В связи с участившимися случаями мошенничеств с платежными картами, а в особенности с картами Приватбанка, просим вас внимательно прочитать следующее предупреждение:

Канал 1+1 показывал сюжет о воровстве у людей, собирающих средства на лечение.
Рассказывали про женщину, которая собрала на лечение ребенка 150 тыс. грн., а потом мошенники каким-то образом сняли с её карты 70 тыс из этих средств.
Оказалось, что зная номер жертвы и номер её карты, украсть деньги с карты можно не прибегая к троянам, вирусам и не выманивая у жертвы секретный код C V V.

Один из методов хищения средств с карты Приватбанка таков:

Этап один - узнаём номер мобильного телефона жертвы. Собирающие пожертвования обычно не задумываются и дают свой основной номер рядом с реквизитами для пожертвований, которые включают и номер платежной карты Приватбанка. Как правило, у человека один номер мобильного телефона и к этому номеру банк привязывает удаленное управление картой через интернет-банкинг или СМС.
Этап два - на телефон жертвы делаются звонки с разных номеров, некоторые сбрасываются и жертва сама на них перезванивает. Так мошенники получают список 5 последних входящих и исходящих звонков. Затем мошенники предлагают пополнить средства на номере жертвы (таким образом внести пожертвования). Жертва обычно с радостью соглашается (а можно и без её согласия пополнить, неважно).
Этап три - мошенник звонит мобильному оператору, представляясь владельцем номера телефона жертвы, называет номер телефона жертвы и просит заблокировать номер с связи с утерей телефона. Оператор спрашивает информацию для идентификации: последние входящие и исходящие звонки и сумму последнего пополнения. Мошенник называет их и номер блокируется. После этого мошенник идет в офис оператора и восстанавливает якобы утерянную сим-карту с номером жертвы, сообщив туже идентификационную информацию. Таким образом он получает на руки сим-карту с номером мобильного телефона жертвы и вуаля! Номер, привязанный к карте Приватбанка уже у мошенника. Все СМС от банка приходят к нему, а жертва остаётся без своего номера, к которому скорее всего привязан интернет-банкинг «Приват 24».
Этап четыре - в «Приват 24» мошенник жмет «забыл пароль», система запрашивает номер телефона и последние 4 цифры номера карты, которая к нему привязана и бинго, контроль над всеми карточными счетами жертвы в «Приват 24» получен.

Вывод: Для обеспечения сохранности средств на карточном счету специалисты настоятельно рекомендуют не указывать одновременно номер карты и мобильный телефон, к которому он привязан.
Либо этот мобильный телефон должен обслуживаться по контрактному тарифному плану (а не по предоплате). Для восстановления сим-карты контрактного тарифного плана, который по сути является именным, нужно предъявить паспорт владельца, что делает ее захват сторонними лицами невозможным. Все операторы предоставляют как тарифные планы по предоплате, так и корпоративные тарифные планы, которые, как правило, немного дороже.

Примеры других преступных схем:

1) Звонят, что хотят перевести деньги и просят номер карты Приватбанка. Далее приходит смс с непонятным содержанием с того же номера что и звонили. Опять звонят - перевели деньги. Вы говорите, что с Приватбанка не было смс. Вам мошенник отвечает, что Вам же пришла смс-ка с моего номера. Надо ее переслать на Приватовский номер 10060. Тогда они вам пополнят счет с моей карты.
ЭТО ОБМАН. С ВАШЕЙ КАРТЫ СНИМУТ ДЕНЬГИ КОТОРЫЕ ЯКОБЫ ХОТЯТ ПЕРЕВЕСТИ ВАМ.

2) Мошенник пытается произвести впечатление обеспеченного человека, вворачивает фразы о дорогой машине, об офисе и т.д. Говорит, что не понаслышке знает о болезни и поэтому хочет помочь. Очевидно это должно внушить доверие. Затем просит номер карточки и ФИО. Затем номер мобильного телефона, к которой привязана карточка.
ВНИМАНИЕ! Для того, чтобы перевести Вам деньги от юр.лица или от физ.лица, или для любого другого перевода НОМЕР ТЕЛЕФОНА НЕ НУЖЕН. ЭТО ОБМАН С ЦЕЛЬЮ ДОСТУПА К КАРТЕ.

3) Звонят, берут у жертвы номер карты Приватбанка и говорят что сейчас перечислят денежки. Потом звонок якобы от сотрудника "Приватбанка" со скрытого номера (Приватбанк никогда не звонит со скрытого номера). Он спрашивает, ждёте ли вы денег в размере такой-то суммы, а потом начинают раскручивать и пытаться выяснить информацию (скорее всего CVV код, пин-код, срок действия карты и т. д.)
ЭТО ОБМАН. ВНИМАНИЕ! CVV код - это 3 цифры с обратной стороны карты над магнитной лентой, там может быть и больше, но код cvv это три последние. Его никому нельзя передавать, так же как и пин код, а также нельзя никому сообщать дату окончания действия карты. Никогда и никому не сообщайте дату до которой действительна карта. Для перевода денег такая информация не нужна. Будьте бдительны!

4) Мошенник звонит со скрытого номера, говорит что деньги с его счета на ваш ушли, но зависли. Начинает давить на жалость. Просит ввести комбинацию на вашем телефоне, типа
21[номер какого-то телефона]#
ВНИМАНИЕ! Никогда не вводите эту или подобные команды на своем телефоне. В данном случае это был USSD-запрос переадресации всех входящих смс и звонков на его номер. Также мошенник может просить вас отправить смс типа SEND2560UAH+1111+4444222233335555. В этом случае с вашей карты будет сделан перевод в сумме 2560 грн на карту 4444222233335555. Изучите команды SMS-банкинга вашего банка (Приватбанка или другого).

5) Мошенник звонит и говорит, что готов перечислить деньги, пытается произвести хорошее впечатление, на фоне разговора даже можно слышать якобы детские разговоры, либо смех и т.д. (это аудио запись для фона), только дайте реквизиты для оплаты: номер карты, ФИО, номер телефона. Вы даёте. Дальше он говорит: "Я вам сейчас пришлю смс-кой код, вы его перешлите на такой-то номер Приватбанка. Приходит смс. В ней последние четыре цифры номера Вашей карты и сумма, которую он якобы собирался перечислять. Если вы пересылаете эту смс на специальный номер «Приватбанка», то этим вы подтверждаете банку операцию "экстренные деньги", то есть снятие наличных в любом банкомате банка без карты. Через минуту звонит тот же мошенник и говорит: «Мы начинаем переводить вам деньги. Сейчас вам придет смс с кодом из банка. Вы его мне продиктуйте, чтобы мы могли завершить операцию». Вам приходит смс: «Секретный код экстренных денег такой-то.» Оказывается, для того чтобы снять деньги в банкомате без карты, нужно ввести номер телефона владельца карты и этот самый секретный код, который вы по незнанию даёте.

Методы мошенников могут быть разными и все время меняются. Как себя обезопасить?

Чтобы не стать жертвами подобных мошенников, не рекомендуется в случае сбора благотворительных средств пользоваться обычными банковскими картами. Для этого в Приватбанке помогут открыть специальную карту для сбора средств с особым режимом безопасности. Обслуживание такой карты абсолютно бесплатно, а банк, имея большой опыт благотворительности, поможет собрать средства.

Кроме того, в Приватбанке напоминают всем клиентам, что никогда нельзя сообщать посторонним секретные данные своих карт или счетов. “Если к Вам обратились с просьбой продиктовать ПИН-код или C V V — код (с обратной стороны карты), сразу обратитесь в банк. Это сигнал, что Вы могли стать целью мошенников.

Любая информация в виде объявления в газете или в Интернете с публикацией номера карты и номера телефона может стать частью преступных планов. Если у вас случайно перестал работать мобильный - тоже сообщите в банк и временно заблокируйте карты, которые к нему привязаны.

Пресс-Служба Приватбанка