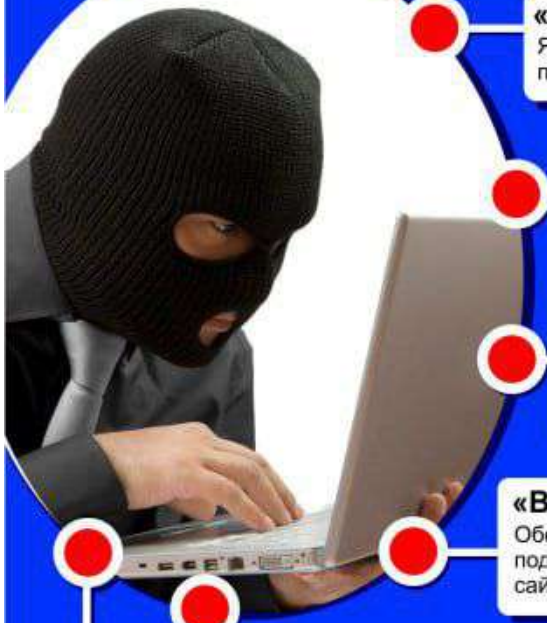
НАИБОЛЕЕ РАСПРОСТРАНЁННЫЕ СХЕМЫ ИНТЕРНЕТ МОШЕННИЧЕСТВА



«ОНЛАЙН ПОКУПКИ»
Якобы продавец просит за товар предоплату либо полную оплату покупки, после чего связь с мошенником прекращается

«МЫ НАШЛИ ВАШИ ДОКУМЕНТЫ»
Якобы нашли ваши утерянные документы и просят вознаграждение за их возврат

«ПРИВЯЗКА КАРТЫ»
Просят привязать вашу банковскую карту к какому-либо номеру телефона или счету

«ВИРУСНАЯ АТАКА»
SMS-сообщение, содержащее ссылку на какой-либо интернет ресурс, содержащая вредоносную программу, дающую доступ мошенникам к вашей банковской карте

«ВЫПЛАТА ПРОЦЕНТОВ»
Обещание больших процентов по вкладам под короткие сроки на различных интернет сайтах

«ПОКУПКА АВИАБИЛЕТОВ»
продажа липовых авиабилетов на мошеннических сайтах

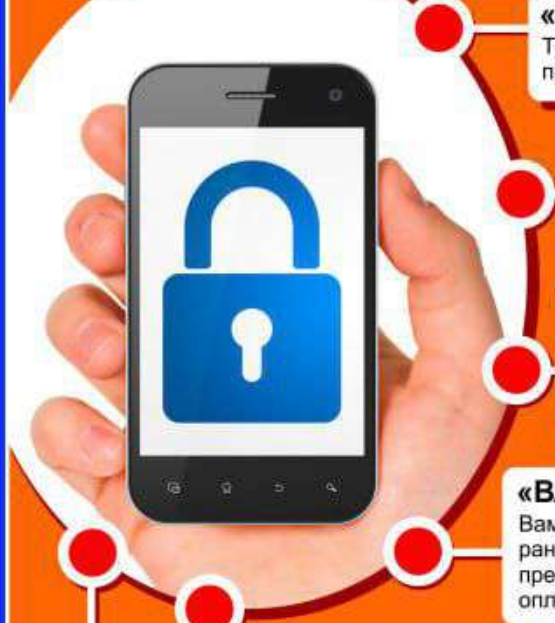
ПРОСЬБА ПЕРЕВЕСТИ КАКУЮ-ЛИБО СУММУ ОТ ВАШЕГО ЗНАКОМОГО, АККАУНТ КОТОРОГО БЫЛ ВЗЛОМАН

ПОМНИТЕ! ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ КИБЕРМОШЕННИКОВ

Помните! Ни в коем случае не привязывайте свою банковскую карту к какому-либо телефону или счету ни под каким предлогом!
Пользуйтесь только проверенными сайтами, на которых решили совершить какие-либо покупки!
Оплачивайте товар только после его получения!

БУДЬТЕ ВНИМАТЕЛЬНЫ И БДИТЕЛЬНЫ!

НАИБОЛЕЕ РАСПРОСТРАНЁННЫЕ СХЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА



«ВАША КАРТА ЗАБЛОКИРОВАНА»
SMS-сообщение о якобы заблокированной банковской карты, для разблокировки которой требуется сообщить ПИН-код вашей карты, либо провести определенные действия с помощью банкомата

«РОДСТВЕННИК В БЕДЕ»
Требование крупной суммы денег для решения проблемы с якобы попавшему в беду родственником

«ВЫ ВЫИГРАЛИ»
SMS-сообщение о том, что вы стали победителем и вам положен приз

«ВИРУСНАЯ АТАКА»
SMS-сообщение, содержащее ссылку на какой-либо интернет ресурс, содержащая вредоносную программу, дающую доступ мошенникам к вашей банковской карте

«ВАМ ПОЛОЖЕНА КОМПЕНСАЦИЯ»
Вам якобы положена компенсация за приобретаемые ранее некачественные БАДы либо иные медицинские препараты, для получения которой вам необходимо оплатить какие-либо пошлины или проценты

«ОШИБОЧНЫЙ ПЕРЕВОД СРЕДСТВ»
просят вернуть деньги за ошибочный перевод средств, дополнительно снимая средства со счета по чеку

УСЛУГА, ЯКОБЫ, ПОЗВОЛЯЮЩАЯ ПОЛУЧИТЬ ДОСТУП К SMS И ЗВОНКАМ ДРУГОГО ЧЕЛОВЕКА

ПОМНИТЕ! ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ ТЕЛЕФОННЫХ МОШЕННИКОВ

Помните! Если вам звонят и тревожным голосом сообщают, что ваш близкий попал в беду, либо вы выиграли приз, либо вам положена какая-либо компенсация, не верьте - это мошенники!
Никогда не проходите по ссылкам присланный в SMS-сообщении с незнакомых номеров!
Никому не сообщайте ПИН-код вашей банковской карты!

БУДЬТЕ ВНИМАТЕЛЬНЫ И БДИТЕЛЬНЫ!

КАК ИЗБЕЖАТЬ ОБМАНА ТЕЛЕФОННЫХ МОШЕННИКОВ

Телефонные мошенники!

Вам звонят из банка под предлогом пресечения несанкционированного списания денежных средств и оформления кредита. Убеждают оформить кредит и перевести деньги на безопасный счет.

- ЧТО ДЕЛАТЬ?

СРАЗУ ПОЛОЖИТЕ ТРУБКУ – ЭТО МОШЕННИКИ!

При необходимости лично посетите отделение банка либо позвоните по телефону, указанному на оборотной стороне банковской карты, а также в правоохранительные органы для получения соответствующих разъяснений

госуслуги

Вам поступил звонок от лица представившегося сотрудником портала «Госуслуг» и сообщает о попытке взлома вашего личного кабинета. Предлагает передать ему сведения в виде логина и пароля для входа в личный кабинет

- ЧТО ДЕЛАТЬ?

СРАЗУ ПОЛОЖИТЕ ТРУБКУ – ЭТО МОШЕННИКИ!

Сотрудники портала «Госуслуг» никогда не просят сообщить им логин и пароль для входа в личный кабинет. При возникновении сомнений смените пароль на более сложный и подключите двухтарифную аунтификацию (для входа использовать одноразовый код)

TeamViewer

AnyDesk

«Специалисты технической поддержки» банка под предлогом пресечения мошеннических действий с вашими денежными средствами предлагают установить на смартфон неизвестное приложение

- ЧТО ДЕЛАТЬ?

СРАЗУ ПОЛОЖИТЕ ТРУБКУ – ЭТО МОШЕННИКИ!

Злоумышленники обычно предлагают установить приложение по удаленному доступу к устройству, после чего получают полный контроль над ним и смогут самостоятельно оформить за вас кредиты с последующим присвоением денежных средств

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

Звонят из банка. Говорят об угрозе вашим деньгам на счете и просят перевести деньги на другой счет. Спрашивают данные карты.

—Что делать?

СРАЗУ ПОЛОЖИТЕ ТРУБКУ— ЭТО МОШЕННИКИ!

Позвоните по телефону, который указан на вашей банковской карте, сотрудник банка прояснит ситуацию.

Звонят и сообщают о выигрышах, выплатах, компенсациях и т.д.

—Что делать?

НЕ ПЕРЕДАВАЙТЕ ДАННЫЕ КАРТЫ!

Если во время разговора вас просят совершить платеж — это мошенники. Положите трубку и, чтобы не сомневаться, уточните информацию на официальном сайте организации, от имени которой звонят.

Звонят и сообщают, что близкий человек попал в беду, просят перевести деньги.

—Что делать?

ПРОЯСНИТЕ СИТУАЦИЮ!

Спросите имя, фамилию звонящего и название организации, которую он представляет. Прекратите разговор и позвоните близкому человеку.
Если дозвониться не удалось, сами найдите телефон организации, от имени которой был звонок, и выясните, что случилось.

ИНТЕРНЕТ

Предлагают вложить деньги на очень выгодных условиях.

—Что делать?

ОТКРОЙТЕ САЙТ WWW.CBR.RU/FINORG

Обо всех финансовых организациях, у которых есть лицензия Банка России, можно узнать на его официальном сайте.

На сайтах с объявлениями («Авито», «Юла» и т.п.) предлагают товары и услуги по заниженным ценам.

—Что делать?

НЕ ВНОСИТЕ ПРЕДОПЛАТУ!

Во время общения с продавцом не сообщайте данные банковской карты, не переходите по ссылкам. Пользуйтесь услугой «Безопасная сделка», которая доступна на сайте с объявлениями.

Нужно перевести деньги или купить билеты. На одном из сайтов условия намного выгоднее, чем на знакомых ресурсах.

—Что делать?

ПОЛЬЗУЙТЕСЬ ТОЛЬКО ПРОВЕРЕННЫМИ САЙТАМИ!

Безопасный сайт должен иметь надпись https:// и «замочек» в адресной строке браузера.