

Как не стать жертвой киберпреступника

За 5 месяцев 2022 года в отношении жителей г. Горки и Горецкого района совершено 15 фактов хищения денежных средств с банковских счетов с использованием сети Интернет. На данный момент основными способами совершения хищений денежных средств с банковских счетов являются «фишинг» и «вишинг».

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.

Вишинг- это один из методов интернет-мошенничества, связанный с использованием социальной инженерии, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определенную роль (сотрудника банка, к примеру), под различными предложениями выманивают у держателя платежной карты конфиденциальную информацию или стимулируют к совершению определённых действий со своим банковским счетом/платежной картой.

Для того, что бы сохранить свои денежные средства, 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.**
5. При поступлении звонков от неизвестных лиц, в том числе в мессенджерах (Viber, WhatsApp), незамедлительно прекратить данный разговор.

Помните! Ваша безопасность- в Ваших руках!

С уважением,
Временно исполняющий обязанности
начальника Горецкого РОВД

Сергей Вячеславович Питяков