

Что такое фишинг и как от него защититься?

Фишинг - 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 письме вам могут предложить подтвердить аккаунт, чтобы воспользоваться «бонусами». Перейдя по ссылке, вы попадаете на поддельный сайт, интерфейс и адрес которого будут максимально похожи на настоящие. Только, чтобы получить какие-либо «бонусы» вам нужно будет перейти по ссылке, подтвердить аккаунт и заплатить, например, налог или взнос для получения «подарка».

Обычно злоумышленники формулируют тему письма так, что на него хочется отреагировать, например: «Ваш аккаунт заблокирован», «Срочное сообщение от банка» и т.п.

Как 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.

[#мвд](#) [#мвд74](#) [#полиция74](#) [#Челябинскаяобласть](#) [#МВДРоссии](#) [#новости](#) [#ПолицияЮжногоУрала](#) [#полицияКатавИвановскийрайон](#) [#мошенничество](#) [#Будьтебдительны](#)

