Вести общение с покупателями (продавцами) только во внутреннем чате торговой площадки
(часто торговые площадки блокируют возможность перехода на поддельные ресурсы).

Общаясь с пользователем, перейти к его профилю и обратить внимание на дату его создания
(если он создан несколько дней назад, то это должно вызвать дополнительную настороженность).

Очень внимательно относиться к любому случаю, когда необходимо ввести данные карты или информацию, предоставленную банком
(смс-код, логин или пароль от интернет-банкинга).

Самый надежный способ уберечь свои средства – это **НИКОМУ НЕ СООБЩАТЬ реквизиты своей карты.**

ИСПОЛЬЗОВАТЬ ОТДЕЛЬНУЮ БАНКОВСКУЮ КАРТУ
для осуществления покупок в сети Интернет, на которой не хранятся денежные средства и на которую не поступает регулярный доход в виде заработной платы, стипендии или пенсии.

Для того чтобы не стать жертвой киберпреступников,

совершая сделки в сети Интернет, следует

ИЗБЕГАТЬ ПЕРЕХОДА ПО НЕИЗВЕСТНЫМ ИНТЕРНЕТ-ССЫЛКАМ,

которые предоставляются в ходе переписки якобы для получения предоплаты или оформления доставки.

Если Вы все же перешли по подобной ссылке и видите уведомление о том, что в системе имеется денежный перевод и для его получения необходимо ввести данные банковской платежной карты,

НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ НЕ ВВОДИТЕ ЗАПРАШИВАЕМЫЕ СВЕДЕНИЯ,

так как это прямой путь к утрате собственных средств.

Если Вы все же ввели данные своей банковской карты на поддельном ресурсе или сообщили их постороннему лицу, необходимо
СРОЧНО ПРОИЗВЕСТИ БЛОКИРОВКУ КАРТЫ,
позвонив в банк.

СТОПОБМАН

ВАШ УЧАСТКОВЫЙ УПОЛНОМОЧЕННЫЙ ПОЛИЦИИ

_____

_____

_____

_____

Важно помнить!!!!!

по телефону НЕ СООБЩАЮТ:

- о выигрыше,
- махинациях с картой,
- блокировке карты,
- вирусной атаке,
- случайно переведенных деньгах.

Даже если Вам называют все Ваши данные:
дату рождения,
номер карты,
регистрацию по месту жительства,
место работы и т.д.

ЭТИ ДАННЫЕ МОШЕННИКИ УКРАЛИ

из какой-либо базы данных.

Самая лучшая
ЗАЩИТА ОТ МОШЕННИКОВ –

НЕ ОТВЕЧАТЬ
на звонки
с незнакомых номеров.

ПРОВЕРЯТЬ ИНФОРМАЦИЮ
у самих родственников
или по горячей линии банка
(телефон указан на карте).

Если Вам звонят с неизвестного номера, или пришло сообщение с неизвестного номера

ТЕКСТ СООБЩЕНИЯ

вирусная атака

с Вашего счета пытаются снять деньги

просьба помочь
(от кого-то из близких)

просьба перечислить деньги

выигрыш

карта заблокирована

на Ваш счет случайно
перевели деньги

ВАШИ ДЕЙСТВИЯ:

не вступать в разговоры;

прекратить разговор и отсоединиться от собеседника;

перезвонить родственнику, который просит о помощи;

позвонить на горячую линию банка (номер указан на карте);

не сообщать никому трехзначный код с карты;

не набирать никаких комбинаций.

ЕСЛИ ВАМ ПОСТУПИЛ ЗВОНОК ИЗ «БАНКА»

ни при каких обстоятельствах,
никому и никогда НЕ СООБЩАЙТЕ
информацию о себе или своей банковской платежной карте.
Настоящим работникам банка известны Ваши данные по карте.

Уточните, с кем именно Вы общаетесь,
после чего положите трубку
и перезвоните на номер
горячей линии банка
(телефон указан на карте).

ЕСЛИ ЖЕ НА ВАС ОКАЗЫВАЕТСЯ ПСИХОЛОГИЧЕСКОЕ ДАВЛЕНИЕ УГРОЗАМИ

о том, что через несколько секунд
Вы понесете финансовые потери,
кто-то оформит на Вас кредит,
или, если Вы не сообщите
требуемую информацию,
то карту вообще заблокируют,

НЕ ВОЛНУЙТЕСЬ,

ЭТО ОБЫЧНАЯ УЛОВКА ПРЕСТУПНИКОВ,

главная цель которых – ввести Вас
в состояние неуверенности и страха
потерять сбережения.

СТОПОБМАН

ЕСЛИ ВАМ ЗВОНЯТ С НЕИЗВЕСТНОГО НОМЕРА, ИЛИ ПРИШЛО СООБЩЕНИЕ С НЕИЗВЕСТНОГО НОМЕРА

ТЕКСТ СООБЩЕНИЯ

вирусная атака

с Вашего счета пытаются снять деньги

просьба помочь (от кого-то из близких)

просьба перечислить деньги

выигрыш

карта заблокирована

на Ваш счет случайно перевели деньги

ВАШИ ДЕЙСТВИЯ:

НЕ ВСТУПАТЬ В РАЗГОВОРЫ;

ПРЕКРАТИТЬ РАЗГОВОР И ОТСОЕДИНИТЬСЯ ОТ СОБЕСЕДНИКА;

ПЕРЕЗВОНИТЬ РОДСТВЕННИКУ, КОТОРЫЙ ПРОСИТ О ПОМОЩИ;

ПОЗВОНИТЬ НА ГОРЯЧУЮ ЛИНИЮ БАНКА (НОМЕР УКАЗАН НА КАРТЕ);

НЕ СООБЩАТЬ НИКОМУ ТРЕХЗНАЧНЫЙ КОД С КАРТЫ;

НЕ НАБИРАТЬ НИКАКИХ КОМБИНАЦИЙ.

ЕСЛИ ВАМ ПОСТУПИЛ ЗВОНОК ИЗ «БАНКА»

ни при каких обстоятельствах,

никому и никогда НЕ СООБЩАЙТЕ

информацию о себе или своей банковской платежной карте. Настоящим работникам банка известны Ваши данные по карте.

Уточните, с кем именно Вы общаетесь, после чего положите трубку и перезвоните на номер горячей линии банка (телефон указан на карте).

Самая лучшая ЗАЩИТА ОТ МОШЕННИКОВ

НЕ ОТВЕЧАТЬ

на звонки с незнакомых номеров

ПРОВЕРЯТЬ ИНФОРМАЦИЮ

у самих родственников или по горячей линии банка (телефон указан на карте)

Важно помнить!!!!! по телефону НЕ СООБЩАЮТ:

о выигрыше,

махинациях с картой,

блокировке карты,

вирусной атаке,

случайно переведенных деньгах.

ЕСЛИ ЖЕ НА ВАС ОКАЗЫВАЕТСЯ ПСИХОЛОГИЧЕСКОЕ ДАВЛЕНИЕ УГРОЗАМИ

о том, что через несколько секунд Вы понесете финансовые потери, кто-то оформит на Вас кредит, или, если Вы не сообщите требуемую информацию, то карту вообще заблокируют,

НЕ ВОЛНУЙТЕСЬ,

ЭТО ОБЫЧНАЯ УЛОВКА ПРЕСТУПНИКОВ,

главная цель которых – ввести Вас в состояние неуверенности и страха потерять сбережения.

Даже если Вам называют все Ваши данные: дату рождения, номер карты, регистрацию по месту жительства, место работы и т.д.

ЭТИ ДАННЫЕ МОШЕННИКИ УКРАЛИ

из какой-либо базы данных.

ДЛЯ ТОГО, ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПНИКОВ, СОВЕРШАЯ СДЕЛКИ В СЕТИ ИНТЕРНЕТ СЛЕДУЕТ

ИЗБЕГАТЬ ПЕРЕХОДА ПО НЕИЗВЕСТНЫМ ИНТЕРНЕТ-ССЫЛКАМ,

которые предоставляются в ходе переписки якобы для получения предоплаты или оформления доставки.

ИСПОЛЬЗОВАТЬ ОТДЕЛЬНУЮ БАНКОВСКУЮ КАРТУ

для осуществления покупок в сети Интернет, на которой не хранятся денежные средства и на которую не поступает регулярный доход в виде заработной платы, стипендии или пенсии

Вести общение с покупателями (продавцами) только во внутреннем чате торговой площадки
(часто торговые площадки блокируют возможность перехода на поддельные ресурсы).

Общаясь с пользователем, перейти к его профилю и обратить внимание на дату его создания
(если он создан несколько дней назад, то это должно вызвать дополнительную настороженность).

Очень внимательно относиться к любому случаю, когда необходимо ввести данные карты или информацию, предоставленную банком
(смс-код, логин или пароль от интернет-банкинга).

Самый надежный способ уберечь свои средства – это

НИКОМУ НЕ СООБЩАТЬ реквизиты своей карты.

Если Вы все же ввели данные своей банковской карты на поддельном ресурсе или сообщили их постороннему лицу, необходимо

СРОЧНО ПРОИЗВЕСТИ БЛОКИРОВКУ КАРТЫ, ПОЗВОНИВ В БАНК.

Если Вы все же перешли по подобной ссылке и видите уведомление о том, что в системе имеется денежный перевод и для его получения необходимо ввести данные банковской платежной карты,

НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ НЕ ВВОДИТЕ ЗАПРАШИВАЕМЫЕ СВЕДЕНИЯ,

так как это прямой путь к утрате собственных средств.

Профилактические меры участкового уполномоченного полиции по предупреждению хищений, совершаемых с использованием IT-технологий

Разъяснительная работа с гражданами:

- о непредоставлении посторонним лицам персональных данных и сведений о банковских картах (номера карты, CVC-кода);
- о недопустимости передавать паспорт другим лицам (в том числе копии);
- о том, как себя вести при получении телефонного звонка (например, от службы безопасности банка, от родственника, который якобы попал в беду и т.д.);
- об их действиях в случае совершения в отношении них преступлений, совершенных с использованием IT-технологий;
- об использовании лицензионных программ для осуществления онлайн-переводов денежных средств, размещенных в PlayMarket, AppStore;
- о том, что в случае поступления якобы ошибочно переведенных денежных средств обратный перевод осуществлять только через сотрудников горячей линии банка;
- о внесении предоплаты за товар только продавцам, заслуживающим доверия, с использованием опции сайта «защищенная сделка»; а также через изучение истории отзывов о товаре;
- о действиях в случае получения в социальных сетях сообщения от знакомого с просьбой одолжить денег.

Предлагать населению приобрести отдельную банковскую карту для онлайн-покупок, на которую переводить небольшие суммы денег.

Распространять среди населения памятки о противодействии мошенничествам с использованием IT-технологий.

Разместить в участковом пункте полиции алгоритм действий при получении сообщения о совершении мошенничества с использованием IT-технологий.