ПАМЯТКА

по защите от мошеннических действий и обеспечению безопасности при использовании дистанционного банковского обслуживания

1. Главное правило: конфиденциальные данные не сообщать никому

- Передача посторонним лицам конфиденциальной информации (например, персональных данных, реквизитов платежной карты, пароля из СМС, секретных слов и так далее), может привести к совершению указанными лицами перевода денежных средств без добровольного согласия клиента.
- Эту информацию НЕЛЬЗЯ сообщать по телефону, в СМС, в мессенджерах и на сайтах**:** сотрудник банка никогда не спросит: номер карты, трёхзначный код на её обороте, пароль, код из СМС или пуш-уведомления, кодовое слово, ПИН-код;
- Любой звонок «из службы безопасности банка», «от полиции» или «от ЦБ» с просьбой назвать коды, перевести деньги на «безопасный счёт» или установить приложение — это мошенники. Прервите разговор и позвоните в банк по номеру с обратной стороны вашей карты;
- Если звонящий давит, торопит, пугает блокировкой счёта или «утечкой данных» — это признак мошенничества.

2. Осторожно с программами, письмами и ссылками на Ваших устройствах

- Не устанавливайте приложения по просьбе незнакомых людей «для верификации», «для собеседования», «для работы». Программы удалённого доступа (например, «AnyDesk», «RustDesk» и подобные) дают злоумышленнику полный контроль над вашим телефоном или компьютером: они видят СМС с кодами и заходят в ваш онлайн-банк.
- Не открывайте электронных писем и особенно с вложениями, от незнакомых адресатов, с разными названиями тем и вложений: «Акт сверки», «Счёт на оплату», «Уведомление об окончании срока бесплатного хранения», «Зарплатная ведомость». Если во вложении неожиданный архив с паролем, указанным тут же в тексте письма - однозначно вредоносное ПО, которое отключает антивирус.
- Устанавливайте приложения на телефон только из официальных магазинов (App Store, RuStore, Google Play). Перед установкой проверяйте отзывы и дату обновления. Никаких «обновлений» по ссылкам из писем.
- На компьютере или телефоне не переходите по ссылкам из подозрительных сообщений: «ваша карта заблокирована», «выигрыш», «выплата пенсии», по ссылкам из объявлений о продаже товаров. Вредоносный файл может быть загружен на ваше устройство после перехода по ссылке из письма.

- Удаляйте неиспользуемые приложения.

3. Защита устройств

- Устанавливайте обновления операционной системы и приложений сразу, как только они выходят: обновлённое устройство взломать сложнее.
- Обязательно используйте и своевременно обновляйте антивирус на компьютере и телефоне, с которых осуществляете управление банковскими счетами. Разрешите антивирусу проверять архивы и блокировать подозрительные процессы.
- Используйте антифишинг-системы, в том числе автоматического анализа ссылок (вложений).
- Постоянно контролируйте конфигурацию устройств для своевременного обнаружения вредоносного ПО.
- Придумывайте пароли длиной не менее 8 символов, состоящие из строчных и прописных букв, специальных символов, разные для каждого сервиса, без дат рождения и имён близких. Регулярно меняйте пароли.
- Никогда не оставляйте компьютер с открытой сессией дистанционного банковского обслуживания (ДБО) без присмотра. Даже на минуту. Блокируйте экран (Win+L) при отходе.
- Не оставляйте носитель с электронной подписью уполномоченных лиц организации постоянно подключенным к USB порту компьютеров. Производите его извлечение из USB-порта сразу после подписания платежных поручений.
- Ограничьте возможности импортирования сертификатов электронной подписи на рабочие персональные компьютеры работников бухгалтерии, или других подразделений, осуществляющих проведение платежей со счетов юридического лица.
- Ограничьте права пользователя: сотрудник, работающий с ДБО, не должен иметь прав администратора на своём компьютере.
- Включите двухфакторную аутентификацию там, где это возможно (подтверждение платежа по SMS, push, звонок).
- Настройте уведомления о любых операциях по счёту - SMS или push от банка. Это поможет заметить попытку перевода мгновенно.
- Если вы формируете зарплатный реестр, всегда сверяйте получателей и суммы. Мошенники могут подменить реквизиты в уже готовом файле.
- Если Вы юридическое лицо ограничьте бесконтрольный доступа работников в сеть «Интернет». С помощью аппаратных или программных средств сетевой защиты (Firewall, корпоративные прокси-серверы) ограничьте доступ в сеть «Интернет». Маршрутизируйте трафик таким образом, чтобы разрешать соединения только с доверенными ресурсами.

4. Подготовка к утере или краже телефона

- Установите автоблокировку экрана (код или биометрия).
- Включите функцию удалённого поиска и стирания данных (Find My iPhone, Find My Device и аналоги).
- Делайте регулярные резервные копии данных.
- Запишите номера телефонов банка, чтобы заблокировать карты и дистанционное банковское обслуживание в случае утери устройства.
- Если телефон украден — первым делом позвоните оператору связи (заблокируйте SIM-карту) и в банк (заблокируйте карты и доступ к онлайн-банку).

5. Если операция прошла без вашего согласия

- Не перезагружайте компьютер, не запускайте антивирусные решения, извлеките криптографический токен (ключ ЭП), отключите компьютер от локальной сети, сети Интернет или Wi-Fi. Это разорвёт удалённое соединение злоумышленника, т.к. Ваш компьютер может находится в данный момент под удаленным управлением злоумышленников.
- Как можно быстрее позвоните в банк по официальному номеру и сообщите о несанкционированной операции, заблокируйте карту или счёт.
- Выполните процедуры создания образов оперативной памяти и жесткого диска с использованием специализированного программного обеспечения (например, «FTK Imager») для дальнейшего проведения расследования.
- Сохраните образец вредоносного программного обеспечения для обеспечения возможности проведения последующего анализа.
- В случае заражения мобильного устройства, необходимо включить авиа-режим и извлечь SIM-карту. Если в устройстве используется электронная сим-карта, допустимо выключить устройство.
- Сбрасывать устройство до заводских настроек не рекомендуется, так как это приведет к удалению следов вредоносной активности и затруднит дальнейшее проведение расследования.
- Подайте в банк заявление о спорной операции и обращение в полицию.
- Сохраняйте все сообщения, чеки и детали переписки — они пригодятся для разбирательства.

6. Остерегайтесь вовлечения в мошенничество (дропперство)

- Не открывайте счёт или карту на своё имя «за вознаграждение» по просьбе третьих лиц и не передавайте им доступ к своим счетам.
- За вывод и обналичивание чужих денег предусмотрена ответственность вплоть до уголовной. Банк может ограничить дистанционное обслуживание, а сведения о вас могут попасть в базу Банка России.