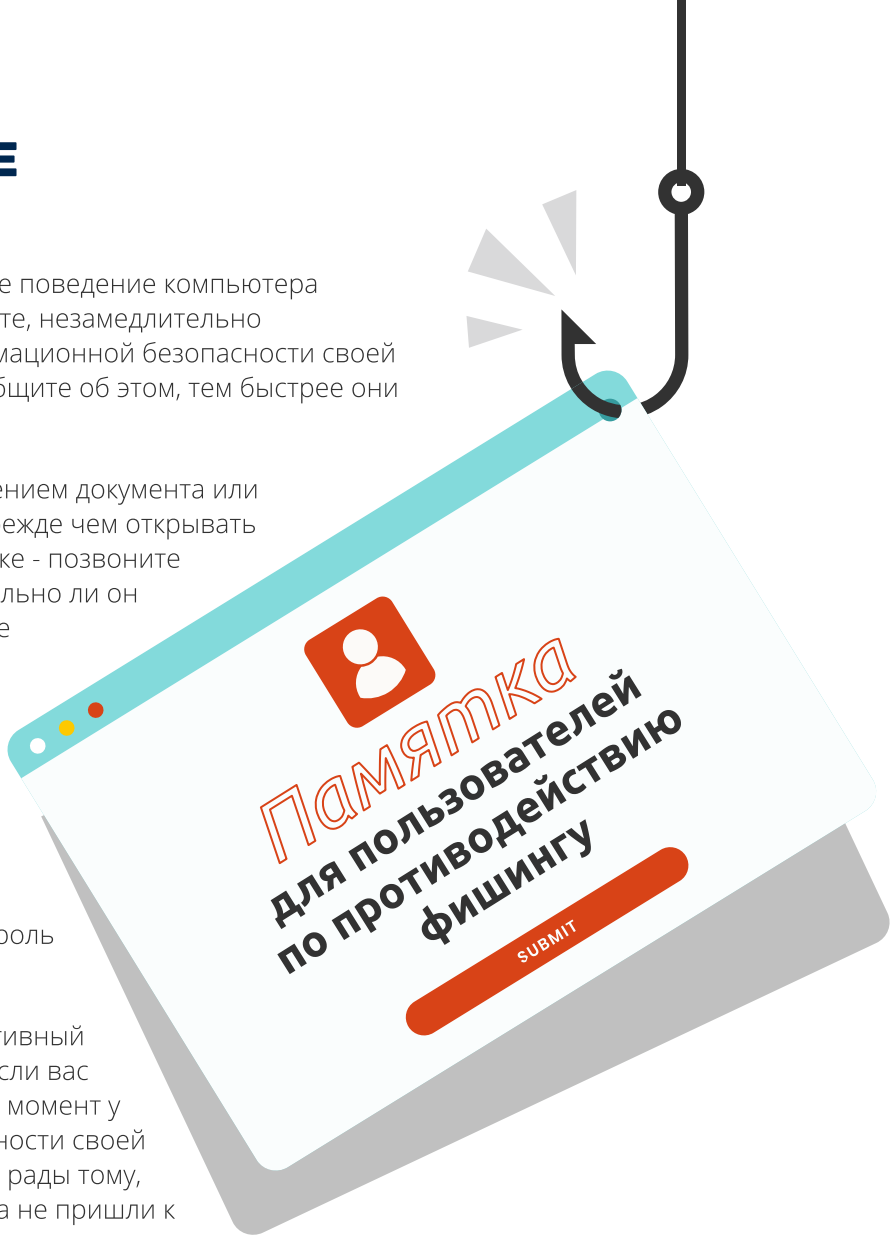
INNOSTAGE



1 Если вы замечаете подозрительное поведение компьютера или подозрительное письмо в почте, незамедлительно сообщите об этом в службу информационной безопасности своей организации. Чем вы быстрее сообщите об этом, тем быстрее они смогут отреагировать.

2 Если вам приходит письмо с вложением документа или ссылки, которое вы не ожидали, прежде чем открывать вложение или переходить по ссылке - позвоните отправителю. Спросите, действительно ли он отправил это письмо? Задайте себе вопрос, а я могу доверять отправителю?

3 Соблюдайте цифровую гигиену:

a. Никогда не храните логины, пароли и другую важную информацию в почте

b. Не сохраняйте в браузере пароль от web-формы входа в почту

4 Никогда не вводите свой корпоративный пароль на сторонних ресурсах, а если вас просят это сделать – уточните этот момент у службы информационной безопасности своей организации. Поверьте, они будут рады тому, что вы спросили это у них сейчас, а не пришли к ним, когда вас «взломали».

5 Никогда не сообщайте пароли по телефону, даже если звонящий представляется сотрудником вашей IT-службы или службы безопасности. Позвоните сами по рабочему номеру в службу безопасности и спросите, почему по телефону спрашивают ваш личный пароль?

Относитесь к своим учетным данным так, как будто это ключи от вашего дома. Вы же не раздаете их всем, кто просит?

Если к вам домой стучат подозрительные люди, то вы вызываете полицию, если к вам приходит подозрительное письмо, то звоните в службу информационной безопасности.

Запишите себе рабочий номер телефона службы информационной безопасности своей организации, чтобы в случае необходимости быстро с ними связаться.

Остались вопросы? Хотели бы провести тестовую фишинговую рассылку для проверки действий сотрудников? Требуется обучение персонала по кибербезопасности?

Свяжитесь с нами и мы поможем с реализацией широкого круга вопросов в области кибербезопасности.

Адрес для запросов: info@innostage-group.ru