ПРОКУРАТУРА
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРОКУРАТУРА
БУРЗЯНСКОГО РАЙОНА
БӨРЙӘН РАЙОНЫ
ПРОКУРАТУРАҺЫ

ул. Уральская, 1/1, с. Старосубхангулово, 453580,
тел.: (34755)3-62-31, факс: (34755)3-52-08

12.01.2024 №1-11-2023/10-24-20800039

на № _____ от _____

380383 916303

Руководителям учреждений
(по списку)

Прокуратурой Бурзянского района во исполнение поручения прокуратуры республики проводится разъяснительная работа по профилактике преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

В указанных целях направляется памятка о правилах безопасности, которую необходимо разместить в чатах мессенджеров, на сайтах, в общедоступных местах, ознакомить трудовые коллективы на оперативных совещаниях.

Дополнительно разъясняю, что информационно-телекоммуникационные технологии могут использоваться диверсионными силами в целях поддержки и финансирования недружественных России агентов различного толка.

Даже неосознанное финансирование деятельности, направленной против интересов России, может стать поводом для проведения проверочных мероприятий.

Прокурор района А.В. Ёлкин

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 577D50F1CBD89910875F16AF5F337592
Владелец Ёлкин Андрей Владиславович
Действителен с 29.05.2023 по 21.08.2024

Прокуратура Бурзянского района Республики Башкортостан
№ 1-11-2023/10-24-20800039

«Осторожно, мошенники!»

Для предупреждения противоправных действий по дистанционному хищению денежных средств важно запомнить следующее.

Сотрудники банка по телефону или в электронном письме не запрашивают:

- персональные сведения (серия и номер паспорта, адрес регистрации, имя и фамилия владельца карты);
- реквизиты, срок действия, ПИН- и CVV-коды банковских карт;
- пароли или коды из СМС-сообщений для подтверждения финансовых операций или их отмены;
- логин и пароль для входа в личный кабинет клиента банка.

Сотрудники банка также не предлагают:

- установить программы удаленного доступа (или иные сторонние приложения) на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки (например, удаление вирусов);
- перейти по ссылке из СМС-сообщения;
- включить переадресацию на телефоне клиента для совершения в дальнейшем звонка от его имени в банк;
- под их руководством перевести для сохранности денежные средства на «защищённые» или «безопасные» счёта;
- зайти в онлайн-кабинет по ссылке из СМС-сообщения или электронного письма.

Чтобы не стать жертвой дистанционного мошенничества следует использовать только официальные каналы связи:

- формы обратной связи на сайте банка и в мобильном приложении;
- телефоны горячих линий;
- группы или чат-боты в мессенджерах (если таковые имеются).

Важно помнить, что мобильные приложения банков следует скачивать через официальные магазины (App Store, Google Play и т.п.).

Необходимо учитывать, что держатель карты обязан самостоятельно обеспечить конфиденциальность ее реквизитов и в этой связи избегать:

- подключения к общедоступным сетям Wi-Fi;
- использования ПИН- или CVV-кодов при заказе товаров и услуг через сеть «Интернет», а также по телефону (факсу);
- сообщения названных кодов третьим лицам (в противном случае любые операции, совершенные с их использованием, считаются выполненными самим держателем карты и не могут быть опротестованы).

При использовании банкоматов отдавайте предпочтение тем, которые установлены в защищённых местах. Перед его использованием, осмотрите и убедитесь, что:

- все операции, совершаемые предыдущим клиентом, завершены;
- на клавиатуре и в месте для приема карт нет дополнительных устройств;
- отсутствуют неисправности и иные повреждения.

При использовании сотовых телефонов (смартфонов) соблюдайте следующие правила:

- при установке мобильных приложений обращайте внимание на полномочия, которые они запрашивают. Будьте особенно осторожны, если приложение просит права на чтение адресной книги, отправку СМС-сообщений и иных уведомлений, доступ к сети «Интернет»;
- отключите в настройках возможность использования голосового управления при заблокированном экране;
- не переходите по ссылкам из СМС-уведомлений, различных чатов и мессенджеров, не убедившись в их достоверности (перезванивайте людям их прислабшим);
- не перечисляйте денежные средства знакомым, родственниками и близким лицам на их просьбы о переводе денежных средств из СМС-уведомлений, различных чатов и мессенджеров, не убедившись в их достоверности (перезванивайте людям их прислабшим);

При использовании интернет-сервисов, в то числе для покупки и продажи товаров и оказания услуг (Авито, Юла и т.п.) запомните ряд простых правил:

- используйте средства общения, предоставленные данными сайтами;
- не переходить на «индивидуальное» общение с посторонними лицами с использованием личных номеров телефонов;
- не передавайте свои персональные данные, в том числа адрес проживания, контактные телефоны, банковские реквизиты и коды подтверждения банковских операций;
- используйте только порядок и формы оплаты, получения товаров, предусмотренные данными интернет-сервисами.

Для минимизации возможных хищений при проведении операций с использованием сети «Интернет» рекомендуется:

- оформить виртуальную карту с установлением размера индивидуального лимита, ограничивающего операции, в том числе с использованием других банковских карт;
- внимательно читать тексты СМС-сообщений и иных уведомлений с кодами подтверждений, проверять реквизиты операций. Если реквизиты не совпадают, то такой пароль вводить нельзя.

В случае утери или смены номера телефона, привязанного к банковской карте, необходимо:

- связаться с банком для отключения услуги СМС-уведомления;
- заблокировать сим-карту, обратившись к сотовому оператору.