АРЕСБАНК

БАНК РОССИИ ФИНЦЕРТ

АКТУАЛЬНЫЕ МОШЕННИЧЕСКИЕ СХЕМЫ

Мошенничество от имени руководителя в мессенджерах

Злоумышленники рассылают сообщения от имени руководителя или директора компании. «Руководитель» рассказывает, что в компании произошла утечка данных. Под угрозой само существование организации, поэтому в ближайшее время сотрудникам будут звонить некие важные люди из органов.

Проверьте профиль отправителя: часто мошенники используют похожие имена или фото, но небольшие ошибки в имени или номере телефона выдают их самостоятельно на свой телефон. Если вы регулярно общаетесь с ним в мессенджерах, у вас должна храниться история сообщений. Свяжитесь с руководителем по телефону или лично, чтобы подтвердить запрос.

Мошенничество через мобильные игры

Мошенники звонят или пишут в мессенджерах, утверждая, что вы выиграли крупную сумму денег или приз в мобильной игре. Они предлагают перевести выигрыш на ваш счет, но для этого требуют доступ к вашему телефону с интернет-банком или данные карты. Мошенники могут также воздействовать на детей, предлагая им внутриигровую валюту, редкие предметы или доступ к платному контенту в обмен на данные банковской карты родителей или доступ к их телефону.

Обучайте детей основам информационной безопасности. Никогда не предоставляйте доступ к телефону или интернет-банку незнакомым лицам. Не сообщайте данные карты или пароли из СМС.

АРЕСБАНК

БАНК РОССИИ ФИНЦЕРТ

АКТУАЛЬНЫЕ МОШЕННИЧЕСКИЕ СХЕМЫ

Фишинг через поздравления в соцсетях

Мошенники находят пользователей соцсетей, у которых день рождения, и отправляют им персонализированные поздравления с обещанием подарков. В сообщении содержится ссылка через VK Link, ведущая на фишинговый сайт, замаскированный под известный бренд. Жертва, вводя свои данные (например, банковскую информацию или учетные записи), передает их злоумышленникам, которые автоматически получают сведения через Telegram-бот и используют их в мошеннических схемах.

Не переходите по подозрительным ссылкам, даже если они выглядят правдоподобно. Проверяйте адрес сайта, прежде чем вводить личные данные. Настройте приватность профиля в соцсетях, чтобы ограничить доступ к информации.

Мошеннические схемы «с поручителем»

При совершении онлайн-покупок, чаще всего связанных с приобретением игровых предметов или аккаунтов злоумышленник выступает от имени покупателя. Связывается с владельцем аккаунта и предлагает приобрести его дороже рыночной стоимости. В ходе переписки мошенник высказывает сомнения по поводу сделки и просит дать контакты лица, которое может подтвердить, что жертва действительно является владельцем этого аккаунта. Получив контакты человека, согласившегося выступить в качестве «поручителя», аферисты создают копию его аккаунта в мессенджере с использованием подменного номера и уже от его лица связываются с потенциальной жертвой.

Не передавайте контактные данные третьих лиц без их согласия. Проверяйте подлинность сообщений, особенно если собеседник просит деньги или коды. Если знакомый пишет с нового номера – свяжитесь с ним другим способом. Не сообщайте никому коды подтверждения.

АРЕСБАНК

БАНК РОССИИ ФИНЦЕРТ

ФИШИНГОВЫЕ САЙТЫ И МОШЕННИЧЕСКИЕ СХЕМЫ

Мошенники активно используют фишинговые сайты для кражи личных данных и финансовых средств. Они создают поддельные веб-страницы, копирующие популярные сервисы, и обманным путем вынуждают пользователей вводить свои учетные данные, данные банковских карт или выполнять переводы денег.

Распространенные схемы фишинга:

– *Фальшивые сайты с "уникальными" предложениями – например, мошенники распространяют ссылки на сайты, якобы продающие популярные товары, такие как «дубайский шоколад», по привлекательным ценам. После оформления заказа покупатели либо остаются без товара, либо теряют деньги и конфиденциальные данные.*

– *Поддельные сервисы для совместных поездок – мошенники создают фишинговые копии BlaBlaCar и других популярных платформ, заманивая пользователей выгодными предложениями. После ввода данных карты для бронирования поездки деньги списываются, но поездка не подтверждается.*

– *QR-коды для "домовых чатов" – в ряде регионов злоумышленники размещают объявления с предложением вступить в домовые чаты через поддельные QR-коды. При сканировании таких кодов пользователи могут попасть на вредоносные сайты, которые крадут их данные или устанавливают вредоносное ПО.*

– *Фальшивые "официальные письма" от ведомств – граждане получают уведомления о якобы имеющихся задолженностях с угрозами штрафов и ареста имущества в случае неуплаты. В таких письмах указывается конкретная сумма долга, прилагается QR-код или ссылка для перехода к оплате, которую предлагают провести через Систему быстрых платежей (СБП). Иногда злоумышленники заманивают жертв "скидками", которые действуют только при немедленной оплате.*

Как защититься от фишинга:

✓ *Проверяйте адрес сайта перед вводом личных данных – мошеннические сайты могут иметь незначительные отличия в доменном имени.*

✓ *Не переходите по сомнительным ссылкам из мессенджеров, социальных сетей и рассылок.*

✓ *Используйте двухфакторную аутентификацию для защиты аккаунтов.*

✓ *Не сканируйте QR-коды из подозрительных источников.*

✓ *Покупки совершайте только на проверенных сайтах с надежной репутацией.*

АРЕСБАНК

БАНК РОССИИ ФИНЦЕРТ

УСТАНОВКА ВРЕДОНОСНОГО ПО

Злоумышленники используют различные схемы для распространения вредоносных *программ, которые могут воровать личные данные, перехватывать банковские операции или предоставлять удаленный доступ к устройству.*

Опасные схемы установки вредоносного ПО:

– *Файлы APK, маскирующиеся под видео или другие форматы – мошенники отправляют пользователям файлы с расширением .apk (исполняемые файлы для Android), выдавая их за видео, документы или изображения. При установке такого файла на смартфон загружается вредоносное ПО, которое может:*
  - *Перехватывать пароли и коды из СМС,*
  - *Красть банковские данные,*
  - *Открывать доступ к переписке и файлам на устройстве,*
  - *Незаметно отправлять платные СМС или подписывать на дорогостоящие услуги.*

– *Уязвимости, использующие NFC – примером является приложение NFCGate, которое позволяет злоумышленникам перехватывать и изменять передаваемые через NFC данные. Вредоносные версии подобных инструментов могут использоваться для атак на бесконтактные платежи и подмены информации, передаваемой между устройствами.*

Как защититься от вредоносного ПО:

✓ *Не скачивайте файлы APK из непроверенных источников, даже если они приходят от знакомых (их аккаунты могли взломать).*

✓ *Не устанавливайте приложения вне Google Play или официальных магазинов.*

✓ *Проверьте разрешения перед установкой – если приложение требует доступ к SMS, контактам или банковским данным без явной необходимости, это тревожный знак.*

✓ *Отключите возможность установки приложений из неизвестных источников в настройках телефона.*

✓ *Будьте осторожны с NFC – включайте его только при необходимости и используйте надежные платежные системы с защитой.*

АРЕСБАНК

БАНК РОССИИ ФИНЦЕРТ

ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ ФИНАНСОВОГО МОШЕННИЧЕСТВА

Шаг № 1

Немедленно заблокируйте карту с помощью мобильного приложения или личного кабинета на сайте банка. Заблокировать ее также можно через контакт-центр банка (телефон указан на оборотной стороне карты) или в любом его отделении.

Шаг № 2

В течение суток после получения сообщения о списании средств напишите заявление в отделении банка о несогласии с операцией.

Шаг № 3

Обратитесь с заявлением о хищении денег в любое отделение полиции.

При подозрении, что в отношении вас могут совершаться или совершаются мошеннические действия (получили подозрительное письмо, странный звонок или СМС/PUSH – сообщение) – незамедлительно обратитесь в ООО КБ «АРЕСБАНК».

Головной офис ООО КБ «АРЕСБАНК»:
+7 (495) 795-32-88 (*пн.-чт.: с 9:00 до 18:00, пт.: с 9:00 до 16:45*)

Филиал «Тульский» ООО КБ «АРЕСБАНК»:
+7 (4872) 36-33-72 (*пн.-чт.: с 9:00 до 17:30, пт.: с 9:00 до 16:30*)

Контакт – центр для блокировки карт:
- по России: **8 (800) 200-45-75** (*круглосуточно*)
- за пределами России: **+7 (383) 363-11-58** (*круглосуточно*)