ПАМЯТКА

о профилактике и предупреждении дистанционных преступлений использованием информационно-телекоммуникационной сети «Интернет» и мобильных устройств

В условиях развития цифровой экономики, электронных платежных систем, персональных электронных устройств и Интернета стремительно возросло количество совершенных с их использованием преступлений.

Совершению данной категории преступлений способствуют доверчивость граждан, недостаточная осведомленность и пренебрежительное отношение к элементарным правилам безопасности.

Чтобы не оказаться жертвой мошенников необходимо знать следующее:

– сотрудники любого банка никогда не просят сообщить данные вашей карты (реквизиты, срок действия, ПИН- и CVV-коды банковских карт), пароли или коды из СМС-сообщений для подтверждения финансовых операций или их отмены;

– внимательно читайте СМС сообщения приходящие от банка;

– никогда и никому не сообщайте пароли и коды, которые приходят вам в СМС сообщении от банка, не сообщаете пин-код третьим лицам, а так же код на оборотной стороне карты;

– помните, что только мошенники спрашивают пароли, которые приходят к вам в СМС сообщении от банка;

– 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 прислaвшим);

– в сети «Интернет» не переходите по ссылкам на неизвестные сайты
– будьте осторожны, если вам поступило смс-сообщение о выигрыше в случае, когда вы не заполняли заявку на участие либо каким-либо другим способом не подтверждали свое участие в розыгрыше.

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);

• сообщить логин и пароль для входа в личный кабинет клиента банка;

• перейти по ссылке из СМС-сообщения;

• 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;

• пройти к банкомату.
Банк может инициировать общение с клиентом только для консультаций по предоставляемым услугам. При этом звонки совершаются с номеров, указанных на

официальных сайтах и банковских документах. Иные номера не имеют никакого отношения к банку.
Остерегайтесь «телефонных» мошенников, которые пытаются ввести вас в заблуждение.

Избегайте телефонных разговоров с подозрительными людьми, которые представляются сотрудниками банка, операторами Госуслуг, сотрудником службы технической поддержки оператора мобильной связи и т.п., не бойтесь прервать разговор, просто кладите трубку. Прекращение разговора с собеседником, личность которого вызывает подозрение, является идеальным способом защиты.

Для противодействия мошенническим действиям не совершайте операции по инструкциям, полученным в результате телефонного разговора. В случае сомнений в добросовестности звонящего лучше завершить звонок и перезвонить по номеру телефона банка или мобильного оператора (в зависимости от того, кем представился звонящий). При этом следует помнить, что ни сотрудники банка, ни другие третьи лица не могут запрашивать важную конфиденциальную информацию по телефону, в связи с чем звонки с соответствующей просьбой с большей долей вероятности являются мошенническими.

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.

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

При использовании банкоматов 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 приславшим);
• внимательно читайте тексты СМС-сообщений и иных уведомлений с кодами подтверждений, проверьте реквизиты операций. Если реквизиты не совпадают, то такой пароль вводить нельзя.
Стоит помнить о том, что злоумышленники научились подменять телефонные номера, с которых осуществляется вызов. Также следует иметь в виду, что современные технологии умеют подделывать голос и видео на высоком уровне.