Что такое фишинговая атака?

Фишинг – это особый вид компьютерного мошенничества. Фишинг-атаки организуются следующим образом: киберпреступники создают подложный сайт, который выглядит в точности так же, как сайт банка или сайт, производящий финансовые расчеты через интернет. Затем мошенники пытаются обманным путем добиться, чтобы пользователь посетил фальшивый сайт и ввел на нем свои конфиденциальные данные – например, регистрационное имя, пароль или PIN-код. Используя их, злоумышленники крадут деньги со счетов попавшихся на удочку пользователей.

Обычно для привлечения пользователей на подложный сайт используется массовая рассылка электронных сообщений, которые выглядят так, как будто они отправлены банком или иным реально существующим финансовым учреждением, но при этом содержат ссылку на подложный сайт. Пройдя по ссылке, вы попадаете на поддельный сайт, где вам предлагается ввести ваши учетные данные. Часто в фишинг-сообщениях используются те же логотипы и оформление, что и в письмах настоящего банка, а также ссылки, похожие на реальный адрес банка в интернете. Кроме того, сообщение может содержать ваше имя, как будто оно действительно адресовано вам лично. В письмах мошенников обычно приводится правдоподобная причина, требующая ввода вами на сайте "банка" своих данных. Например, ваш банк якобы проводит выборочную проверку безопасности учетных записей или изменил свою компьютерную инфраструктуру, в связи с чем всем клиентам необходимо заново ввести свои личные данные.

Как защититься от фишинговых атак?

Соблюдение перечисленных ниже правил (а также советов по защите компьютера от вредоносных программ и хакерских атак, изложенных на других страницах этого раздела) позволит вам успешно противостоять фишинговым атакам.

Относитесь с опаской к сообщениям, в которых вас просят указать ваши личные данные. Вероят

Не заполняйте полученные по электронной почте анкеты, предполагающие ввод личных данных.

Связывайтесь с банком по телефону всякий раз, когда ситуация покажется вам подозрительной

Не проходите по ссылкам в электронных письмах в формате HTML: киберпреступники могут спр

Убедитесь, что ваше антивирусное решение способно блокировать переход на фишинговые сайт

Регулярно проверяйте состояние своих банковских счетов (в том числе счетов, к которым привяз

Следите за тем, чтобы у вас всегда была установлена последняя версия интернет-обозревателя