КАК ИХ РАСПОЗНАТЬ?

ТОЛЬКО МОШЕННИКИ:

- Звонят под видом сотрудника банка или сотрудника полиции
- Предлагают положить деньги на "безопасный" счет
- Просят сообщить реквизиты карты или код из СМС
- Требуют деньги за спасение родственника от уголовной ответственности
- Просят оплатить "комиссию" за выигрыш

ЗАПОМНИТЕ!

НЕ ОТВЕЧАЙТЕ НА ЗВОНКИ, поступившие с неизвестных номеров, особенно зарегистрированных в другом регионе;

НЕ ВЕРЬТЕ любой информации от незнакомца, **ДАЖЕ ЕСЛИ** звонок поступил с официального телефона горячей линии банка;

ПРЕРВИТЕ РАЗГОВОР и самостоятельно позвоните на телефон горячей линии банка, набрав номер **ВРУЧНУЮ**;

ПОМНИТЕ: код от вашей карты и пароли подтверждения операции **НЕ ИМЕЕТ ПРАВА** спрашивать даже сотрудник банка!

НИКОГДА НЕ ПРИНИМАЙТЕ ПОСПЕШНЫХ РЕШЕНИЙ

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

СОТРУДНИКИ СЛУЖБЫ БЕЗОПАСНОСТИ БАНКОВ НИКОГДА НЕ ЗВОНЯТ КЛИЕНТАМ ДЛЯ ПРЕДУПРЕЖДЕНИЯ ОБ ИМЕЮЩИХСЯ ПРОБЛЕМАХ, СВЯЗАННЫХ С КАРТАМИ!



Не следуйте инструкциям звонивших и не отвечайте на задаваемые вопросы, а просто положите трубку!



Проверить информацию можно, позвонив в контактный колл-центр банка по телефону, указанному на задней стороне вашей банковской карты.

Никогда и никому не сообщайте данные своей банковской карты (ПИН-код, код безопасности, пароли и др.)

Знайте, что мошенники уже могут располагать некоторой информацией о ваших персональных данных! Будьте внимательны!







Если у Вас возникло подозрение, что Вы столкнулись с мошенниками:

- не паникуйте
- немедленно прекратите разговор
- перезвоните в банк для проверки информации
- сообщите о звонке мошенников в полицию:

112 или 02

ПРЕДУПРЕДИТЕ СВОИХ РОДНЫХ И БЛИЗКИХ

Дежурная часть ОМВД России по Гагаринскому району г. Севастополя
8 (8692) 73-87-00,
8 (8692) 73-87-01,
8 (8692) 73-87-02

ПРОКУРАТУРА ГАГАРИНСКОГО РАЙОНА ГОРОДА СЕВАСТОПОЛЯ



ВАША ЗАЩИТА ОТ МОШЕННИКОВ: РУКОВОДСТВО ПО БЕЗОПАСНОСТИ В ЦИФРОВОМ МИРЕ



ОСТОРОЖНО, **МОШЕННИКИ!**

Хищения средств в интернете проходят по нескольким сценариям:

Онлайн банкинг



С помощью сайтов-зеркал (копий настоящих сайтов банков) или вредоносного ПО мошенники получают доступ к личному кабинету клиента.
Также мошенники совершают звонки, представляясь сотрудниками банка и запрашивая у клиента его идентификационные данные.

Мобильный банкинг



На мобильное устройство пользователя загружается вредоносное ПО, с помощью которого мошенники могут посредством SMS списывать деньги с банковского счета без ведома его законного владельца.

Онлайн шоппинг



При совершении покупок в онлайн-магазинах злоумышленники получают данные карты, в том числе и CVV/ CVC-код.
Другой вид обмана реализуется, когда хотят что-то купить у пострадавшего: мошенник переводит на его счет бОльшую сумму, а затем требует вернуть ему разницу. После возвращения переплаченной суммы, мошенник отзывает свой первоначальный платеж.