# Что такое фишинг? Примеры и определение фишинговых атак - Cisco**Фишинг и как ему противостоять**

****

**Фишинг** (англ. *phishing* от *fishing* «*рыбная ловля, выуживание*») — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам, паролям и иной персональной информации. Это достигается путём проведения массовых рассылок электронных писем от имени различных организация, а также личных сообщений внутри сервисов, например, от имени банков или посредством социальных сетей и мессенджеров. В письме зачастую содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом (перенаправлением). После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, реквизиты банковских платежных карт или иные персональные данные, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Таким образом, ***фишинг*** *—* ***одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности***. В частности, многие не знают простого факта: сервисы не рассылают писем с просьбами сообщить свои учётные данные, пароль и иную информацию, а в мессенджерах нельзя получить денежный перевод путем перехода по ссылке.

Большинство методов фишинга сводится к тому, чтобы замаскировать поддельные ссылки на фишинговые сайты под ссылки настоящих организаций. Адреса с опечатками или субдомены часто используются мошенниками. Например «www.kufar.be», «www.bel-post.by» или «www.belarusbank-erip.cc» визуально похожи на адреса реальных организаций, однако на самом деле они ссылается на фишинговые составляющие сайтов «www.kufar.by», «www.belpost.by» и «www.belarusbank.by», соответственно.

Другая распространённая уловка заключается в использовании на иных неофициальных ресурсах внешне правильных ссылок, в реальности ведущих на фишинговый сайт из-за измененного атрибута html-ссылки (использование в HTML-теге <a> значения href, отличного от текста ссылки).

Ещё одна проблема была обнаружена при обработке браузерами интернациональных доменных имён (содержащие символы национальных алфавитов, например: «115.бел», «президент.рф» и т.п.): адреса, визуально идентичные официальным, могли вести на сайты мошенников.

Обман не заканчивается на посещении жертвой фишингового сайта. Некоторые фишеры используют JavaScript для изменения адресной строки. Это достигается либо путём размещения картинки с поддельным URL поверх адресной строки либо закрытием настоящей адресной строки и открытием новой с поддельным URL.

Злоумышленник может использовать уязвимости в скриптах подлинного сайта. Этот вид мошенничества (известный как межсайтовый скриптинг) наиболее опасен, так как пользователь авторизуется на настоящей странице официального сайта, где всё (от веб-адреса до сертификатов) выглядит подлинным. Подобный фишинг очень сложно обнаружить без специальных навыков. Данный метод применялся в отношении такой крупной компании, как PayPal еще в 2006 году.

Сегодня фишинг выходит за пределы интернет-мошенничества, а поддельные веб-сайты стали лишь одним из множества его направлений. Письма, которые якобы отправленные из банка, могут сообщать пользователям о необходимости позвонить по определённому номеру для решения проблем с их банковскими счетами. Эта техника называется вишинг (голосовой фишинг). Позвонив на указанный номер, пользователь заслушивает инструкции автоответчика, которые указывают на необходимость ввести или сказать номер своего счёта, банковской карты, PIN-код или иную информацию. К тому же вишеры могут сами звонить жертвам, убеждая их, что они общаются с представителями официальных организаций, используя фальшивые номера. В конечном счёте, человека также попросят сообщить его учётные данные.

Набирает свои обороты и SMS-фишинг, также известный как смишинг (англ. *SMiShing* — от *«SMS»* и *«фишинг»*). Мошенники рассылают сообщения, содержащие ссылку на фишинговый сайт, — входя на него и вводя свои личные данные, жертва аналогичным образом передаёт их злоумышленникам. В сообщении также может говориться о необходимости позвонить мошенникам по определённому номеру для решения «возникших проблем». Иногда смишинг может предшествовать вишингу, например злоумышленники отправляют sms-сообщение на телефон жертвы от имени банка о попытке транзакции с карты, а потом звонят, представляясь уже сотрудником того же банка и предлагают отменить указанный, якобы мошеннический перевод, для чего просят предоставить реквизиты банковской карты или иную персональную информацию клиента, которая настоящему сотруднику банка и так должна быть известна.



**Как не попасться на уловки фишеров?**

Один из методов борьбы с фишингом заключается в том, чтобы научить людей различать фишинг и бороться с ним. Люди могут снизить угрозу фишинга, немного изменив своё поведение. Так, в ответ на письмо с просьбой «подтверждения» учётной записи (или любой другой обычной просьбой фишеров) необходимо связаться с компанией, от имени которой отправлено сообщение, для проверки его подлинности. Кроме того, рекомендуется самостоятельно вводить веб-адрес организации в адресную строку браузера вместо использования любых гиперссылок в подозрительном сообщении.

Практически все подлинные сообщения организаций содержат в себе упоминание некой информации, недоступной для фишеров. Некоторые, например, всегда обращаются к своим адресатам по именам, а письмо с общим обращением «Уважаемый клиент» может расцениваться как попытка фишинга, однако, даже к электронным письмам, содержащим более подробные данные о себе необходимо относиться с опаской, т.к. эта информация также может стать известна мошенникам иными путями. Письма от банков и кредитных учреждений часто содержат в себе часть номера счёта. Однако, люди не различают появление первых или последних цифр счёта, в то время как первые цифры могут быть одинаковы для всех клиентов финансового учреждения. Людям можно объяснить, что подозрительны любые письма, не содержащие какой-либо конкретной личной информации, но фишинговые атаки могут содержать подробную персональную информацию, следовательно, наличие такого рода сведений не гарантирует безопасность сообщения. Кроме того, статистические показатели гласят, что присутствие личной информации существенно не изменяет процент успеха фишинговых атак, что свидетельствует о том, что большинство людей вообще не обращает внимания на подобные детали.

Стоит помнить, что мошенники идут в ногу со временем, поэтому обычные методы фишинга в скором времени могут стать не актуальными, поскольку люди всё больше узнают о социальной инженерии, используемой фишерами, поэтому в любой ситуации нужно оставаться предельно внимательными и досконально разобраться в случившемся, прежде чем сообщить кому-то свои персональные данные.

