

Одноклассники и др.), после чего вступает в переписку с друзьями пользователя и просит занять денежные средства под различными предложениями (болезнь родственника, срочная покупка и пр.).

- Не спешите переводить денежные средства. Позвоните другу по телефону, задайте вопросы-ловушки.

• **ПОЗВОНИЛ НЕЗНАКОМЕЦ И ПОТРЕБОВАЛ ДЕНЬГИ ДЛЯ СПАСЕНИЯ РОДСТВЕННОКА, ПОПАВШЕГО В БЕДУ:** Требование крупной суммы денег для решения проблемы с якобы попавшим в беду родственником.

- Не переводите денежные средства! Прекратите телефонный разговор. Позвоните родственнику по знакомому номеру.

• **ПОЗВОНИЛ «РОДСТВЕННИК» И ПОПРОСИЛ ПЕРЕВЕСТИ ДЕНЬГИ С ЦЕЛЬЮ ИЗБЕЖАНИЯ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ:** Просьба перевода крупной суммы денег для решения проблемы с якобы совершением им противоправных действий (совершение дорожно-транспортного происшествия, причинение телесных повреждений и материального ущерба и пр.). Для придания реальности произошедшего в телефонный разговор подключается другой злоумышленник, который представляется сотрудником полиции, следственного комитета, прокуратуры.

- Не переводите денежные средства! Прекратите телефонный разговор. Позвоните родственнику по знакомому номеру.

• **ПРЕДЛОЖЕНИЕ В СЕТИ ИНТЕРНЕТ О ДОПОЛНИТЕЛЬНОМ ЗАРАБОТКЕ ПУТЕМ ВКЛАДЫВАНИЯ ДЕНЕЖНЫХ СРЕДСТВ В КРИПТОВАЛЮТУ ИЛИ ПУТЕМ ИГРЫ НА ФИНАНСОВЫХ БИРЖАХ ЧЕРЕЗ ОПРЕДЕЛЕННЫЕ КОМПАНИИ:** Злоумышленник предлагает потенциальному покупателю внести денежные средства для получения в дальнейшем дополнительного заработка, не намереваясь фактически исполнять взятые на себя обязательства. Все общение со злоумышленниками осуществляется дистанционно через средства телефонной связи и социальные мессенджеры.

- Не переводите денежные средства на счета злоумышленников, не удостоверившись в реальном существовании организаций и роде их деятельности!



ПРОКУРАТУРА ВОЛОГОДСКОЙ ОБЛАСТИ

О способах мошенничества, совершаемых с использованием информационно-телекоммуникационных технологий

г. Вологда
2023 год



С каждым годом все больше людей становятся потерпевшими от действий мошенников! Злоумышленники, похищая денежные средства граждан, могут представляться сотрудниками банка, правоохранительных органов, представителями других официальных ведомств и организаций, знакомыми или друзьями Ваших близких. Звонки или СМС-оповещение теперь могут поступить не только с неизвестного номера, но и схожего или дублирующего номера рассылки банка или другого кредитно-финансового учреждения.

При этом мошенники **постоянно придумывают новые способы** выманить у людей деньги или конфиденциальные данные для доступа к счетам.

Но какой бы ни был способ совершения преступления, **есть приметы, по которым можно сразу же вычислить мошенников:**

1. На Вас выходят сами.
2. С Вами говорят о деньгах.
3. Вас просят сообщить свои данные.
4. Вас выводят из эмоционального равновесия.
5. На Вас оказывают давление, не давая времени обдумать ситуацию.

Наиболее распространенные схемы мошенничества и краж, а также действия по исключению фактов хищения денег:

• **ЗВОНОК ОТ «СПЕЦИАЛИСТА» САЙТА ГОСУСЛУГ О ВЗЛОМЕ УЧЕТНОЙ ЗАПИСИ:** Злоумышленник в ходе разговора под различными предложениями (изменение пароля для входа в учетную запись, изменение номера телефона, привязанного к учетной записи и пр.) узнает о поступающих паролях на телефонный номер потерпевшего, в результате чего мошенник получает доступ к учетной записи последнего, с помощью которой впоследствии осуществляется оформление кредита.

- Прекратите разговор! Никому не сообщайте поступающие на мобильный телефон пароли.

• **ЗВОНОК ОТ «ПРЕДСТАВИТЕЛЯ» СЛУЖБЫ БЕЗОПАСНОСТИ БАНКА О ЯКОБЫ СОВЕРШАЕМЫХ СОМНИТЕЛЬНЫХ ОПЕРАЦИЯХ ПО БАНКОВСКОЙ КАРТЕ ПОТЕРПЕВШЕГО ИЛИ О БЛОКИРОВКЕ КАРТЫ:** Злоумышленник в ходе разговора узнает от собеседника всю информацию о банковской карте (ее номер, срок действия, CVV-код и пр.) и о поступающих паролях на телефонный номер, в результате чего впоследствии осуществляются неправомерные переводы с банковского счета потерпевшего.

- Прекратите разговор! Никому не сообщайте данные о своей банковской карте, и поступающие на мобильный телефон пароли.

• **ПРОДАВЕЦ-МОШЕННИК РАЗМЕЩАЕТ НА САЙТАХ ОБЪЯВЛЕНИЙ (АВИТО, ЮЛА, ЦИАН И ДР.) ИНФОРМАЦИЮ О ПРОДАЖЕ КАКОГО-ЛИБО ТОВАРА, СДАЧЕ В АРЕНДУ ЖИЛЫХ ПОМЕЩЕНИЙ ИЛИ ОКАЗАНИИ ПЛАТНЫХ УСЛУГ:** Злоумышленник предлагает потенциальному покупателю внести предоплату, не намереваясь в дальнейшем исполнять взятые на себя обязательства.

- Не переводите денежные средства в качестве предоплаты!

• **ПОКУПАТЕЛЬ-МОШЕННИК ЗВОНИТ ЛИЦУ, РАЗМЕСТИВШЕМУ ОБЪЯВЛЕНИЕ НА САЙТАХ ОБЪЯВЛЕНИЙ (АВИТО, ЮЛА, ЦИАН И ДР.), И СООБЩАЕТ О ЖЕЛАНИИ ПРИОБРЕСТИ ТОВАР:** Злоумышленник сообщает о желании внести задаток за приобретаемый товар, для чего просит продиктовать сведения о банковской карте и поступивший на телефон потерпевшего код либо потерпевший под влиянием мошенника с использованием банкомата выполняет ряд комбинаций, в результате чего подключается мобильный банк на телефонный номер злоумышленника. В результате вышеуказанных действий с банковского счета потерпевшего впоследствии списываются денежные средства.

- Никому не сообщайте данные о своей банковской карте, и поступающие на мобильный телефон пароли, не осуществляйте без необходимости операции по изменению учетных данных банковской карты!

• **МОШЕННИЧЕСТВО СО ВЗЛОМОМ СТРАНИЦ СОЦИАЛЬНЫХ СЕТЕЙ:** Злоумышленник осуществляет взлом персональной страницы пользователя социальной сети (Вконтакте,