ВООРУЖЕН ЗНАНИЯМИ – ЗНАЧИТ ЗАЩИЩЕН

ПАО «МАРФИН БАНК» очень серьезно относится к защите своих клиентов. Мы проводим большую работу, рассказывая и разъясняя клиентам о различных видах современного мошенничества. К сожалению, сегодня мошенники для совершения своих незаконных операций часто используют технические новинки. Иногда и банкоматы, в которых Вы, уважаемый Клиент, снимаете деньги, становятся объектами нападения вандалов и грабителей, а также средством, с помощью которого мошенники крадут деньги с карточных счетов.

Существует множество различных способов неправомерного завладения деньгами с карточного счета другого человека с помощью банкоматов:

- **использование украденной карты и ПИН-кода**, разглашенного держателем, в том числе и, так называемое, «дружеское мошенничество» - использование карты путем свободного доступа членами семьи, близкими, друзьями, коллегами по работе. Это также предполагает разглашение ПИН-кода;

- **подглядывание ПИН-кода** из-за плеча с последующей кражей карты – простейший, но широко распространенный способ;

- **«ливанская петля»** - еще один способ мошенничества, когда блокируется окно подачи карты так, чтобы карта застряла. Мошенник, предварительно подсмотревший ПИН-код, сочувствует и рекомендует срочно идти и звонить в банк или сервисную службу. Как только владелец отходит, преступник извлекает карту, освобождает картоприемник и снимает деньги с этой карты;

- **установка фальшивых банкоматов** - достаточно редкий способ, требующий технической оснащенности. Выглядят такие банкоматы как настоящие, размещают их в людных местах. Банкомат принимает карту, требует ввода ПИН-кода, после чего выдает сообщение о невозможности выдачи денег (под предлогом отсутствия денег в банкомате или технической ошибки) и возвращает карту. В банкомате происходит копирование данных с карты и ПИН-кода, что позволяет мошенникам впоследствии изготовить дубликат карты и снять с ее помощью деньги со счета клиента;

- **изготовление новой поддельной (клонированной) карты** путем считывания информации с карты клиента (скимминга) с помощью подставных устройств и последующего похищения средств с их счетов. Мошенники всё активнее используют скиммеры, устройства которые считывают или сохраняют в памяти (варианты: отправляет СМС или радиосигналом) информацию с магнитной ленты платежной карты. Такие устройства устанавливаются на банкомат (считыватель – на окно подачи карты (картридер), дополнительной клавиатурой накрывают настоящую или устанавливают скрытую видеокамеру для фиксирования вводимого ПИН-кода). Полученные мошенническим путем данные наносятся на «белый» пластик и через любой банкомат «обнуляется» чужой счет.

Банкоматы новейшей модификации уже конструктивно защищены от постороннего воздействия. Но иногда для защиты хватает совсем несложных профилактических действий самого клиента.

Пользуясь банкоматом, убедитесь, что он выглядит нормально, нет посторонних устройств на его картридере, накладок на клавиатуре, нет следов взлома, индикаторы мигают. Если Вы привыкли снимать деньги в одном и том же банкомате, запомните его внешний вид. При изменении внешнего вида картридера (приемника для карточки) лучше ее даже не вставлять.

Вот так выглядит картридер обычного банкомата (фото. 1).

Фото 1

А вот так картридер с установленным на нем считывающим устройством – скиммером (фото. 2, 3 ,4, 5). Скиммер (и др. приспособления мошенников) обычно изготовлен под дизайн конкретного банкомата, что бы владелец карты ничего не заподозрил.

Фото 2

Фото 3

Фото 4

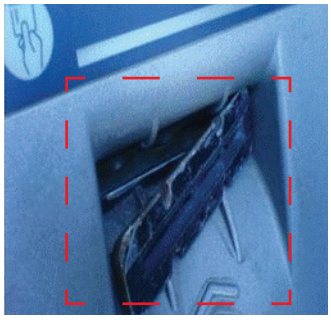

Фото 5

Обратите внимание, картридер на банкомате выполнен цельнолитым с корпусом (фото 1). У скиммера же, между корпусом банкомата и установленной накладкой, всегда есть зазоры, да и по цвету он отличается, пусть незначительно, но отличается (фото 2, 3, 4). Картридер на фото 4 и 5 выполнен грубо и не аккуратно. Такой картридер должен сразу насторожить Ваше внимание.

Другим дополнительным устройством, позволяющим мошенникам воспользоваться вашим счетом, является накладка на клавиатуру, с помощью которой они узнают ПИН-код вашей карты или замаскированная миниатюрная видеокамера.

Вот так выглядят некоторые накладки на клавиатуру (металлическая на фото 6, 8 и пластиковая на фото 7).

Фото 6.

Фото 7

Фото 8

Фото 8а

А это панель на всю рабочую поверхность с клавиатурой и скиммер (фото 9):

Существуют целые накладные панели, которые накладываются сразу на всю поверхность банкомата и одновременно считывают и ПИН-код, и номер банковской карты. Вот один из вариантов такой панели (фото 10):

Фото 10

А видеокамера может выглядеть просто как накладная панель (фото 11) или коробочка с рекламой, прикрепленной сбоку от банкомата (фото 12, 13):

Фото 11

Фото 12

Фото 13

БУДЬТЕ ВНИМАТЕЛЬНЫ! При подозрительном виде банкомата лучше немедленно перезвонить в банк и не пользоваться банкоматом. Телефон банка обычно указан на передней панели банкомата. Если у Вас возникли подозрения по поводу разъема для карточек, возьмитесь за него и попробуйте пошатать. Ни один настоящий разъем банкомата никак не отреагирует на такие действия, а вот скиммер может остаться у Вас в руках. Тот же совет касается камеры, скрытой за рекламной вывеской или еще чем-то. Конечно же мы не говорим о камерах, находящихся в самом банкомате и направленных на лицо клиента (видеонаблюдение банка). Камеры мошенников всегда направлены на клавиатуру банкомата.

И еще несколько советов держателям платежных карт:

1. Никогда и никому не сообщайте Ваш ПИН-код. Если его просят предоставить, то Вы имеете дело с мошенником. ПИН-код нужно запомнить или хранить отдельно от банковской карты, в недоступном для других месте.

2. При работе с банкоматом прикрывайте ладонью клавиатуру во время ввода ПИН-кода и обращайте внимание на людей, стоящих у Вас за спиной. Не позволяйте увидеть им вводимые Вами цифры.

3. Подключите услугу СМС-Банкинг для отслеживания состояния Вашего карточного счета. Это позволит Вам всегда получать информацию о проведенных транзакциях по карте, например, о снятии наличных средств в то время, когда Вы не совершали подобной операции. Это поможет Вам незамедлительно сообщить в банк о сомнительных транзакциях и заблокировать карту до выяснения обстоятельств. Подробности об услуге СМС-Банкинг можно узнать на нашем сайте: **http://marfinbank.ua/RU/eBanking/Individuals/Pages/SMS-Banking.aspx** или по круглосуточному телефону информационной службы – **0-800-500-255** (звонки со стационарных телефонов по Украине бесплатно).

4. Если банкомат «захватил» карту или не выдал деньги, нужно немедленно связаться с банком-владельцем АТМ. А также свяжитесь со своим банком – эмитентом карты и заблокируйте карту до ее возврата. Связываться с банками следует, по возможности, не отходя от банкомата.

5. С целью получения персональных данных держателя, а также реквизитов самой платежной карты злоумышленники могут позвонить по номеру телефона клиента и представиться сотрудниками банка. После подтверждения фамилии, имени и отчества клиента мошенники пытаются под тем или иным предлогом узнать паспортные данные, номер самой карты, ПИН-код и код безопасности. Будьте внимательны! Сотрудники банка никогда не совершают такого рода звонков. Кроме того, банк не рассылает электронные письма и СМС-сообщения клиентам-держателям карт банка с просьбой подтвердить номер платежной карты и/или другие персональные идентификаторы.

6. В конце каждого месяца нужно проверять все совершенные транзакции по выписке с Вашего счета. Немедленно сообщайте о подозрительных операциях в банк-эмитент. Вообще телефон горячей линии для клиентов тех банков, картами которых вы пользуетесь, желательно всегда иметь при себе в мобильном телефоне или записной книжке.

7. При получении банковской карты распишитесь на ее оборотной стороне. Это снизит риск использования карты без вашего согласия в случае ее утери или кражи. Карта без подписи ее владельца считается не действительной и может быть изъята кассиром до уточнения данных о владельце карты. В случае утери карты или ее кражи необходимо немедленно сообщить об этом по телефону горячей линии банку-эмитенту и заблокировать карточный счет.

8. Наиболее защищенные от действий мошенников банкоматы по статистике находятся в помещениях банков или в многолюдных местах.

**БУДЬТЕ БДИТЕЛЬНЫ –
ЗАЩИТИТЕ СВОИ СРЕДСТВА!**

Статья подготовлена
Управлением маркетинга и рекламы ПАО «МАРФИН БАНК»
по материалам СМИ