Фишинг: как распознать и не стать жертвой мошенников

Очень важно уметь защищаться от фишинга, поскольку киберпреступники все чаще прибегают к онлайн-мошенничеству для кражи персональных данных. Мы уже научились различать спам, однако фишинговые письма часто выглядят обманчиво правдоподобными. Иногда они даже содержат персональное обращение. Поскольку рано или поздно вы непременно столкнетесь с фишинговой атакой, важно знать, на какие признаки следует обращать внимание. Мошенничество в интернете – обычное явление, но выявить фишинг иногда бывает сложнее, чем кажется.

С помощью фишинга интернет-мошенники во всем мире выманивают у ничего не подозревающих жертв банковские реквизиты, паспортные данные и прочую информацию. При этом они используют все более изощренные способы маскировки. Они могут выдавать себя за ваших знакомых и доверенных лиц: коллег, сотрудников банка и даже представителей государственных органов. Стоит вам перейти по фишинговой ссылке, и вы можете стать следующей жертвой злоумышленников.

Прежде чем говорить о способах защиты от фишинга, давайте ответим на несколько важных вопросов.

- Могу ли я стать жертвой фишинговой атаки?
- Какие бывают виды фишинга?
- Как распознать фишинг?
- Что такое фишинговое письмо?
- Что делать, если я получил фишинговое письмо?
- Как не стать жертвой фишинга?

Что такое фишинг?

Фишинг – это такой вид мошенничества, когда злоумышленник вынуждает вас совершить действие, позволяющее ему получить доступ к вашему устройству, учетным записям или персональным данным. Выдавая себя за человека или говоря от имени организации, которым вы доверяете, мошенник легко может заразить ваше устройство вредоносным ПО или украсть реквизиты вашей банковской карты.
Другими словами, при помощи методов социальной инженерии он ловит вас на наживку доверия, чтобы получить ценную информацию. Это может быть что угодно: от учетной записи в соцсетях до полной идентификации вашей личности с помощью паспортных данных.
Используя эти методы, мошенник принуждает вас открыть вложение, перейти по ссылке, заполнить форму или сообщить ему персональные данные. Следовательно, нужно постоянно быть начеку, что может быть довольно утомительно.

Самый распространенный сценарий фишинга выглядит следующим образом.

- Вы открываете электронную почту и обнаруживаете там фишинговое письмо с уведомлением от вашего банка. Перейдя по ссылке в письме, вы попадаете на веб-страницу фишингового сайта, которая выглядит похожей на сайт вашего банка.

- Это и есть наживка: мошенники специально создали эту страницу, чтобы похитить ваши данные. В банковском уведомлении будет сказано, что с вашей учетной записью возникла проблема и вам нужно подтвердить логин и пароль.
- После того как вы вводите свои учетные данные на открывшейся странице, вас обычно перенаправляют на настоящий сайт банка, чтобы вы ввели данные повторно. Именно поэтому вы не сразу понимаете, что ваши данные были похищены.

Мошенники могут быть очень изобретательными и использовать все каналы коммуникации, в том числе **телефонные звонки**. Опасность фишинга в том, что попасться на крючок может любой человек, если он недостаточно внимателен к мелким деталям.
Чтобы защитить себя, не впадая при этом в паранойю, давайте разберемся, как происходят фишинговые атаки.

Как происходит фишинг?
Мишенью для фишинга может стать любой пользователь интернета или телефонной связи. С помощью фишинга мошенники обычно пытаются сделать следующее:

- заразить ваше устройство вредоносным ПО;
- похитить конфиденциальную информацию, чтобы получить доступ к вашим деньгам или персональным данным;
- получить доступ к вашим учетным записям;
- убедить вас добровольно перевести деньги или другие ценности.

Иногда под угрозой оказываетесь не только вы лично. Если злоумышленник получает доступ к вашей электронной почте, списку контактов или аккаунтам в соцсетях, он может рассылать вашим знакомым фишинговые письма от вашего имени.
Доверие к тому, кто звонит, и срочность вопроса – вот на что делается ставка в фишинге, и именно это делает его опасным и позволяет обмануть вас. Если преступнику удается заручиться вашим доверием и убедить вас действовать быстро, ничего не обдумав, вы становитесь легкой жертвой.
Кто рискует стать жертвой фишинговых атак?
Любой человек, независимо от возраста, может стать жертвой фишинга – дома или на работе.
Устройствами, подключенными к интернету, сегодня пользуются все от мала до велика. Если мошенник обнаружит в открытом доступе вашу контактную информацию, он может внести ее в список адресов для фишинга.
Сейчас сложно скрыть свой номер телефона, адрес электронной почты, идентификаторы в мессенджерах или аккаунты в соцсетях. Так что шансы стать мишенью для атаки с использованием одного из каналов связи из этого списка довольно велики. Кроме того, мошенники могут адресовать свои фишинговые атаки не только широкому кругу людей, но и конкретным лицам.
Фишинг с помощью спам-рассылки – это широко раскинутая сеть, в которую может попасть любой ничего не подозревающий человек. К этой категории относится большинство фишинговых атак.
Проще говоря, спам – это электронный аналог бумажной рекламы, которую бросают в ваш почтовый ящик. Но если бумажная реклама просто раздражает, то спам может быть опасен, особенно если он является частью фишинговой схемы.
Фишинговый спам массово рассылают мошенники и киберпреступники, которые преследуют следующие цели:

- выудить деньги хотя бы у небольшого количества адресатов, ответивших на сообщение;
- обманным путем получить пароли, номера карт, реквизиты банковских аккаунтов и другую информацию;
- внедрить вредоносный код на компьютеры своих жертв.

Фишинг с помощью спам-рассылки – это один из самых популярных способов, которыми пользуются мошенники, чтобы заполучить ваши данные. Однако некоторые атаки имеют более точную цель.

Какие бывают виды фишинга?

Прежде всего нужно знать, чего следует ожидать от фишинга. Фишинговая атака может быть осуществлена самыми разными способами, включая телефонные звонки, sms-сообщения и даже со взломанных вполне легальных сайтов.

Фишинг гораздо легче распознать, если вы уже видели его в действии. Скорее всего, вы уже встречались с тем или иным видом фишинга, но просто игнорировали его как обычный спам.

Мошенники пытаются достигнуть своей цели разными путями, поэтому **большинство людей, вероятно, сталкивались хотя бы с одним из видов фишинга**, перечисленных ниже.

- **Почтовый фишинг.** Фишинговые письма приходят на вашу электронную почту и, как правило, содержат предложение перейти по ссылке, совершить платеж, прислать личные данные или открыть вложение. При этом адрес отправителя может быть очень похож на подлинный, а в письме может содержаться информация, которую вы воспринимаете как личную.
- **Подделка доменного имени.** Это популярный способ, с помощью которого злоумышленники имитируют подлинные адреса электронной почты. Для этого они берут доменное имя реально существующей компании (например, @america.com) и слегка меняют его. Вы можете отреагировать на письмо с обратным адресом, к примеру, @arnerica.com и таким образом стать жертвой мошеннической схемы.
- Голосовой фишинг, или вишинг (vishing). Мошенники звонят по телефону и выдают себя за реально существующего человека или компанию. Они могут использовать перенаправление с помощью автоматического помощника и маскировать свой номер телефона. Их задача – не дать вам повесить трубку и добиться от вас определенных действий.
- **SMS-фишинг, или смишинг (smishing)**. Как и в случае вишинга, мошенники выступают от имени реально существующей компании и имитируют срочную проблему, но делают это с помощью SMS-сообщений. В таком сообщении обычно содержится ссылка или телефонный номер, которыми вам предлагают воспользоваться. Пользователи онлайн-мессенджеров также рискуют оказаться жертвами подобной атаки.
- **Фишинг в соцсетях.** В этом случае киберпреступники заманивают вас в ловушку с помощью постов или личных сообщений. В одних сообщениях предлагаются бесплатные подарки, другие представляют собой примитивные подделки под официальные страницы различных организаций, где содержатся какие-либо срочные требования. Мошенники могут действовать от лица ваших друзей или долго и методично выстраивать с вами отношения, прежде чем перейти в атаку.
- **Клон-фишинг (clone phishing).** Злоумышленники копируют реальные письма, которые вы уже получали ранее, при этом заменяют настоящие вложения и ссылки на вредоносные. В основном они делают это через электронную почту, но иногда создают для этого поддельные аккаунты в социальных сетях и мессенджерах.

В некоторых случаях с целью фишинга злоумышленники могут подделывать или видоизменять легальные веб-сайты.

- **Водопой (watering hole).** Средством для этой разновидности фишинга служат популярные сайты с большим количеством посетителей. Мошенники пытаются

эксплуатировать уязвимости таких сайтов для осуществления разнообразных атак. Эти схемы обычно связаны с рассылкой вредоносного ПО, перенаправлением по вредоносным ссылкам и т. п.

- Фарминг (pharming), или **отравление кеша DNS.** Мошенники перенаправляют трафик с безопасного веб-сайта на фишинговую страницу с помощью вредоносного ПО или используя уязвимости самого сайта. Если веб-сайт стал жертвой фарминга, то даже если посетители вручную вводят его веб-адрес, они все равно попадают на вредоносный сайт.
- **Тайпсквоттинг (typosquatting), или перехват веб-адресов.** В этом случае мошенники пытаются ловить людей, которые ошибаются при вводе веб-адреса. Например: злоумышленники создают поддельный фишинговый сайт, адрес которого всего на одну букву отличается от настоящего. Если вы ошибетесь и напечатаете в адресе «wallmart» вместо «walmart», вы можете оказаться на таком вредоносном сайте.
- **Кликджекинг (clickjacking).** Мошенники используют уязвимости веб-сайтов для встраивания скрытых ловушек. С их помощью осуществляется перехват логинов, паролей и любой другой информации, оставленной вами на сайте, который в остальном является совершенно безопасным.
- **Табнабинг (tabnabbing).** Это тактика, когда мошенническая веб-страница при отсутствии вашей активности перезагружается на страницу ввода пароля, имитирующую легальный сайт. Вернувшись на страницу, вы можете принять ее за настоящую, ввести учетные данные и таким образом дать злоумышленникам доступ к вашему аккаунту.
    - **HTTPS-фишинг.** В этом случае мошенническая страница маскируется под защищенный веб-сайт с помощью классического изображения замка в начале адресной строки. Если раньше этот знак зашифрованного соединения появлялся исключительно на сайтах с подтвержденным сертификатом безопасности, то теперь его может получить любой веб-сайт. Таким образом, ваше соединение и передаваемая вами информация может быть закрыта для посторонних, однако сами вы оказываетесь на фишинговом сайте, принадлежащем киберпреступнику. Даже ваше текущее интернет-соединение может оказаться небезопасным.
- **«Злой двойник» (evil twin).** Мошенники имитируют действующие публичные сети Wi-Fi в общественных местах, таких как кофейни или аэропорты. Их цель – заставить вас подключиться к своей сети и отследить все ваши действия.

И еще несколько видов фишинга, о которых следует знать.

- **Фишинг в поисковых системах.** В этом случае мошенники манипулируют результатами поисковой выдачи, так что поддельные страницы появляются в них раньше, чем настоящие. Такой вид фишинга еще называется SEO-фишинг или SEM-фишинг. Если вы будете невнимательны, вы можете оказаться на вредоносной странице вместо настоящей.
- **Англер-фишинг (angler phishing).** Мошенники представляются сотрудниками службы поддержки реально существующей компании, чтобы выманить у вас информацию. При упоминании вами в соцсетях компании с использованием значка @, мошенники отмечают это и отправляют вам поддельный ответ от имени службы поддержки компании.
- **Взлом корпоративной почты (Business email compromise, BEC).** Этот метод включает в себя различные способы взлома корпоративных каналов коммуникации для получения ценной информации. Мошенник может представляться руководителем компании или выдавать себя за поставщика услуг, пытаясь инициировать денежный перевод с помощью поддельного счета-фактуры.

- **Криптовалютный фишинг.** Этот вид мошенничества нацелен на держателей криптокошельков. Вместо того чтобы долго и нудно заниматься майнингом криптовалюты, преступники пытаются украсть ее у тех, кто ею уже владеет.

Таким образом, разновидностей фишинга существует множество и список постоянно пополняется. Мы перечислили самые распространенные виды атак на сегодняшний день, но уже через несколько месяцев могут появиться новые их виды.

Мошеннические схемы быстро меняются с учетом текущих реалий, поэтому их бывает так сложно распознать. Однако способы защиты существуют, и для начала необходимо быть в курсе наиболее свежих примеров таких схем.

Несколько типичных фишинговых схем

Невозможно перечислить все известные фишинговые схемы, так что отметим самые типичные, которых следует опасаться.

Иранская кибератака. Злоумышленники присылают письмо с поддельного адреса Microsoft и предлагают войти в систему для восстановления якобы заблокированного в целях безопасности аккаунта. После этого они похищают ваши учетные данные к аккаунту Microsoft. Мошенники рассчитывают на ваш страх потерять доступ к ОС Windows, а для большей правдоподобности используют актуальную новостную повестку.

Уведомление об удалении файлов от Microsoft Office 365. Это еще один вид мошенничества с целью получить ваши учетные данные к аккаунту Microsoft. Вам приходит письмо с информацией, что из вашего аккаунта был удален большой объем файлов. Для восстановления вам предлагают ссылку для входа в аккаунт, что, конечно, приводит к утечке ваших учетных данных.

Банковское уведомление. Мошенники пытаются ввести вас в заблуждение с помощью поддельного уведомления от банка. Обычно в таком письме содержится ссылка на веб-форму, где вам предлагают ввести банковские реквизиты для верификации аккаунта. Никогда не делайте этого. Свяжитесь со своим банком, чтобы там могли принять меры в связи с этим мошенническим письмом.

Письмо от друга. Мошенники представляются вашим другом, который якобы находится за границей и нуждается в вашей помощи. Эта «помощь», как правило, заключается в денежном переводе. Прежде чем отправить деньги, позвоните другу, чтобы проверить информацию.

Выигрыш или наследство. Получив сообщение о том, что вы неожиданно выиграли приз или получили наследство от незнакомого родственника, не спешите радоваться. Скорее всего, это мошенническое письмо, в котором от вас потребуют перейти по ссылке и ввести свои личные данные для получения приза или верификации права на наследство.

Возврат налога или бонус. Это популярный сценарий мошенничества, поскольку большинство людей ежегодно платят налоги. Обычно в таких фишинговых сообщениях говорится, что вы либо имеете право на возврат части налога, либо к вам есть вопросы у налоговой инспекции. Вам предлагают оформить запрос на возврат налога или заполнить налоговую декларацию (с указанием полных данных). После этого злоумышленники либо похищают ваши деньги, либо продают ваши личные данные третьим лицам, либо и то и другое.

Как выглядит фишинговое письмо?

Опасность фишинговых писем (и, к сожалению, их эффективность) заключается в том, что их специально делают похожими на настоящие. Вот типичные признаки фишингового письма, которые должны вас насторожить:

- наличие вложений или ссылок;
- ошибки и опечатки;
- неправильные грамматические конструкции;
- непрофессиональная графика;

- требование немедленно подтвердить адрес электронной почты или другие личные данные;
- универсальное, безличное обращение, например «Уважаемый клиент».

Злоумышленники часто торопятся побыстрее запустить фишинговые сайты, поэтому некоторые из них могут значительно отличаться от сайтов настоящих компаний. По этим признакам вы можете отличить вредоносное письмо.

Что же делать, если фишинговое письмо все же преодолело ваш спам-фильтр и попало в ваш ящик?

Что делать, если вы обнаружили фишинговое письмо?

Главное – быть настороже и быть готовым распознать признаки фишинга. Если такое письмо не было автоматически отфильтровано как спам и попало в ваш почтовый ящик, действуйте следующим образом.

- **Удалите письмо, не открывая его.** Вирусы чаще всего активируются, когда вы открываете вложение или нажимаете на ссылку в фишинговом письме. При этом некоторые почтовые клиенты поддерживают скрипты, и в таком случае можно заразиться, просто открыв подозрительное письмо. Так что лучше вообще такие письма не открывать.
- **Заблокируйте отправителя вручную.** Если почтовый клиент позволяет вам вручную блокировать отправителей, так и поступайте. Отметьте домен электронной почты отправителя и добавьте его в список заблокированных. Особенно важно это сделать, если почтовым ящиком пользуются другие члены вашей семьи. Иначе письмо, которое не попало в спам и выглядит безобидно, может обнаружить кто-то еще и поддаться на уловку.
- **Установите дополнительный уровень защиты.** Предосторожность никогда не бывает лишней. Подумайте о приобретении антивирусного ПО. Оно поможет поддерживать безопасность почтового ящика.

Помните: при обнаружении фишингового письма лучше всего его **немедленно удалить**. Любые дополнительные действия по ограничению рисков – на ваше усмотрение.

Кроме удаления вредоносного письма, есть еще несколько способов обезопасить себя от фишинга.

Рекомендации по защите о фишинга

Хотите вы этого или нет, фишинговые письма будут присылать вам каждый день.

Большинство из них автоматически отправляется в спам почтовыми сервисами, да и сами пользователи большей частью научились распознавать такие письма и руководствоваться здравым смыслом, не поддаваясь на их уловки.

Однако вы уже поняли, каким коварным может оказаться фишинг. Вы уже знаете, что фишинговые атаки задействуют не только электронную почту, но и все каналы коммуникации и веб-поиска.

Если вы будете следовать нескольким простым рекомендациям, вы значительно уменьшите свои шансы оказаться жертвой мошенников.

Меры предосторожности для защиты от фишинга

Ваша безопасность в интернете начинается с вашего отношения к потенциальным киберугрозам и правильного поведения.

С помощью фишинга мошенники обманом заставляют своих жертв сообщить им логины и пароли к разнообразным аккаунтам, таким как электронная почта, учетная запись во внутренней сети предприятия и т. п.

Даже осторожные пользователи не всегда могут распознать фишинговую атаку. С течением времени такие атаки становятся все более изощренными. Мошенники изобретают все новые схемы и сочиняют более чем убедительные письма, заманивая людей в ловушку.

Вот некоторые меры предосторожности, которые нужно всегда соблюдать при работе с электронной почтой и другими каналами коммуникации.

- **<u>Руководствуйтесь здравым смыслом,</u> прежде чем сообщать кому-либо конфиденциальную информацию.** Получив уведомление от банка или другой крупной организации, никогда не переходите по ссылкам в письме. Вместо этого введите веб-адрес в адресную строку вручную. Так вы убедитесь, что заходите на настоящий сайт организации.
- **Никогда не верьте тревожным сообщениям.** Известные компании не будут запрашивать у вас идентификационные или учетные данные по электронной почте. Это касается, в том числе, вашего банка, страховой компании или любой другой организации, с которой вы ведете дела. Если вы получите письмо с просьбой предоставить такую информацию, сразу удалите его и позвоните в компанию, чтобы убедиться в безопасности своего аккаунта.
- **Не открывайте вложения**, содержащиеся в подозрительных письмах или письмах от неизвестного адресата, особенно файлы в форматах Word, Excel, PowerPoint или PDF.
- **Никогда не переходите по ссылкам в письме**, поскольку это может привести к загрузке вредоносного ПО. С осторожностью относитесь к письмам от поставщиков или третьих лиц. Никогда не переходите по содержащимся в них ссылкам. Вместо этого зайдите на сайт поставщика, введя его веб-адрес вручную, и ознакомьтесь с его правилами и политиками в отношении запроса информации у контрагентов.
- **Своевременно обновляйте ПО и операционную систему.** Продукты для операционной системы Windows часто становятся мишенью для фишинга и других вредоносных атак, так что убедитесь, что они надежно защищены и своевременно обновляются. Особенно если у вас установлены более ранние версии ОС, чем Windows 10.