**ПРОКУРАТУРА УБИНСКОГО РАЙОНА РАЗЪЯСНЯЕТ**

«Меры, которые необходимо принять в случае подозрения о совершении дистанционного мошенничества (если вы только что разгласили данные, которые мошенники могут использовать для взлома учетной записи, например, код двухфакторной идентификации, CVV и т.д.). Банковская карта. Риск: взлом учетной записи в банковском сервисе, кража денег со счетов, оформление кредита на жертву. 1. Необходимо оперативно сменить пароль, код доступа в банковский сервис. 2. Заморозить банковские карты и счета. 3. Оперативно свяжитесь с банком по номеру, указанному на банковской карте или официальном сайте, сообщите о звонке или сообщении - продиктуйте им номер телефона злоумышленников. Далее банк будет самостоятельно принимать меры по блокировке вашего счета, перевыпуску карт и блокировке номера мошенника. 4. Предупредите родных, близких, работодателя, что пока ваши банковские карты могут быть скомпрометированы и лучше не переводить на них деньги. Сервис государственных услуг Риск: компрометация личной информации, подтверждение личности в кредитной организации, сервисе мобильного оператора, оформление кредита. 1. Необходимо оперативно сменить пароль, код доступа в банковский сервис. 2. Позвоните на горячую линию сервиса и сообщите о возможной компрометации. 3. Если есть доступ к личному кабинету, проверьте заявки, разрешения, в том числе в сторонних сервисах. 4. Обратитесь в МВД и передайте всю возможную информацию об инциденте. Мобильный номер Прокуратура Убинского района Новосибирской области 2 Риск: злоумышленники смогут сбросить пароли и получать коды двухфакторной идентификации во всех сервисах, в которых указан украденный номер. 1. Свяжитесь с вашим мобильным оператором (по официальному номеру телефона, в приложении или в салоне связи) и сообщите, о том, что ваш номер, может быть, скомпрометирован. Сотрудник клиентского сервиса должен предложить алгоритм действий. Порядок действий может немного отличаться в зависимости от вашего мобильного оператора. 2. По возможности, привяжите сервисы, соцсети, мессенджеры к нескомпрометированному номеру телефону. 3. Внимательно следите за приходящими смс о блокировке, перевыпуске или переносе SIM-карты. 4. Предупредите родных, друзей, коллег, что с вашего номера могут звонить, писать злоумышленники с просьбой одолжить денег, поделиться чувствительной информацией и т.д. Мессенджеры и соцсети Риски: компрометация переписок, доступ злоумышленников к чувствительной информации, мошенничество с просьбой одолжить деньги, шантаж. Использование аккаунта в дальнейших сложных кибер-преступных схемах. 1. Попробуйте сменить пароль на совершенно новый и достаточно сложный, включить двухфакторную идентификацию. 2. В списке привязанных к аккаунту устройств нужно срочно отключить все незнакомые и недоступные вам девайсы. 3. Смените пароли, защитите ссылки, которые могли быть в переписках. 4. Если подозреваете, что учетная запись скомпрометирована, например, не приходят одноразовые коды безопасности, то следуют сразу обратиться в службу поддержки. 5. Предупредите ваш круг контактов, что вашим аккаунтом в мессенджере могут завладеть злоумышленники с целью, например, рассылать сообщения с просьбой одолжить денег. 6. Попросите родственников и близких: если мошенники будут писать с украденного контакта, то следует массово жаловаться в службу поддержки мессенджера. Риски можно свести к минимуму, если заблаговременно соблюдать правила цифровой гигиены, настроить все доступные инструменты безопасности в сервисах, не переходить по подозрительным ссылкам, не открывать сомнительные файлы и не сообщать посторонним персональную информацию и коды безопасности». Заместитель прокурора района юрист 1 класса С.П. Лобыня