес вручную, но нужно быть внимательным — иногда ошибка даже в одном символе приведет вас на фишинговый сайт-двойник.

Всегда проверяйте адресную строку браузера. Иногда можно попасть на фишинговый сайт даже при переходе с одной страницы известного вам портала на другую.

Безопасность соединения. Если вы хотите ввести персональную информацию или данные карты, сделать покупку через сайт, то перед его адресом обязательно должно стоять **https** и **значок закрытого замка**. Буква s и закрытый замок означают, что соединение защищено: когда вы вводите на сайте данные, они автоматически шифруются и их не могут перехватить.

Защищенное соединение — требование обязательное, но не достаточное. Хакеры не могут подключиться к такому сайту и узнать ваши данные. Но это не гарантия того, что сам сайт создан законопослушной компанией. В последнее время и преступники умудряются получать сертификаты безопасности для своих сайтов.

Дизайн. Даже если вы проморгали лишнюю букву в адресе, а преступники организовали защищенное соединение, плохой дизайн сайта должен броситься в глаза.

Преступники создают онлайн-ресурсы с простой целью — собрать конфиденциальные данные. Поэтому в большинстве случаев они не мудрят со структурой и дизайном сайта.

Небрежная верстка, орфографические ошибки, неработающие разделы и ссылки — явные признаки фальшивки.

Но если у мошенников большие амбиции, они могут вложиться в создание сайта, который максимально точно повторяет интернет-ресурс известной организации. Или создать красивый и качественный сайт своего собственного «проекта». Так что только на дизайн тоже ориентироваться нельзя.

Ошибка № 4: платить через небезопасные страницы

Фальшивый «интернет-магазин» предложил Николаю провести «пробный платеж» и для этого ввести код с обратной стороны карты и код из СМС-сообщения прямо на своем сайте. Николай не обратил внимания, что для проведения оплаты его не перекинули на страницу платежной системы.

Что нужно знать

После ввода реквизитов карты сайт магазина должен перекинуть вас на шлюз платежной системы вашей карты. Это отдельная безопасная страница, интернет-магазин не может получить доступ к информации, которую вы там введете.

Платежные шлюзы соединяют владельца карты с его банком при проведении платежа. Банк присылает клиенту в СМС-сообщении одноразовый код для подтверждения операции. И только после того, как покупатель его вводит, проходит платеж.

Никому не сообщайте секретные коды от банка — проверьте, совпадают ли данные из СМС с деталями операции. Если все в порядке, вбейте код в специальное поле на странице оплаты. Если нет — позвоните в банк.

Безопасные шлюзы есть у всех платежных систем. Ищите их логотипы на странице оплаты: Visa Secure, MasterCard SecureCode и Mir Accept. Причем логотипы должны быть активными ссылками, которые ведут на сайты платежных систем. На страницах мошенников эти логотипы — просто картинки.

Ошибка № 5: использовать одну и ту же карту для всех платежей

Николай платил в интернет-магазинах своей зарплатной картой. Теперь ему придется заказать новую. А пока банк будет ее перевыпускать, доступ к остатку денег на счете он сможет получить только в отделении банка.

Как стоит поступать

Для онлайн-покупок и оплаты услуг через интернет лучше завести отдельную карту. Стоит переводить на нее деньги прямо перед платежом и класть ровно ту сумму, которую собираетесь перечислить.

Некоторые банки и системы электронных платежей (электронные кошельки) предлагают заводить виртуальные карты — у них есть реквизиты, но в виде пластика они

не существуют. Иногда можно даже создавать виртуальные карты, которые действительны лишь для одной онлайн-покупки.

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?

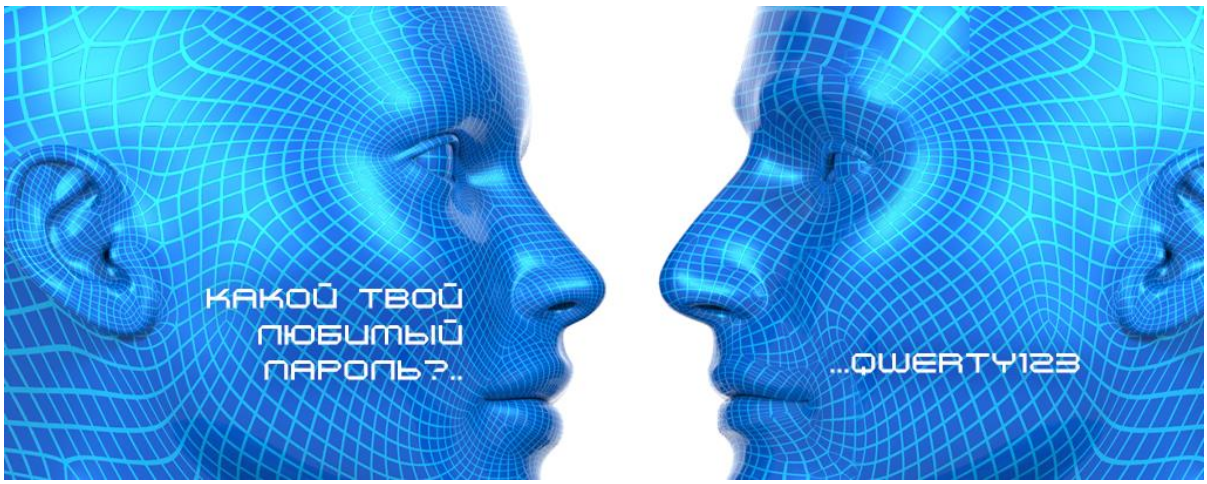
Ключом к деньгам на вашем счете могут стать реквизиты карты, включая срок действия, три цифры с оборота, а также пароли и коды из уведомлений банка. Либо логины и пароли от вашего онлайн-банка и других приложений и личных кабинетов, к которым привязана платежная информация.

«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!

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.