Прокуратура г. Александровска Пермского края

РАЗЪЯСНЯЕТ: КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКА

В соответствии с ч . 1 ст. 159.6 УК РФ мошенничество в сфере компьютерной информации наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев с банковского счета, а равно в отношении электронных денежных средств

С распространением цифровых технологий отмечается рост преступлений, связанных с хищением чужого имущества путем обмана либо злоупотребления доверием, т.е. мошенничества.

Не вводите личные данные. Обычно для входа в интернет-банк кредитная организация запрашивает от клиента только логин и пароль. Номер телефона, данные паспорта, ПИН-код и другие личные данные - все это требовать от вас не должны.

Проверяйте адрес сайта. Если адрес сайта отличается даже одной буквой - это вредоносный сайт. Если интернет-обозреватель предупреждает, что сертификату безопасности сайта доверять нельзя - не доверяйте.

Пользуйтесь одноразовым паролем. Для защиты от мошенников большинство банков при подтверждении операций просят вводить одноразовый пароль. Это очень важный элемент безопасности, который никому и ни при каких обстоятельствах разглашать нельзя.

Не входите в свой личный кабинет с чужих компьютеров. Лучше входить в интернет-банк только со своего персонального компьютера. А вот рабочее место или интернет-кафе - не лучшее место для этого. Если же в силу определенных причин вам пришлось войти в личный кабинет с чужого компьютера, обязательно по окончании работы нажмите иконку "выход" и очистите кэш-память.

Используйте сложный пароль. Придумайте для входа в онлайн-банкинг сложный пароль и никому его не сообщайте, а тем более не записывайте на карте. Лучше не ставить такой пароль на автоматическое запоминание, а каждый раз вводить его вручную.

Обновляйте антивирус. Первое, что нужно сделать, это установить антивирус на ваш компьютер и в дальнейшем его своевременно обновлять. Еще один вариант - разрешить его автоматическое обновление. Далее следует периодически производить антивирусную проверку для своевременного обнаружения вредных программ.

Устанавливайте современные операционные системы. Старайтесь не использовать старые операционные программы, лучше отдать предпочтение более своевременным и в дальнейшем их обязательно обновлять. Это относится также к интернет-браузеру и почтовым программам. Дело в том, что последние обновления операционных систем разрабатываются с учетом новых появившихся вирусов.

Применяйте дополнительное программное обеспечение. Используйте "программы-сторожа", персональные межсетевые экраны, программы защиты от спам-рассылок и др.

Используйте кодированное соединение. Проверяйте, что установлено защищенное (кодированное) соединение с официальным сайтом банка. Самое распространенное - это SSL-соединение, которое поддерживается большинством современных браузеров. Определить, используется ли защищенное соединение, можно по адресу в браузере: там должно стоять https.

Подключите СМС-оповещение. Такая услуга сейчас предоставляется практически во всех банках - клиенту подключается СМС-уведомление по операциям с картой. При получении сообщения об операции, которую вы не совершали, следует сразу же обратиться по телефону в службу поддержки вашего банка.

Установите лимиты на операции в интернет-банке. Можно установить лимиты на онлайн-операции по карте. Так мошенники не смогут снять с карты больше той суммы, на которую установлено ограничение.

ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ , НЕЗАМЕДЛИТЕЛЬНО ОБРАТИТЕСЬ В ТЕРРИТОРИАЛЬНЫЙ ОТДЕЛ ПОЛИЦИИ