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

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.

Целевой фишинг

Когда говорят о **целевом (таргетированном) фишинге**, обычно имеют в виду целенаправленный фишинг (spear phishing) или его наиболее распространенную разновидность – уэйлинг (whaling).
Уэйлинг нацелен на лиц высокого уровня, в то время как **целевой фишинг** охватывает более широкий круг людей. Мишенями для подобного фишинга обычно становятся сотрудники конкретных предприятий или правительственных организаций. Однако целью мошенников может стать любой человек, который представляется им особенно ценным или легко уязвимым. Вы можете оказаться мишенью, если являетесь клиентом банка, который интересует мошенников, или сотрудником медицинского учреждения. Даже если вы просто откликнулись на предложение дружбы от незнакомого человека в социальной сети, вас могут попытаться поймать на крючок.

При этом мошенники терпеливо выстраивают свои схемы. Чтобы получить вознаграждение или увеличить свои шансы на успех, они тратят много времени на подготовку таких персонализированных атак.

Для этого им может потребоваться информация о вас или об организации, к которой вы имеете отношение.

Эту информацию мошенники могут получить из следующих источников:

- профили в социальных сетях;
- произошедшая ранее утечка данных;
- другая информация в открытом доступе.

Злоумышленник может атаковать вас стремительно и попытаться побудить вас к немедленным действиям. В других случаях он будет выстраивать отношения с вами в течение нескольких месяцев, чтобы завоевать ваше доверие перед тем, как сделать главный бросок.

Мошенники не ограничиваются сообщениями или телефонными звонками. Чтобы достичь своих целей, они могут взламывать вполне легальные сайты. Если вы не будете осторожны, вы можете оказаться на крючке, просто войдя в свой аккаунт на сайте, который ранее был совершенно безопасным.

К сожалению, многие люди оказываются легкой добычей для киберпреступников. По мере того как частота подобных атак возрастает, фишинг, увы, становится нормой нашей повседневной жизни.

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.

Фишинг и другие вредоносные угрозы во время эпидемии COVID-19

Эпидемия COVID-19 подтолкнула кибермошенников задействовать страх в своих новых фишинговых схемах. В одной из самых известных схем используется банковский троянец Ginp, который, проникнув на устройство пользователя, открывает веб-страницу под названием Coronavirus Finder («Найди коронавирус»). Пользователю предлагается заплатить деньги, чтобы узнать, кто из соседей болеет коронавирусом. В результате преступники получают реквизиты банковских карт и исчезают.
Известны также случаи, когда мошенники представляются сотрудниками солидных государственных организаций и даже Всемирной организации здравоохранения (ВОЗ). Они связываются со своими жертвами напрямую, обычно через электронную почту, и предлагают ввести банковские реквизиты или перейти по ссылке. Таким образом они пытаются заразить компьютер вредоносным ПО или похитить личные данные.

Такие письма или сообщения могут выглядеть как настоящие. Однако присмотревшись к указанному в ссылке веб-адресу или адресу отправителя, можно легко заметить признаки подделки. Например, письмо от представителя ВОЗ или государственной организации не может быть отправлено с почтового сервера Gmail. Кстати, при изучении веб-адреса нужно быть осторожным, чтобы случайно не нажать на ссылку.

Не попадайтесь на эту удочку. Организации такого рода никогда не просят предоставить конфиденциальные личные или банковские данные. Вероятность того, что их представители предложат вам загрузить приложение или программу на ваш компьютер, тоже практически нулевая. Поэтому получив подобное письмо, особенно если ничто не предвещало его появления, не переходите по ссылкам и не сообщайте свои личные или банковские данные. Если у вас возникли сомнения, обратитесь в соответствующие органы или в ваш банк. Используйте только доверенные веб-сайты и ресурсы.

Вот что следует делать, если вы получили такое письмо.

1. Проверьте адрес электронной почты отправителя. В электронных адресах сотрудников ВОЗ используется шаблон *person@who.int* и никогда *@gmail.com* и т. п.
2. Проверьте ссылку, прежде чем перейти по ней. Убедитесь, что в начале строки стоит https://, а не http://.
3. Будьте осторожны, сообщая свою личную информацию. Никогда не раскрывайте свои учетные данные третьим лицам, даже если они представляются сотрудниками ВОЗ.
4. Избегайте спешки и панической реакции. Мошенники, рассчитывают на них, чтобы заставить вас перейти по ссылке или открыть вложение.
5. Если вы раскрыли конфиденциальную информацию, не впадайте в панику. Обновите свои учетные данные на всех веб-сайтах, где вы их использовали. Смените пароли и немедленно свяжитесь с вашим банком.
6. Всегда сообщайте о случаях мошенничества.