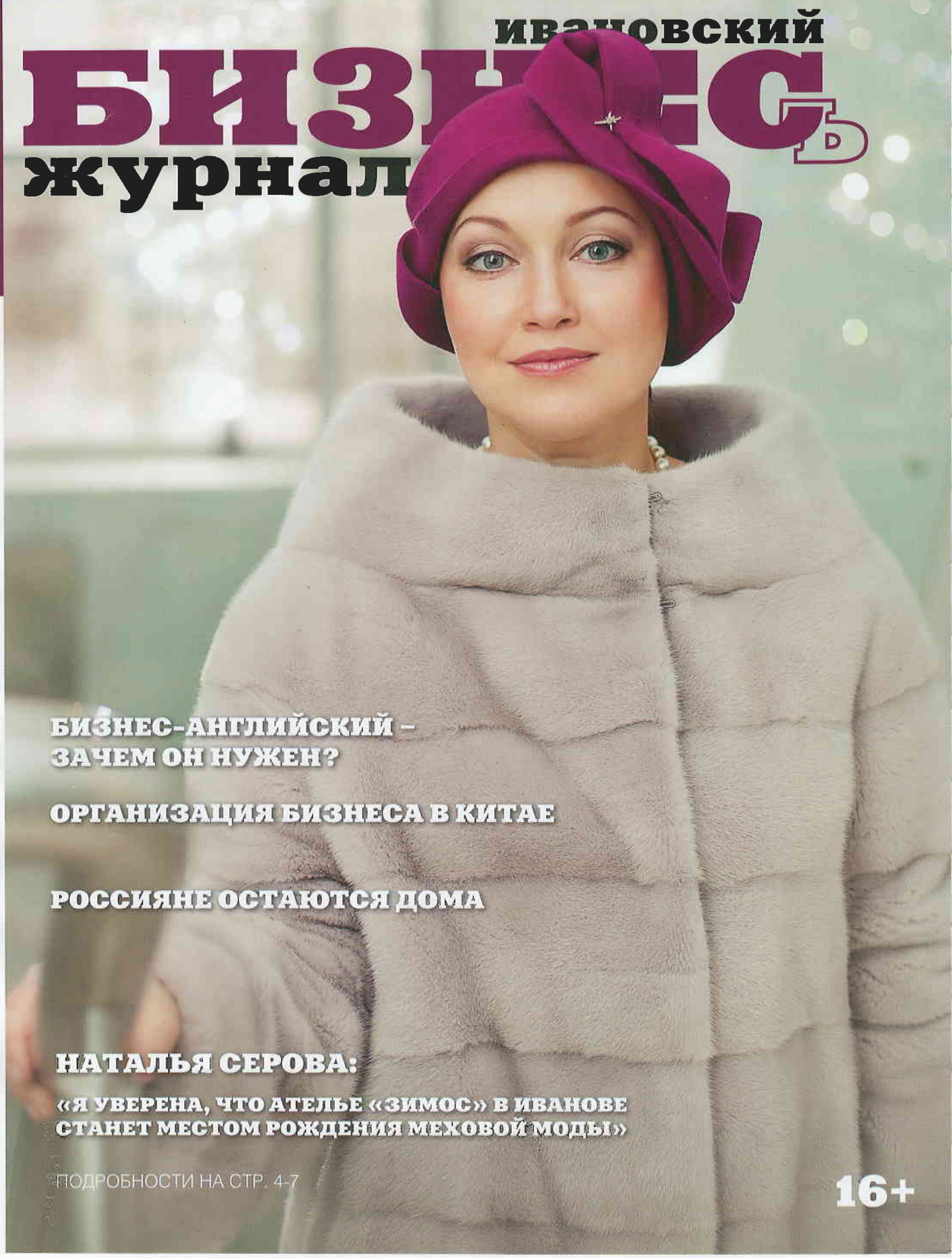
О БЕЗОПАСНОМ ИСПОЛЬЗОВАНИИ БАНКОВСКИХ КАРТ И ОНЛАЙН-БАНКИНГА 8

ИСТОРИЯ ФЕРМЕРА МИХАИЛА ЧИСТОВА – МОСКВИЧА, СОЗНАТЕЛЬНО ПЕРЕЕХАВШЕГО В ДЕРЕВНЮ ИВАНОВСКОЙ ОБЛАСТИ 12

ивановский
БИЗНЕСЪ
журнал

#11
2015



НАТАЛЬЯ СЕРОВА:

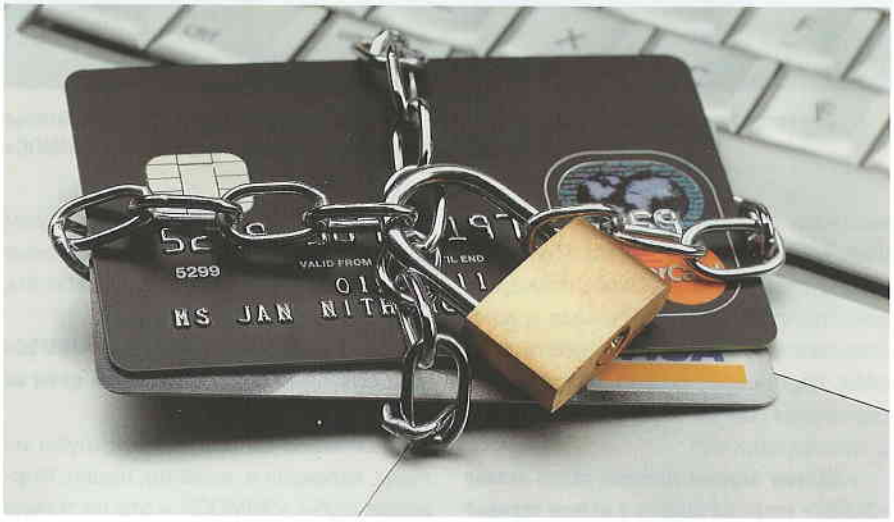
«Я УВЕРЕНА, ЧТО АТЕЛЬЕ «ЗИМОС» В ИВАНОВЕ СТАНЕТ МЕСТОМ РОЖДЕНИЯ МЕХОВОЙ МОДЫ»

ПОДРОБНОСТИ НА СТР. 4-7

16+

О БЕЗОПАСНОМ ИСПОЛЬЗОВАНИИ БАНКОВСКИХ КАРТ И ОНЛАЙН-БАНКИНГА

ДИСТАНЦИОННОЕ БАНКОВСКОЕ ОБСЛУЖИВАНИЕ И ПРИМЕНЕНИЕ БАНКОВСКИХ КАРТ СТАНОВИТСЯ УДОБНЫМ И ПРИВЫЧНЫМ ДЛЯ ШИРОКОГО КРУГА ГРАЖДАН. ВМЕСТО НАБИТОГО КУПЮРАМИ КОШЕЛЬКА МОЖНО БРАТЬ С СОБОЙ БАНКОВСКУЮ КАРТУ. ОПЛАТИТЬ ТУРИСТИЧЕСКУЮ ПУТЕВКУ ИЛИ КОММУНАЛЬНЫЕ СЧЕТА МОЖНО БЕЗ ВИЗИТА В БАНК, СКАЖЕМ, С ПОМОЩЬЮ ТЕЛЕФОНА И ОН-ЛАЙН БАНКА. ОДНАКО СЛЕДУЕТ ПОМНИТЬ, ЧТО АФЕРИСТЫ ТОЖЕ НЕ ДРЕМЛЮТ, ИЗОБРЕТАЯ НОВЫЕ СПОСОБЫ КИБЕРОХОТЫ ЗА ДЕНЬГАМИ НЕОСТОРОЖНЫХ ГРАЖДАН. СОБЛЮДЕНИЕ НЕСКОЛЬКИХ НЕСЛОЖНЫХ ПРАВИЛ ПОЗВОЛИТ БЕЗОПАСНО ИСПОЛЬЗОВАТЬ ПЛАСТИКОВЫЕ КАРТЫ И РАЗЛИЧНЫЕ ДИСТАНЦИОННЫЕ СЕРВИСЫ.



Защита персональных данных держателей карт

Самое главное правило – никогда не допускать, чтобы данные вашей карты попадали к третьим лицам, тем более незнакомым.

Одним из самых распространенных методов мошенничества является фишинг, когда мошенники получают доступ к конфиденциальным данным вкладчика от него самого. Нужно знать, что банки и операторы платежных систем никогда не присылают писем и не звонят клиентам с просьбой предоставить им данные о счете, PIN-код или иные персональные данные – вся необходимая информация у банка и так имеется.

Злоумышленники используют несколько тактик. Наиболее распространенной является рассылка ложных sms- и e-mail-сообщений в адрес клиентов различных кредитных организаций о блокировке банковской карты клиента и предложения перезвонить по указанным в сообщениях телефонным номерам. В качестве отправителей сообщений, как правило, указываются: «Центробанк России», CentroBank, «Служба безопасности Банка России», то есть наименования, ассоциирующиеся с названием Центрального банка Российской Федерации (Банка России).

У граждан, обращающихся по указанным в сообщениях телефонным номерам, злоумышленники пытаются выяснить номера якобы заблокированных банковских карт, PIN-коды, количество денежных средств, размещенных на карточных счетах, персональные данные владельца карты и другую конфиденциальную информацию.

Центральный банк Российской Федерации никакого отношения к указанным sms-сообщениям и e-mail-рассылкам не имеет. Подобные действия регулятор расценивает как мошенничество, осуществляемое с использованием имени Центрального банка Российской Федерации.

При получении подобного рода sms-сообщений и e-mail-рассылок гражданину необходимо незамедлительно обращаться в подразделения кредитной организации, выдавшей ему банковскую карту, чтобы удостовериться в полученной информации. Делать это следует по тому телефону, который написан на оборотной стороне карты. Обращаясь же по телефону, указанному в сообщении, существует большая вероятность столкнуться с мошенниками.

Необходимо как можно чаще проверять выписки со своего счета, для чего из соображений безопасности желательно подключить услугу sms-информирования о совершенных операциях.

К мошенничествам относится и скупка кредитных карт у владельцев. Злоу-

мышленники даже размещают объявления о том, что готовы приобрести чужие кредитные карты.

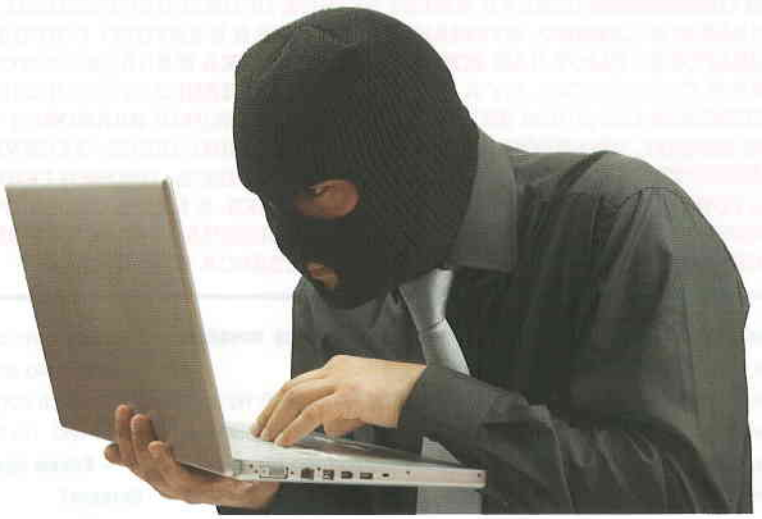
Банк России предупреждает, что, во-первых, сам факт передачи карты представляет собой нарушение правил использования электронных средств платежа, во-вторых, владелец карты рискует быть привлеченным к ответственности как соучастник в случае, если его карта будет использована при совершении противоправных действий.

Поэтому, в случае утраты карты, тем более при ее краже, необходимо как можно скорее сообщить о случившемся в обслуживающий банк по телефону горячей линии.

Подчеркнем, что не следует передавать платежную карту другим лицам, в том числе родственникам. В отличие от находящихся на карточном счете средств, сама карта является собственностью банка, а не клиента. Пользоваться ей может только тот человек, чьи фамилия и имя указаны на карте. Передача карты другим лицам и сообщение им PIN-кода – это нарушение порядка использования электронных средств платежа, устанавливаемого банками-эмитентами и международными платежными системами. При выявлении такой передачи банк в дальнейшем вправе отказать владельцу карты в возмещении денежных средств по совершенным несанкционированным операциям. В случае необходимости предоставить кому-либо доступ к карточному счету лучше обратиться в банк с заявлением на выпуск дополнительной карты, на которой можно установить лимиты расходных операций, а в случае необходимости – заблокировать. Кроме того, отчеты по всем операциям, совершенным с использованием дополнительной карты, будут поступать к основному держателю карты.

Режим безопасности электронных платежей

Для обеспечения безопасного онлайн-банкинга используются такие методы, как двухфакторная аутентификация и протоколы шифрования. Несмотря на сложное наименование, речь идет о поэтапном доступе к онлайн-банку: сначала осуществляется ввод логина и пароля, а затем дополнительных одноразовых кодов для подтверждения проведения операций. Эти коды пользователь может получить в банкомате обслуживающего банка в виде распечатки со списком паролей, на свой мобильный телефон в виде sms-сообщения, создаваемого сервером банка на каждую операцию клиента, а также сгенерировать специальным криптографическим устройством, которое клиент получает при открытии счета и подключении услуги онлайн-банкинга. Самым популярным является отправка sms-сообщения с паролем – она применяется в 91% систем онлайн-банкинга. В 44% систем используется сгенерированный пароль, в 32% систем – пароль из предоставленного клиенту списка.



Для похищения денег с банковского счета злоумышленник должен не только узнать пару «логин-пароль», но и получить доступ к одноразовым кодам. Если телефон, на который ваш банк отправляет sms-сообщения с кодами, потерян или украден, нужно немедленно обратиться к оператору сотовой связи и заблокировать sim-карту. Предоставленный банком список кодов надо также тщательно хранить – он «стоит» не меньше, чем PIN-коды банковских карт. Если список потерян или украден, следует немедленно аннулировать все неиспользованные одноразовые коды.

Следует отметить, что компьютеры с общим доступом (в интернет-кафе, аэропортах, клубах, гостиницах, библиотеках) для входа в систему онлайн-банка или покупок в интернет-магазинах использовать нежелательно. Эти компьютеры могут быть заражены шпионскими программами, и вводимые логины и пароли могут стать известны мошенникам. Не рекомендуется также подключать собственный компьютер, используемый для финансовых операций, к общедоступным сетям Wi-Fi во избежание перехвата трафика администратором сети или киберпреступниками. В случае, если возникает необходимость произвести те или иные действия с использованием собственного устройства, предпочтительно использовать сеть сотового оператора – вероятность злонамеренного вмешательства извне в этом случае ниже, нежели при использовании общедоступных сетей Wi-Fi в общественных местах. ■

по материалам ГУ Банка России по Центральному федеральному округу