Как действуют мошенники?

Главная задача фишинга – завладеть вашим логином и паролем от определенного сайта, в данном случае – от кабинета в интернет-банкинге. Они также не против узнать ПИН от вашей карточки и другую полезную информацию.

Как уберечься?

Совет 1. *Никому не сообщайте свой пароль*. Банк никогда не будет требовать от вас внезапного ввода пароля и – тем более! – его пересылки в электронном письме.

Совет 2. *Внимательно проверяйте, что написано в адресной строке сайта*, на котором вы вводите свои логин и пароль. Обычно сайт-подделка имеет почти неотличимый от оригинального адрес – различаются только одна-две буквы. Также проверяйте, с какого ящика вам пришло письмо – вряд ли банк будет пользоваться бесплатными почтовыми ящиками на сервисе Mail.ru.

Совет 3. *С осторожностью относитесь к электронным письмам и смс*, в которых запрашивают конфиденциальную информацию. Банки так не действуют!

Совет 4. *Остерегайтесь неопределенных формулировок в тексте полученных сообщений*. В письмах от настоящих банков к вам почти всегда обратятся по имени: «Иван Васильевич», в сообщениях от мошенников в лучшем случае будет написано «Уважаемый клиент!» (просто потому, что они не знают ваше имя).

Совет 5. *Не поддавайтесь панике, если вам угрожают закрытием счета* или списанием большой суммы денег. Просто позвоните в свой банк и уточните, действительно ли у него есть такие намерения.

Совет 6. *Установите на компьютер программу, автоматически распознающую фишинговые схемы*. Например, Norton Internet Security.

Совет 7. *Обращайте внимание на текст писем, пришедших на почту*. Поверьте, банковские сотрудники, занимающиеся рассылкой, – грамотные и внимательные. Они не будут писать «в течениИ» или делать опечатки.

Совет 8. *Не звоните по телефонам, которые «банк» присылает вам в смс*. Если это, конечно, не бесплатный номер, начинающийся с «8(800)…» Впрочем, даже такой номер может оказаться потенциально опасным.