Что такое фишинг и как от него защититься

В 2022 году в Рунете обнаружили 18 000 мошеннических сайтов, мимикрирующих под популярные ресурсы вроде VK или «Сбера». Если перейти на них и ввести свои личные данные — логин и пароль или платёжную информацию, — то можно потерять доступ к аккаунту или деньги.

Хакерская атака, при которой персональные данные и деньги похищают с помощью фейковых сайтов, аккаунтов или электронных писем, называется фишингом. В этой статье мы подробно разберёмся, в чём её смысл, как она проводится и какие есть способы от неё защититься.

Что такое фишинговые атаки

Фишинг (от англ. **fishing** — рыбачить, выуживать) — это вид кибератаки, при которой злоумышленник пытается получить доступ к личной информации пользователя, например к логину и паролю от электронной почты или данным банковской карты.

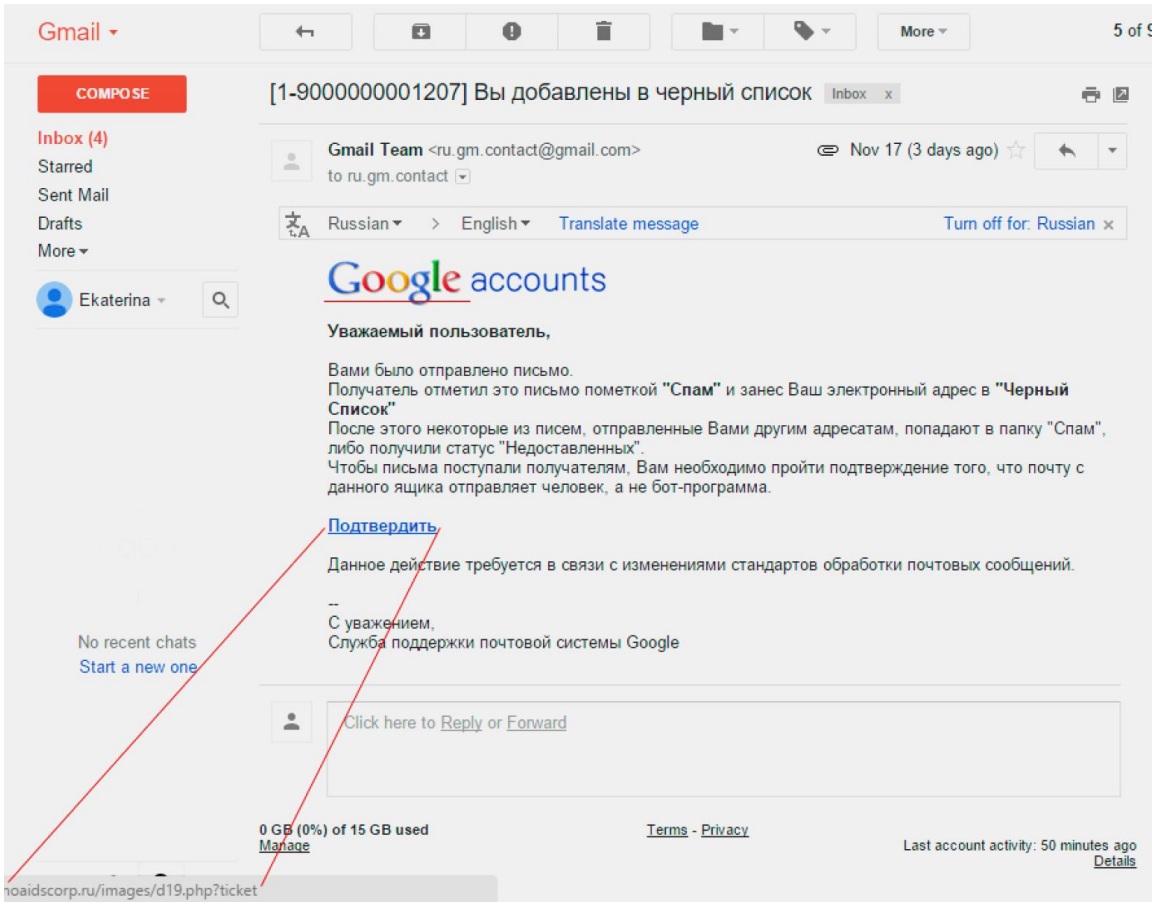
Фишинг отличается от других видов хакерских атак тем, что мошенники активно манипулируют базовыми человеческими эмоциями, такими как любопытство и страх, а также используют информацию, которые смогли собрать из открытых источников о человеке.

Фишинг проходит по электронной почте, SMS, в мессенджерах и в социальных сетях. Атака выглядит так: человек получает письмо или сообщение от сервисов, которым он доверяет. Например, от своего банка, интернет-провайдера или магазина, где недавно совершил покупку. В этом письме его просят срочно указать личные данные или обновить их, иначе счёт будет заблокирован или возникнут другие проблемы. Это и есть приманка, так называемое «забрасывание удочки».

Если приглядеться к такому «срочному» письму или СМС, можно заметить, что домен или номер телефона не совпадают с официальными контактами сервиса, банка или магазина. А в самом письме или сообщении будет ссылка, ведущая на копию официального сайта. Если пользователь введёт там свои данные, то они попадут к мошенникам.

Посмотрим на примеры фишинговых писем, сайтов и сообщений.

Фишинговое письмо маскируется под запрос от существующей компании или сервиса. Например, пользователь может получить письмо, в котором указан безобидный запрос на подтверждение личных данных. На первый взгляд всё хорошо.

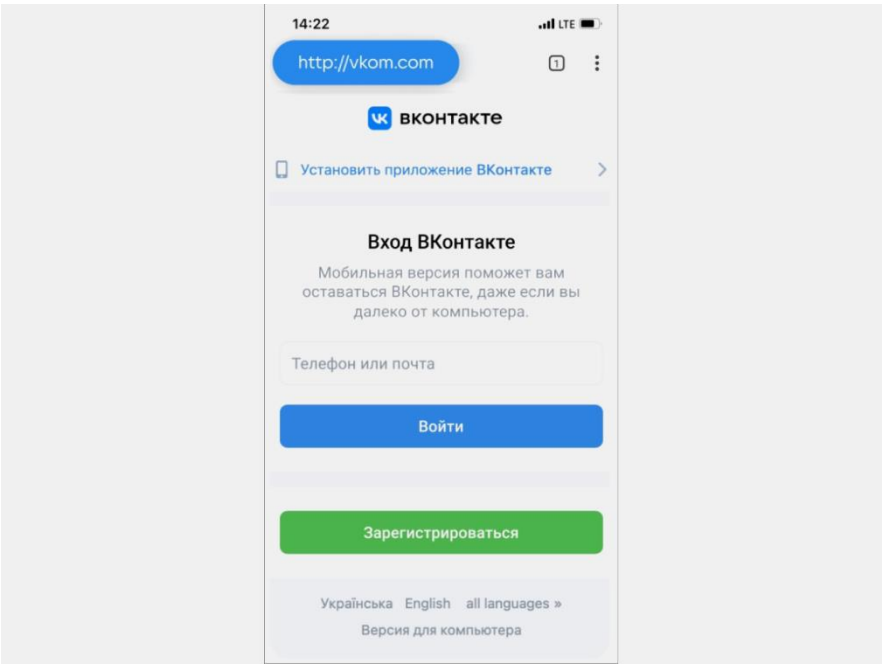


Пример фишингового письма

Человек может решить, что он получил запрос от Google: есть логотип компании, официально написанный текст, подпись в письме и почтовый ящик, намекающий на связь с компанией. Но почтовый ящик с доменом gmail.com может зарегистрировать любой пользователь. Если навести курсор на текст, на который поставили ссылку, то видно, что она ведёт на сайт с доменом .ru, который не имеет ничего общего с Google.

Оказывается, фишинговые письма существовали задолго до появления интернета и распространялись обычной почтой. Как правило, мошенники просили у получателя поучаствовать в многомиллионных операциях, а взамен обещали процент от сделки. Из-за того, что такой вид мошенничества был особенно популярен в Нигерии, письма стали называться «нигерийскими», а ложная выгода, которую сулили отправители таких писем, — «наследством нигерийского принца».

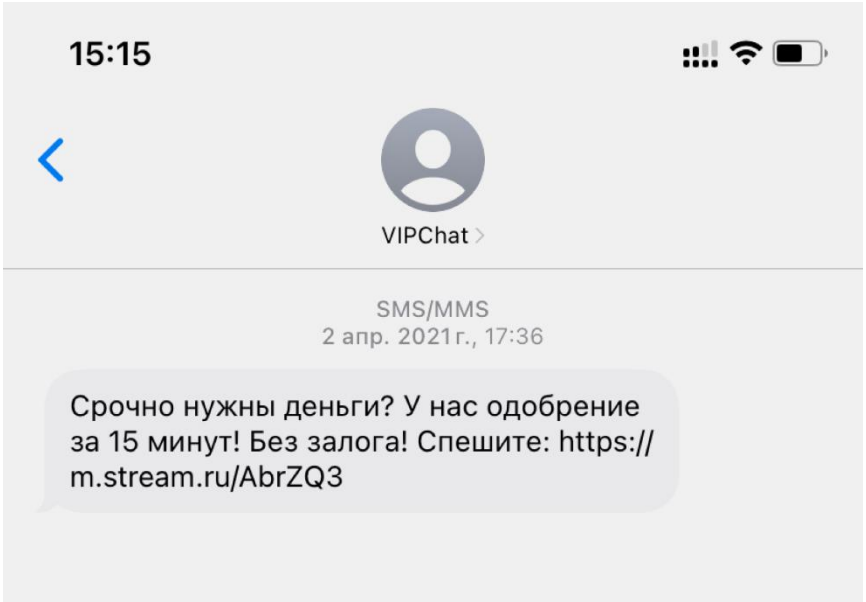
Фишинговый сайт делают похожим на веб-страницу популярного сервиса. Если не обратить внимания на его адрес, то можно и не заметить разницы:



Пример фишингового сайта социальной сети

Форма для авторизации выглядит так же, как и на официальном сайте VK. Но вместо привычного vk.com в адресной строке видим vkom.com. Здесь лучше не авторизовываться — логин и пароль попадут в руки мошенников.

Фишинговое сообщение работает так же. Это СМС или сообщение в социальных сетях, которые заставляют пользователя совершить необходимое мошенникам действие — перейти по ссылке или перезвонить на их номер.



Фишинговое сообщение, обещающее лёгкое получение денег. Как правило, на таком сайте попросят ввести данные карты, включая CVV-код, для её пополнения, а затем код из СМС с подтверждением операции

С

Реже фишинг проводят по телефону, звоня человеку. В этом случае мошенники звонят и представляются сотрудниками компании, например службы безопасности банка. Но цель одна и та же — получить идентификационные данные человека.

Цели фишинга.

Фишеры, то есть мошенники, которые занимаются фишингом, преследуют разные цели.

Кража

Идентификационные данные, например номер телефона, можно использовать для кражи денег пользователей. Мошенники, представляясь сотрудниками службы безопасности банка, сообщают человеку, что кто-то пытается привязать к его карте другой номер телефона. И предлагают провести с карты идентификационный перевод для подтверждения личности. Пользователю нужно сообщить «сотрудникам банка» данные карты и код подтверждения, который придёт в СМС или пуш-уведомлении. Так фишеры могут похитить деньги с карты.

Есть и другие схемы, например «перевод по ошибке». Мошенники присылают фейковое сообщение, маскируясь под банковское приложение, с якобы ошибочным переводом, а затем от имени банка просят вернуть деньги. Чтобы это сделать, опять же потребуется сообщить данные карты и код подтверждения операции.

Фишингу могут подвергаться не только отдельные люди, но и целые компании. В период с 2013 по 2015 год мошенники обманули «Фейсбук»* и Google на 100 миллионов долларов. Фишер воспользовался тем, что обе компании использовали тайваньскую компанию Quanta в качестве поставщика. Злоумышленник выдал себя за представителя компании и отправил компаниям серию фальшивых счетов, которые оплатили и «Фейсбук»*, и Google.

В итоге мошенничество было раскрыто, а злоумышленник был арестован. Но удалось вернуть лишь 49,7 млн долларов из 100.

Шантаж

Мошенники могут взломать облачные хранилища человека, например на «Яндекс Диске», или получить доступ к файлам его телефона. В таком случае киберпреступники шантажируют жертву, например, украв интимные фотографии и угрожая выложить их в открытый доступ. Скандалы со взломом телефонов знаменитостей и распространением личных фотографий сегодня не редкость. Продавая снимки таблоидам, мошенники могут хорошо заработать.

В 2017 году фишеры похитили фильм Disney и требовали за него выкуп. Disney не разглашала информацию о том, что это за фильм и сколько потребовали мошенники. Но, скорее всего, речь шла о пятой части «Пиратов Карибского моря». Хакеры угрожали слить фильм в Сеть, если компания не заплатит им. В итоге этого не случилось, а в интернете появились только его отдельные фрагменты. Видимо, компания смогла договориться со злоумышленниками.

Месть

В 2014 году группа киберпреступников из КНДР, называющих себя «Миротворцами», атаковала компанию Sony Pictures. Они использовали фишинговые письма, а также внедрились в офис Sony, устроившись на работу в качестве IT-специалистов. Так им удалось заразить сотни компьютеров вредоносными программами и похитить более 30 000 файлов: документов, имейлов и сценариев будущих фильмов.

Причина кибератаки — планы кинокомпании выпустить в прокат фильм, высмеивающий северокорейского лидера Ким Чен Ына.

Виды фишинга.

Фишинг — это не только ссылки в электронных письмах и СМС. Арсенал злоумышленников постоянно растёт, так как о старых способах узнаёт всё больше людей. Разберём основные варианты фишинговых атак.

Социальный фишинг

Это фишинговые атаки, целью которых являются аккаунты в популярных соцсетях, например VK или «Одноклассниках».

Мошенники создают фейковую страницу входа в соцсеть и приглашают человека перейти по ссылке. Для этого они отправляют на его электронную почту письмо о том, что кто-то пытается войти в аккаунт и требуется срочно подтвердить пароль для его защиты.

Как только человек вводит данные на фейковом сайте, фишеры получают доступ к его аккаунту. Затем страница перенаправляет пользователя на настоящий сайт соцсети, и он может даже не заметить, что изначально был не там. Другая опасность в том, что, если человек использует одни и те же логины и пароли в других соцсетях и сервисах, то фишеры получат доступ и к ним.

Сделать так, чтобы сообщения от мошенников выглядели настоящими, не так уж и сложно. Невнимательный пользователь может не заметить разницы. Например, у официального сайта LinkedIn есть несколько доменов электронной почты, включая linkedin@**e**.linkedin.com и linkedin@**el**.linkedin.com. Поэтому сложно проверить, какие домены в самом деле принадлежат LinkedIn, а какие нет.

То же касается и других сетей — нужно внимательно проверять адрес отправителя письма и адрес страницы, где вы вводите свои данные: vk.com — это настоящий сайт, а vkom.com — подделка.

Фишинг-атаки на электронную почту

Мошенники отправляют электронные письма с поддельными ссылками, которые выглядят как официальные письма от банков, онлайн-магазинов или сервисов. При переходе по ссылке пользователь попадает на поддельный сайт, где требуется ввести информацию для входа в аккаунт. В итоге мошенники могут получить доступ к личным данным.

Такой вид мошенничества встречается реже, так как современные почтовые сервисы имеют надёжные спам-фильтры и отправляют подозрительные письма в папку со спамом. Открывать их там точно не стоит.

Байтинг

Байтинговые атаки побуждают жертв перейти по ссылке в письме или сообщении без запугивания. Наоборот, они обещают призы и выгодные предложения. Например, пользователю может прийти письмо от Apple с поздравлением и сообщением о выигрыше новой модели iPhone. Сложно удержаться и не перейти по ссылке, чтобы получить приз.

Фарминг

Фарминг — это форма фишинга, которая направлена на получение личных данных через поддельные сайты. Кажется, что это похоже на классический фишинг, но есть различие. В фарминге пользователя автоматически перенаправят на поддельный сайт, даже если он зашёл по проверенной ссылке. Это происходит из-за вируса, который устанавливает вредоносный код на DNS-сервер.

Для фарминговой атаки не обязательно заражать компьютер через email. Хакеры могут «отравить» сам DNS-сервер и атаковать сразу большое число жертв. При вводе пароля или данных карт мошенники легко их похитят без подозрений со стороны пользователей.

Целевой фишинг, или спирфишинг

Обычно фишинг носит массовый характер. Но спирфишинг — это целенаправленная попытка украсть конфиденциальную информацию у конкретной жертвы. Часто целями спирфишинга являются топ-менеджеры крупных компаний, которые могут инвестировать большие средства в кибербезопасность: хакерам не пробиться к ним с помощью технических средств. Но лазейка в виде человеческого фактора остаётся всегда.

Для успешного целевого фишинга преступникам нужно изучить жертву: с кем она общается, где живёт, работает, куда ходит отдыхать или заниматься спортом. Затем злоумышленники притворяются другом или другим важным лицом, например начальником, чтобы получить конфиденциальную информацию, как правило, по электронной почте или через другие онлайн-сообщения. Именно на спирфишинговые атаки приходится 65% всех успешных кибератак на компании.

Например, крупная французская кинокомпания Pathé потеряла 19 млн евро, то есть 10% годовой прибыли, именно из-за спирфишинга. Мошенники использовали личную учётную запись генерального директора Марка Лакана, чтобы получить одобрение на перевод крупной суммы. Перевод состоялся, а генерального директора в итоге уволили.

Голосовой фишинг, или вишинг

Это фишинговые атаки по телефону. Мошенники могут выдавать себя за представителей банков и государственных учреждений. Некоторые из них используют имитацию голоса родных и друзей с помощью искусственного интеллекта. Так вишеры пытаются выманить у жертвы деньги напрямую, например через перевод на карту мошенника.

Кто чаще становится жертвой фишинга

Жертвами фишинга может стать любой человек, независимо от возраста, пола или социального статуса. Если вы откроете папку для спама в своей электронной почте, то наверняка обнаружите не одно подозрительное письмо.

Однако часто мошенники ориентируются на людей, которые хуже разбираются в современных технологиях или не знают о фишинг-атаках, например на пожилых людей и детей. Поэтому важно делиться с близкими информацией о том, что такое фишинг и что делать, чтобы не попасться на уловки мошенников.

Среди сервисов чаще всего страдают банки и электронные платёжные системы, то есть те сервисы, которые работают с деньгами.

Как защититься от фишинговых атак.

Для защиты от фишинга важно помнить несколько базовых правил.

Не отвечайте на подозрительные сообщения

Фишинговые атаки часто начинаются через электронную почту, сообщения в социальных сетях или мессенджерах. Мошенники используют разные способы, чтобы убедить человека предоставить им личные данные или перевести деньги. Никогда не отвечайте на подозрительные сообщения и не переходите по ссылкам, которые вы не запрашивали.

Проверьте адрес отправителя

Мошенники могут подделать адрес отправителя, чтобы сделать письмо более правдоподобным. Однако если вы внимательно посмотрите на него, то обнаружите, что он не соответствует официальному адресу компании. Если сомневаетесь в подлинности письма, обратитесь в службу поддержки компании и уточните информацию.

Используйте антивирусы и определители номеров

Антивирусное программное обеспечение помогает защитить компьютер от спам-сообщений, а определитель номеров — от звонков, которые используют для фишинговых атак. Обновляйте своё антивирусное ПО регулярно, чтобы защитить себя от новых видов угроз.

Используйте разные пароли для разных сайтов

Многие люди используют один пароль для всех сервисов. Это удобно, но, насколько бы он ни был сложным, узнав его, злоумышленники смогут авторизоваться на всех сайтах, которыми пользуется человек.

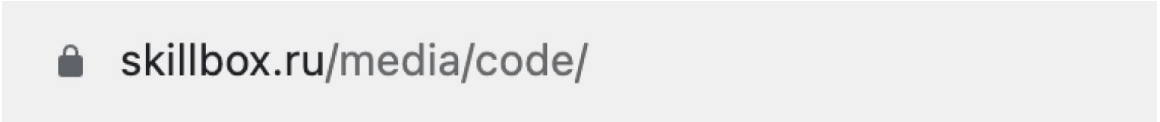
Важно, чтобы пароли всегда были уникальными. Если вам сложно их запомнить, то используйте специальные приложения: Kaspersky Password Manager, «Пассворк» и другие.

Настройте двухфакторную аутентификацию

Почтовый ящик, для доступа к которому используется мобильный телефон, тоже может быть взломан. Мошенники могут перехватить SMS-уведомления и всё равно войти в ваш аккаунт. Однако сделать это будет сложнее, а далеко не все мошенники технически подкованы.

Будьте осторожны, совершая онлайн-покупки

При покупке товаров или услуг убедитесь, что сайт использует безопасный протокол передачи данных, — в строке с адресом сайта должно быть написано https, а не http. Такие сайты в адресной строке браузера обозначаются символом замка:



Если нажать на него, то можно увидеть информацию о сертификате безопасности: наименование организации, которой он принадлежит, и его срок действия.

Никогда не вводите свои платёжные данные на сайтах, которым вы не доверяете. Заведите отдельную банковскую карту для покупок в интернете и не храните на ней большую сумму денег.

Обновляйте программное обеспечение

Обновление операционной системы, браузера и других программ позволяет повысить их защищённость. Как правило, в новых версиях устраняются выявленные уязвимости.

Будьте осторожны, когда используете общественный Wi-Fi

Общественные Wi-Fi-сети могут быть небезопасными, так как мошенники часто используют их для доступа к личным данным людей. Любая операция через такую сеть может привести к перехвату информации, например данных банковских карт.