

## **КАК РЕАГИРОВАТЬ НА МОШЕННИКОВ И ВЫМОГАТЕЛЕЙ**

- Нельзя выиграть в лотерею или получить налоговый вычет случайно, предварительно не предпринимая никаких действий.
- Электронные письма, которые приходят к Вам, могут содержать вредоносные ссылки или программы, а следовательно, не стоит переходить по незнакомым ссылкам, сохранять подозрительные файлы. А также верить провокации, что ваши данные были украдены и вам нужно перевести деньги для их спасения.
- Любую информацию, касающуюся ваших действий, стоит перепроверять. Мошенники могут представиться банком, полицией, органом власти. Помните, что сейчас существует возможность подмены номера.
- Старайтесь сохранять спокойствие, состояние паники - это то, что хотят вызвать у вас злоумышленники. В таком состоянии человек не способен использовать критическое мышление.
- В РФ органы государственной власти, ведомства и службы не высылают документы гражданам на личную почту. Штрафы, повестки и прочие документы проходят на портал Государственных услуг.
- Передача персональных данных и личной информации третьим лицам недопустима. Мошенники часто говорят о подозрительных операциях, или иной активности как с вашими счетами и вкладами, так и с их получением. Сотрудники банка могут уточнить у вас для идентификации только кодовое слово оставленное вами при регистрации.

## **КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ**



## **ВАЖНО ОБРАЩАТЬ ВНИМАНИЕ ЕСЛИ ВАМ ПРЕДЛАГАЮТ:**

- назвать номер банковской карты, трёхзначный код на оборотной стороне карты, ПИН-код;
- произвести манипуляции с банковской картой у банкомата;
- сообщить пришедший на телефон код;
- перевести сумму денег (аванс, залог, пошлина, налог, ошибочно переведённый платеж и т.п.);
- перейти по ссылке в Интернете, в СМС-или ММС-сообщении на смартфоне;
- позвонить по указанному в СМС-сообщении номеру телефона;
- отправить ваш номер телефона;
- отправить СМС-сообщение на короткий номер;
- назвать пароли от ваших личных страничек в социальных сетях.

## **КЛЮЧЕВЫЕ РЕКОМЕНДАЦИИ**

- Создайте уникальный и надежный пароль для каждого сайта.
- Не переходите по ссылкам в письмах или сообщениях от неизвестных отправителей.
- Проверьте детали: опечатки в адресе сайта, странные адреса сайтов (например, Госуслуги расположены по адресу gosuslugi.ru, у сайта-подделки может быть адрес gosuslugil.ru) и ошибки в текстах — признаки опасных страниц.
- Не публикуйте личные данные на подозрительных сайтах, такие как номер телефона, адрес электронной почты, номер кредитной карты.
- Не стоит доверять сообщениям о подарках и внезапных выигрышах, особенно если Вы не участвовали в розыгрышах.



- Используйте актуальные версии браузеров, антивирусных программ.
- Периодически проверяйте своё устройство на наличие вирусов и вредоносных программ. При обнаружении, их необходимо вылечить и обезвредить с помощью антивирусной программы.
- При потере своей банковской карты, необходимо обратиться в банк и заблокировать карту. Не забывайте периодически следить за вашей банковской активностью. В случае странных действий, которые Вы не совершали, обратитесь в банк.
- Приобретайте услуги, вещи и лекарственные препараты только на проверенных сайтах.
- Используйте антивирусные программы и устанавливайте СМС верификацию входа в аккаунт.