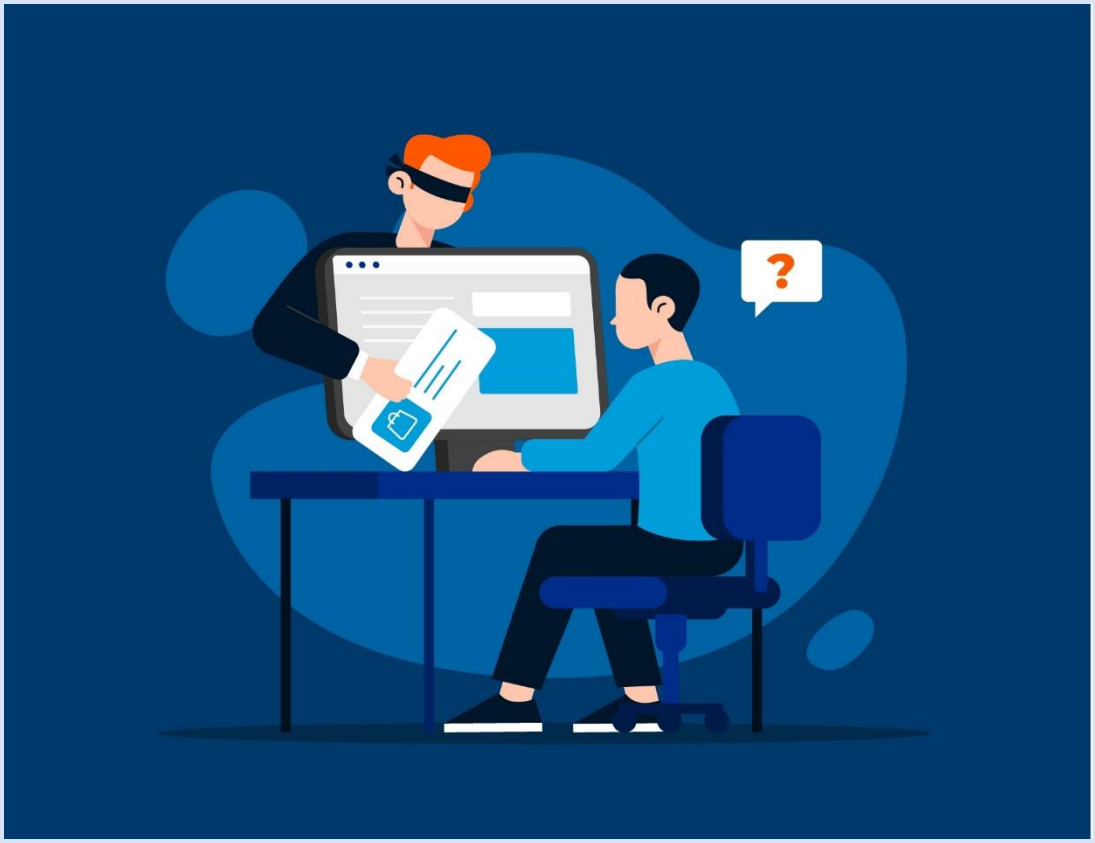
Что такое фишинг и как от него защититься?



Фишинг — вид интернет-мошенничества, целью которого является получение идентификационных данных пользователей (логин, пароль, номер кредитной карты и другой конфиденциальной информации), а также запуск вредоносного программного обеспечения на компьютере пользователя.

Для этого мошенники рассылают сообщения с вредоносными ссылками. По ссылке вас может ждать вирус, вредоносная программа, фишинговый сайт, с помощью которых мошенники украдут ваши логин и пароль, реквизиты банковской карты, информацию об устройстве и другие личные данные.

Злоумышленники могут прислать фишинговую ссылку:

• в сообщении в социальных сетях или мессенджере от имени незнакомого человека или знакомого, взломав его аккаунт;

• в электронном письме от имени якобы реального интернет-магазина, банка, государственного учреждения или другой организации;

• в электронном письме от имени вымышленных организаций. Часто в таких письмах обещают выигрыш.

Такой вид интернет-мошенничества, как правило, основан на психологической манипуляции и его цель - вывести человека на такие эмоции, как интерес, страх, жадность, злость, желание помочь. Подобные действия позволяют ослабить концентрацию человека, усыпить его бдительность.

Обычно злоумышленники формулируют тему письма так, что на него хочется отреагировать, например: «Ваш аккаунт заблокирован», «Срочное сообщение от банка», «Привет! Отправляю обещанные фотографии».

Если вы получили письмо, в котором от вас требуют какого-либо взаимодействия, в том числе незамедлительного, или же такое письмо вызывает у вас любопытство, чувство страха или побуждает к действиям, например, «открой», «прочитай», «ознакомься», то задумайтесь и задайте себе следующие вопросы:

• ожидаю ли я это письмо?

• есть ли смысл в том, что от меня требуют?

• знаю ли я автора этого письма?

• уверен ли я в безопасности полученного электронного письма?

Если ответ хотя бы на один из озвученных выше вопросов «нет» - внимательно проанализируйте содержимое письма.

Чтобы защититься от фишинга:

• не открывайте сомнительные письма о крупных выигрышах, легких викторинах, лотереях и одобренных кредитах;

• не загружайте вложенные файлы из сообщений, которых вы не ожидали;

• не переходите по ссылкам от незнакомых людей, а если ссылку прислал человек, которого вы знаете, позвоните ему и убедитесь, что это он отправил вам сообщение;

• если пришло письмо о том, что вам положена какая-то выплата, возьмите паузу и проверьте информацию в официальных источниках;

• внимательно проверяйте адресную строку сайта, на котором просят ввести ваши данные, название поддельного сайта может отличаться от настоящего на один-два символа. Обращайте особое внимание на название сайта, на который вам предлагают перейти. В нем может быть изменен порядок букв или, например, некоторые буквы могут быть заменены на цифры (например, www.s0branie.ru). Кроме того, для введения в заблуждение злоумышленником могут быть использованы специализированные сервисы сокращения ссылок (например, bit.ly, tinyurl.com);

• проверьте наличие вложений. Если отправитель, электронное письмо и причина, по которой Вас просят открыть вложение, вызывает даже самое незначительное подозрение - ни при каких обстоятельствах не открывайте его;

• не вводите свои персональные данные и данные вашей банковской карты на сомнительных сайтах;

• всегда проверяйте электронный адрес, с которого пришло письмо. Если он отличается от известного вам адреса магазина, банка или другой организации хотя бы одним символом, не открывайте письмо. Если адрес вам не знаком и вы не ждете сообщений от новых адресатов, письмо лучше удалить;

• помните, что ошибки и плохой дизайн, большое количество прописных букв, совпадение названий организации, имени отправителя и содержимого в тексте электронного письма — это признаки поддельного письма, но будьте внимательны, даже если все выглядит идеально;

• при оплате с помощью QR-кода проверяйте, правильно ли указаны реквизиты организации, сумма, которую нужно оплатить, и другие данные в документе и на странице, открывшейся после сканирования кода. Если данные не совпадают, обратитесь в организацию, которая прислала документ, чтобы подтвердить его подлинность;

• не пересылайте письма коллегам, родным, близким и иным лицам;

• удалите фишинговое письмо.

Если вы стали жертвой мошеннических действий, незамедлительно обращайтесь в правоохранительные органы.