8 признаков фишинга, которые должен знать каждый

Источник: https://hi-tech.mail.ru/card/8_phishing_signs/#reference8

Фишинг — один из видов интернет-мошенничества. Цель злоумышленников — спровоцировать пользователя пройти по фальшивой ссылке, чтобы конфиденциальные данные (логин, пароль и т.д.) попали в их руки. Рассказываем, что надо знать, чтобы не попасться на удочку фишеров.

1

Письмо. Кому и от кого?

Если в поле «Куда» указано не ваше имя, значит, это массовая безличная рассылка, где имена в поле «Куда» не имеют отношения к реальности или проставляются методом перебора. И если в поле «От кого» указан неизвестный вам адрес, при этом в самом письме в качестве отправителя указывается сайт хорошо знакомый, значит, письмо пришло вовсе не от той организации, под которую подделываются мошенники. Имейте в виду, ни одна крупная организация не будет посылать письма с бесплатного почтового ящика.

2

Слова искажены

Например, «Lloan» вместо «Loan», «Youwon» вместо «You won». Это один из приемов, которым пользуются спамеры, чтобы обойти спам-фильтры.

3

Dear friend!

Безличные обращения, например, Dear Friend, Dear Customer, Уважаемый пользователь, означают, что адресант не знает вашего имени, то есть письмо разослано наудачу по многим адресам.

4

Нежданное письмо

Вы получили письмо, СМС или звонок от банка/платежной системы/почтового провайдера с просьбой сообщить свои персональные данные. Вы не пользуетесь данным банком/платежной системой/почтовым провайдером. Значит, письмо определенно мошенническое.

5

E-mail: пройди по ссылке и залогинься

Вы получили сообщение от банка/платежной системы/почтового провайдера. У вас есть учетная запись в данной системе. Внимательно

прочитайте текст сообщения: если вас под каким-нибудь предлогом просят ввести логин/пароль, пройдя по ссылке, то письмо мошенническое, — банки, платежные и почтовые системы никогда не просят пользователей залогиниться, пройдя по ссылке в письме. В этих системах логин и пароль требуется вводить только для доступа в свой персональный кабинет.

6

Не совпадает домен второго уровня

Еще один простой способ отличить фишинговое письмо от настоящего — подвести курсор к ссылке. Тогда во всплывающей подсказке, либо в нижнем левом углу почтового клиента, вы увидите настоящий адрес сайта, на который попадете, если пройдете по ссылке. Внимательно посмотрите на него: домен второго уровня (то, что стоит непосредственно перед первым слешем) должен принадлежать организации, от которой идет рассылка.

Так, в письме от платежной системы PayPal ссылка вида

- http://anything.paypal.com/anything

будет верной, в то время как ссылки

- http://paypal.confirmation.com/anything,
- http://anything.pay-pal.com/anything,
- http://anything.paypal.com.anything.com/anything

и любые другие ссылки, не содержащие непосредственно перед первым слешем домена paypal.com, будут мошенническими.

7

Обновите ваш профиль в Fakebook

Смотрите внимательно, на какой сайт вы переходите, зачастую мошенники делают названия своих доменов похожими на названия легальных сайтов, заменяя или переставляя местами лишь одну букву.

8

Внезапная удача

Щедрое рекламное предложение, внезапная акция, выигрыш в лотерею, для участия или получения денежного приза в которой требуется ввести данные своей карты или другую персональную информацию также должны вызывать подозрения. Если организатором акции обозначена известная организация — следует связаться с ней напрямую и уточнить условия конкурса. Если нет — не стоит рисковать своими деньгами ради сомнительной выгоды.