ФИШИНГ
как способ хищения денежных средств с банковских счетов с использованием логотипа сайта «kufar»

За три месяца 2022 года в отношении жителей г. Горки и Горецкого района совершено 5 фактов хищения денежных средств с банковских счетов с использованием способа, получившего название «фишинг». При совершении вышеуказанных хищений, приманкой для обмана граждан послужили объявления, размещенные на сайте «kufar.by».

Фишинг- это один из видов интернет-мошенничества, основной целью которого является получение доступа к конфиденциальным данным пользователей: логинам и паролям, реквизитам банковских платежных карт, с использованием которых возможно осуществить регистрацию в системе дистанционного банковского обслуживания (Интернет-банкинг), идентификационного номера паспорта, а так же сессионных кодов, поступающих на мобильный телефон в виде смс-сообщений. В этом случае «фишер» в ходе переписки со своей будущей жертвой предоставляет ссылку на «фишинговый» сайт и убеждает ее перейти по ней на сайт, на котором необходимо ввести реквизиты банковской карты для получения денежных средств за продаваемый товар, к примеру. После ввода на данном сайте реквизитов банковской карты (номер, срок действия, CVC/CVV код) «фишер» осуществляет регистрацию в системе Интернет-банкинг, после чего на мобильный телефон жертвы поступают сообщения от банковского учреждения, содержащие сессионные коды, необходимые для подтверждения регистрации в системе Интернет-банкинга. «Фишер» заверяет жертву о необходимости ввода поступивших сессионных кодов на «фишинговом» сайте, после чего у него имеется неограниченный доступ к банковскому счету жертвы, который позволяет ему похитить все денежные средства с банковского счета, путем перевода на подконтрольный ему банковский счет, в том числе иностранного государства.

Рассмотрим на конкретном примере, который произошел в марте 2022 года. Гражданка А. разместила объявление о продаже велосипеда на сайте «kufar.by». Спустя 40 минут с ней связался «фишер» в мессенджере «Viber». В ходе состоявшейся переписки «фишер» заверил гражданку А. о том, что оплатил покупку ее велосипеда с использованием сервиса «куфар-доставка» на сайте «kufar.by» для того, что бы избежать обмана с ее стороны. Далее в одном из сообщений «фишер» предоставил ссылку на «фишинговый» сайт, при этом убедил гражданку А., что ей необходимо перейти по данной ссылке и на открывшемся сайте ввести необходимые реквизиты ее банковской карты, а так же сессионные коды, которые поступили ей в дальнейшем на мобильный телефон в виде смс-сообщений. Гражданка А. ввела все необходимые реквизиты банковской карты, сессионные коды, после чего с ее банковского счета произошло списание денежных средств в сумме 440 рублей путем перевода их на банковский счет преступника.

Для того, что бы не стать жертвой киберпреступника, необходимо руководствоваться следующими простыми правилами:

1. При продаже какого-либо имущества на различных интернет-сайтах, не вести с покупателем переписку в мессенджерах (Viber, WhatsApp), а так же социальных сетях (Одноклассники, Вконтакте, instagram).
2. Не переходить по ссылкам, которые предоставит Вам покупатель в ходе переписки, а так же не вводить реквизиты банковских карт на неизвестных сайтах в сети Интернет.
3. По вопросу отправки товара настаивать на его доставке по почте либо европочте «наложенным платежом» (оплата товара происходит при получении).
4. Если покупатель отказывается от доставки товара «наложенным платежом»- прекратить с ним переписку, потому что в данном случае Вы ее ведете с «фишером», основной целью которого является не приобретение продаваемого Вами товара, а **хищение денежных средств с Вашего банковского счета.**

Помните! Ваша безопасность- в Ваших руках!

С уважением,
Старший оперуполномоченный группы
по противодействию киберпреступности
криминальной милиции Горецкого РОВД Александр Васильев