# Полиция Зеленограда предупреждает жителей об одном из способов мошенничества – фишинге

17.01.2020

УВД Зеленограда ранее рассказывало жителям округа о различных способах дистанционного мошенничества. Чаще всего оно происходит с помощью телефонного звонка, во время которого злоумышленник представляется сотрудником банка и убеждает жертву перечислить денежные средства на счет злодея. Однако встречаются и преступления, в результате которых жертва теряет свои деньги, не разговаривая с мошенником по телефону.

Один из способов – так называемый фишинг. Это мошенничество по получению конфиденциальных данных, которое не связано с банковскими картами напрямую. Жертва получает электронное письмо якобы от имени банка или другой организации, переходит, ничего не подозревая, по ссылке, которая есть в письме. Для входа в аккаунт вводит свой логин и пароль, который и получают злоумышленники. Такие сайты специально создаются мошенниками для сбора конфиденциальной информации. Для создания сообщений используется логотип, стиль организации, от которой якобы отправлено письмо, оно может быть именным. Спустя некоторое время, вы заметите, что по карте происходят списания денежных средств, хотя сама карта не была утеряна и подозрительных звонков вам не поступало.

Так, в полицию обратилась 40-летняя жительница Зеленограда с заявлением о том, что неизвестное лицо осуществило покупки на одном из интернет-сайтов, используя данные банковской карты заявительницы, на общую сумму более 3500 рублей. Со слов женщины, банковскую карту она не теряла, данные никому не передавала и покупок на указанном сайте ранее не совершала. В настоящий момент полиция проводит проверку по поступившему заявлению.

Чтобы не стать жертвой мошенников необходимо помнить и соблюдать несложные правила:

· никогда не переходить по подозрительным ссылкам, полученным по электронной почте и в смс-сообщении. Они могут вести на «зеркальные» сайты-однодневки, созданные мошенниками! Основной признак «зеркального» сайта банка – появление надписи о техническом обслуживании сайта после ввода логина и пароля на странице или любая информация, в которой будет указано о том, что обратиться на сайт можно позднее. При этом на телефон не поступает смс-сообщение от банка о входе в личный кабинет, если такая форма оповещения предусмотрена. Прежде чем переходить по ссылке, позвоните в банк и выясните, направляли ли они что-либо в ваш адрес;

· подключить услугу смс-информирования – это обеспечит контроль за проведением любых операций по карте. При получении смс-сообщения о несанкционированном списании средств со счета, можно успеть заблокировать карту и сохранить часть суммы на счете;

· установить лимит выдачи денежных средств в сутки и за одну операцию (это можно сделать в отделении банка или удаленно в Интернет-банке). Мошенники не смогут воспользоваться сразу всей суммой, которая находится на карте.

Если вы стали жертвой мошенников, незамедлительно обращайтесь в полицию!

---



---