Что такое фишинг и как от него защититься?

Фишинг — это вид интернет-мошенничества, который используется для кражи конфиденциальных данных человека.

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

Мошенники 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;

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

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;

• 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 — это признаки поддельного письма, но будьте внимательны, даже если все выглядит идеально;

• следите, чтобы QR-код был напечатан вместе с этикеткой или упаковкой. Если на месте оригинального кода приклеен другой, не сканируйте такой QR-код и сообщите о нем сотруднику магазина;

• 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.

В случае совершения в отношении вас мошеннических действий незамедлительно обращайтесь в правоохранительные органы.