Как не стать жертвой киберпреступников: о примерах хищений денежных средств

В Витебской области участились случаи хищений денежных средств с использованием платежных банковских карт и социальных сетей.

За 4 месяца этого года в Витебской области следователями возбуждено 720 уголовных дел (в 2020 году - 2 820) по ст. 212 (хищение путем использования компьютерной техники) Уголовного кодекса Республики Беларусь.

Одним из способов завладения реквизитами платежных банковских карт является **фишинг** (англ, phishing, от fishing - рыбная ловля, выуживание). Неизвестные лица рассылают людям электронные сообщения, в которых содержится ссылка на сайт, внешне неотличимый от настоящего. Когда пользователь попадает на поддельную страницу, мошенники побуждают его ввести на ней свои логин и пароль доступа к определенному сайту, что позволяет им получить доступ к аккаунтам и банковским счетам.

Вишинг (англ, vishing - voice+phishing). - одна из разновидностей фишинга, при котором также используются методы социальной инженерии, но уже с помощью телефонного звонка.

Как обычно действуют злоумышленники «вишеры»?

На телефон поступает звонок от сотрудника банка и оператор предупреждает, если прямо сейчас не будет представлена полная информация банковской карты ему по телефону, то карту заблокируют, или вымышленные злоумышленники похитят весь остаток денежных средств, находящийся на карте. Доверчивый пользователь, слыша подобную «угрозу» сразу же впадает в панику и может выдать все персональные данные вплоть до проверочного кода из SMS.

Также при вишинге может быть предложена выгодная покупка с огромной скидкой или озвучена информация о выигрыше в какой-либо акции. Не нужно сразу же радоваться столь удачной покупке или выгодной акции, всегда стоит лишний раз перепроверить информацию, обратившись к официальным источникам.

В любой непонятной ситуации главное не паниковать. Помните - всегда всё можно проверить. Вежливо попрощайтесь с собеседником и позвоните на горячую линию организации, представителем которой назвался звонивший. Так вы легко сможете понять был ли звонок обоснованным, или вы чуть не стали жертвой вишинга.

К примеру, днем 4 февраля этого года в мессенджере Viber 67-летней жительнице Новополоцка позвонили неизвестные и представились сотрудниками банка. Последние сказали, что с ее банковских карт пытаются снять денежные средства и предложили обезопасить их. Беседа с мошенниками длилась практически час - в итоге, после того, как потерпевшая предоставила необходимые данные к личному кабинету интернет-Банкинга, с ее карт, в том числе валютного депозитного счета были похищены все денежные средства, находящиеся на них - более 62 тысяч рублей. Возбуждено уголовное дело по ч. 4 ст. 212 Уголовного кодекса Республики Беларусь.

Схожий случай произошел в период времени с 12 по 14 апреля этого года. Неизвестное лицо связалось с витебчанином в мессенджере Viber. В ходе

разговоров мужчину уговорили взять на себя кредит, якобы для выявления сотрудника банка, занимающегося противоправными действиями, после чего, завладев реквизитами банковской кредитной карты, с расчетного счета потерпевшего было похищено более 4300 рублей. Возбуждено уголовное дело по ч. 2 ст. 212 Уголовного кодекса Республики Беларусь.

Ещё один случай имел место в марте этого года. Жительнице Витебска написали в социальной сети Instagram и под предлогом приза, разыгрывающегося на одном из сайтов, завладели реквизитами принадлежащей ей платежной банковской карты. В результате с карт-счета были похищены денежные средства. Возбуждено уголовное дело по ч. 2 ст. 212 Уголовного кодекса Республики Беларусь.

Также, 12 апреля этого года мужчина разместил на торговой площадке Куфар объявление о продаже товара. В мессенджере «Telegram» ему написал «покупатель» и, под предлогом приобретения товара, якобы для оформления его доставки, отослал ему ссылку на фишинговый сайт. Потерпевший перешел по ссылке и ввел данные своей платежной банковской карты в поле для реквизитов. В результате у мужчины с карт-счета похитили все денежные средства, то есть более 290 рублей. По данному факту возбуждено уголовное дело по ч. 2 ст. 212 Уголовного кодекса Республики Беларусь.

Мошенники продолжают придумывать различные способы хищений денежных средств, а граждане во многих случаях проявляют излишнюю доверчивость и невнимательность.

Чтобы не стать жертвой подобных преступлений, следователи рекомендуют соблюдать следующие правила:

Вам позвонили/прислали SMS из «банка» с неизвестного номера:

- не торопитесь следовать инструкциям;
- не сообщайте персональные данные неизвестным лицам, даже если они представляются сотрудниками банка;
- проверьте информацию, позвонив в контактный центр банка;
- незамедлительно обратитесь в правоохранительные органы.

Вам позвонили/прислали SMS с неизвестного номера с просьбой о помощи близкому человеку:

- не впадайте в панику. Не торопитесь предпринимать действия по-инструкциям неизвестных людей;
- задайте звонящему вопросы личного характера, помогающие отличить близкого вам человека от мошенника;
- под любым предлогом постарайтесь прервать контакт с собеседником, позвоните родным и узнайте, все ли у них в порядке.

Вы заподозрили интернет-продавца в недобросовестности:

- необходимо оставаться бдительным, не принимать поспешных решений и при первых же подозрениях отказаться от покупки;
- никогда не переводите деньги незнакомым людям в качестве предоплаты.

Как не стать жертвой фишинга:

- внимательно проверьте ссылку, по которой собирайтесь кликнуть: не перепутаны ли буквы в названии сайта;

- зачастую фальшивые письма и фальшивые сайты во всем повторяют дизайн настоящих;

- вместо того, чтобы кликать по ссылке, следует ввести адрес вручную в новом окне браузера;

- перед тем как вводить логин и пароль, нужно проверить защищено ли соединение. Перед адресом сайта вы увидите префикс https (где s означает secure) - безопасное соединение;

- не заходите в онлайн-банки и тому подобные сервисы через открытые Wi-Fi-сети в кафе или на улице. Лучше воспользоваться мобильным интернетом или потерпеть, чем потерять все деньги на карте;

- даже если письмо или сообщение со ссылкой пришло от лучшего друга, все равно нужно помнить, что его тоже могли обмануть или взломать. Поэтому ведите себя не менее осторожно, чем при обращении со ссылками, пришедшими из неизвестного источника.

Следователи призывают граждан к проявлению бдительности и осмотрительности! Поделитесь данной информацией со своими друзьями, родными и близкими.

Следственное управление УСК по Витебской области