Как действуют мошенники:

-вводят в заблуждение и требуют срочного решения: могут сообщать о близких, которые якобы попали в беду, и просить срочно перевести деньги;
-присылают сообщение якобы от имени банка о подозрительных операциях с вашими деньгами или о блокировке счёта, просят сообщить код из СМС, перезвонить по указанному номеру, крадут личные данные или заражают устройство вирусом, который даст им доступ к данным банковских карт;
-предлагают «выгодную» работу и требуют зарегистрироваться на неизвестном сайте или предоставить данные банковской карты под предлогом зачисления «аванса»;
-предлагают упростить процедуру личного банкротства, быстрее, легче получить кредитные или ипотечные каникулы, помочь оформить пособия, справки 2-НДФЛ;
-организуют псевдоблаготворительные акции (в том числе для пострадавших от COVID-19), забирая собранные средства себе.

Мошенничество путём манипулирования через телефонные звонки, СМС

Кем может представиться мошенник:

-родственником или другом, якобы попавшим в беду;
-сотрудником Пенсионного Фонда России или других официальных организаций, которые оформляют льготы и путевки, пенсии и пособия;
-сотрудником службы занятости, кадрового агентства или известной компании, которые предлагают удаленную работу и при этом просят оплатить регистрационный взнос;
-сотрудником банка, который сообщает о подозрительных операциях с вашей картой и для их отмены требует продиктовать данные карты или код из СМС;
-сотрудником благотворительного фонда или волонтером, который собирает средства на срочное лечение или иную благотворительную цель;
-покупателем вашего товара, который хочет узнать данные вашей карты или код из СМС, чтобы якобы перевести вам деньги.

Как не стать жертвой телефонных мошенников:

- Если вы получили СМС о переводе, которого не совершали, позвоните в банк по официальному номеру, не стоит возвращать деньги самостоятельно;
- Не сообщайте никому логины и пароли от банковских приложений, коды из СМС, данные банковских карт;
- Будьте крайне внимательны и осторожны при переходе по ссылкам, указанным в получаемых от банка сообщениях;
- Установите мобильное приложение Getcontact и проверяйте неизвестные номера
- Проверяйте информацию о благотворительных акциях на официальных страницах известных вам благотворительных организаций;
- Отказывайтесь от сомнительных предложений заработать деньги или участвовать в «успешном» проекте с обязательным первоначальным взносом;
- Проверяйте на официальных сайтах государственных органов информацию о мерах поддержки – например, на сайте Роспотребнадзора www.rospotrebnadzor.ru/region/korono_virus/zachit_prav.php

Как действуют мошенники:

-присылают сообщение в мессенджере о снятии с вашего счета денежных средств и о том, что их можно вернуть, перейдя по прикрепленной ссылке;
-взламывают страницы друзей и родственников в социальных сетях, пишут от их имени и просят перевести деньги;
-используют чужие фотографии товара и просят заранее оплатить покупку, не собираясь ее отправлять;
-создают копии сайтов банков, интернет-магазинов , благотворительных организаций с полями для ввода платежных данных;
-просят у получателя письма помощи в многомиллионных денежных операциях, обещая солидные проценты с сумм, при соглашении выманивают у получателя выманивают все более крупные суммы денег, а в итоге оставляют ни с чем ;

Кибермошенничество (через интернет)

Актуально во время коронавируса!

Мошенники создают сайты, где продаются поддельные товары и услуги: псевдолекарства, псевдотесты и псевдовакцины от коронавируса; поддельные больничные листы с информацией о перенесенном COVID-19; псевдодезинфекцию квартиры.

Как не стать жертвой кибермошенников:

- -если собираетесь вводить личные/платежные данные в интернете – проверьте, что адрес начинается с https, (в конце обязательно должна быть буква «s»);
- -читайте отзывы об онлайн-магазине;
- -регулярно обновляйте программное обеспечение и антивирус телефона и компьютера;
- -не вкладывайте деньги в подозрительные схемы, обещающие огромных заработков за короткое время;
- -если ваш друг или знакомый обращается с просьбой о финансовой помощи в соцсети, задайте несколько личных вопросов, чтобы убедиться, что это именно ваш близкий, а не мошенник;
- -не переходите по коротким ссылкам вида bit.ly и goo.gl, если не доверяете источнику.