**«Стоп, мошенник! Полиция предупреждает граждан: подставные (фишинговые) сайты – нажива для мошенников»**

Фишинг - кража любых персональных данных, владение которыми позволяет преступникам получать выгоду. Это серии и номера паспортов, реквизиты банковских карт и счетов, пароли для входа в электронную почту, платежную систему и аккаунты в социальных сетях. Персональную информацию мошенники используют для получения доступа к аккаунтам, к которым привязаны банковские карты, что позволяет похищать с их счетов денежные средства.

Для кражи персональных данных злоумышленники массово рассылают электронные письма от имени известных компаний, крупных банков или онлайн-магазинов. Их цель - заставить получателей перейти по указанной в письме ссылке на поддельный сайт компании, интерфейс которого внешне не отличим от настоящего сайта, и ввести свои личные данные. Для привлечения внимания к письму в теме указывается на перспективу большой выгоды или на проблему, требующую срочного разрешения.

Подставные страницы действуют недолго - как правило, не более одной недели, ввиду частого обновления базы антифишинговых программ и фильтров. Однако мошенники, следуя отлаженной схеме, создают все новые и новые сайты-фальшивки для сбора персональных данных.

*Жительница Мясниковского района обратилась в полицию с сообщением о мошенничестве. Гражданка пояснила, что она выиграла крупную сумму в лотерее и для получения ей было необходимо пройти по ссылке, ведущей на сайт одного из банков. Когда женщина нажала указанный адрес в письме, перед ней открылся сайт, внешне схожий с настоящим, поэтому не вызвал никаких подозрений. После она ввела данные своей банковской карты якобы для начисления ей выигрыша. Однако после совершенных действий ей пришли уведомления о списании всех денег с карты – более 30 тысяч рублей. Когда женщина поняла, что ее обманули, обратилась в полицию.*

Следует помнить, что банки и платежные системы никогда не присылают писем и не звонят на телефоны граждан с просьбой предоставить свои данные. Не переходите по сомнительным интернет-ссылкам, если такая ситуация произойдет, вас попросят приехать в банк лично.

Пресс-служба ГУ МВД России по Ростовской области