ОСТОРОЖНО: МОШЕННИКИ!

НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

ИНТЕРНЕТ-МОШЕННИКИ

ОБЪЯВЛЕНИЕ О ПРОДАЖЕ

Мошенники-продавцы просят перечислить деньги за товар, который впоследствии жертва не получает.

ситуация 2

ОБЪЯВЛЕНИЕ О ПОКУПКЕ

Мошенники-покупатели спрашивают реквизиты банковской карты и (или) смс-код якобы для перечисления денег за товар, после чего похищают деньги с банковского счета.

ситуация 4

СООБЩЕНИЯ ОТ ДРУЗЕЙ

Мошенник пользуется чужой страничкой в социальной сети в Интернете, и под видом друга (родственника) просит перечислить ему деньги или сообщить данные Вашей карты якобы для перечисления Вам денег под различными предлогами.

ситуация 6

ТЕЛЕФОННЫЕ МОШЕННИКИ

ЗВОНОК О НЕСЧАСТНОМ СЛУЧАЕ

Мошенники звонят жертве от лица близкого человека или от представителя власти и выманивают деньги.

Мама, я попал в аварию!

ситуация 7

БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ

Сообщение о блокировании банковской карты с номером, по которому нужно позвонить. Цель – узнать личный код банковской карты.

ситуация 1

ПОЛУЧЕНИЕ ВЫИГРЫША (компенсации за потерянный вклад)

ситуация 3

Мошенники сообщают о выигрыше приза, возможности получения компенсации за потерянный вклад в «финансовую пирамиду» и т.п. Жертве можно забрать его, заплатив налог или плату якобы «за сохранность денег».

ВИРУС В ТЕЛЕФОНЕ

Мошенники запускают вирус в телефон, предлагая пройти по «зараженной ссылке» (в том числе и от имени друзей). С помощью вируса получают доступ к банковской карте, привязанной к телефону. Установите антивирус и не проходите по сомнительным ссылкам.

ситуация 5

УМВД России по Костромской области

Дежурная часть

397-547

397-647

02

КРУГЛОСУТОЧНО

Интернет-мошенничество - памятка для граждан.

СИТУАЦИЯ 1.

Вы получили смс-сообщение о том, что ваша банковская карта заблокирована?

Никогда не отправляйте никаких денежных средств по координатам, указанным в сообщении, не перезванивайте на номер, с которого оно пришло, и не отправляйте ответных смс.

Самым правильным решением в данной ситуации будет позвонить в банк, выпустивший и обслуживающий вашу карту. Телефон банка вы найдете на обороте вашей карты.

СИТУАЦИЯ 2.

Вы решили купить в интернет-магазине новый мобильный телефон, ноутбук или фотоаппарат по суперпривлекательной цене, но магазин просит перечислить предоплату?

Никогда не перечисляйте деньги на электронные кошельки и счета мобильных телефонов.

Помните о том, что интернет-магазин не может принимать оплату за покупку в такой форме. Если вас просят оплатить товар с использованием терминалов экспресс-оплаты или перевести деньги на электронный кошелек, вероятность того, что вы столкнулись с мошенниками крайне высока.

СИТУАЦИЯ 3.

Вы получили электронное сообщение о том, что вы выиграли автомобиль и вас просят перевести деньги для получения приза?

Никогда не отправляйте деньги незнакомым лицам на их электронные счета.

Помните, что вероятность выиграть приз, не принимая участия в розыгрыше стремится к нулю, а вероятность возврата денег, перечисленных на анонимный электронный кошелек злоумышленников, и того меньше.

СИТУАЦИЯ 4.

Вы решили продать товар и после подачи объявления в ближайшие дни Вам звонит желанный покупатель и говорить что готов оплатить сразу всю сумму за товар, но ему необходимо узнать номер Вашей карты и пароли, которые поступят в смс-сообщении или другие данные с карты?

Никогда никому не сообщайте номер Вашей карты, пароли из смс-сообщений и другие реквизиты карты, иначе с Вашей карты похитят денежные средства. Для перевода денежных средств Вам, покупателю достаточно знать один номер Вашей карты и больше никакие сведения не требуются. Также можно предложить способ оплаты, через платежные переводы в банках на Ваше ФИО, тогда у Вас похитит денежные средства будет невозможно!

СИТУАЦИЯ 5.

Вы получили СМС или ММС сообщение со ссылкой на скачивание открытки, музыки, картинки или программы?

Никогда не переходите по ссылке, указанной в сообщении.

Помните, что перейдя по ссылке вы можете, сами того не подозревая, получить на телефон вирус или оформить подписку на платные услуги.

Даже если сообщение пришло от знакомого вам человека, убедитесь в том, что именно он является отправителем.

СИТУАЦИЯ 6.

Общаетесь в интернете и имеете аккаунты в соцсетях? К Вам обратился знакомый с просьбой одолжить ему денежные средства? Никогда не переводите деньги не связавшись с другом по телефону и не выяснив причину его просьбы, даже если в сообщении он пишет, что не может говорить.

Никогда не размещайте в открытом доступе и не передавайте информацию личного характера, которая может быть использована во вред.

Общение в сети в значительной мере обезличено, и за фотографией профиля может скрываться кто угодно.

Помните о том, что видео и аудиотрансляции, равно как и логин вашей сетевой переписки, могут быть сохранены злоумышленниками и в последствии использованы в противоправных целях.

СИТУАЦИЯ 7.

Вам позвонили на телефон (сотовый или городской) под видом родственника и сказали, что попали в ДТП, в полицию и просят за решение вопроса перечислить денежные средства на карты, телефоны и др. счета?

Помните, что прежде чем расстаться с деньгами, необходимо связаться с родственником под видом, которого звонят злоумышленники и убедиться, что с ним все в порядке. Также можно задать контрольный вопрос якобы родственнику (дата рождения, имя матери, адрес проживания) и злоумышленник сам закончит разговор.

Банк России

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ

КАК ЗАЩИТИТЬСЯ

ОТ ОНЛАЙН-МОШЕННИКОВ

Чтобы добраться до ваших банковских счетов, мошенникам нужны ваши персональные данные и реквизиты карт

Какие схемы используют аферисты?

ОБЕЩАЮТ ЗОЛОТЫЕ ГОРЫ
Опросы за вознаграждение, социальные выплаты или сверхприбыльные инвестиционные проекты. Гарантия быстрого обогащения – признак обмана

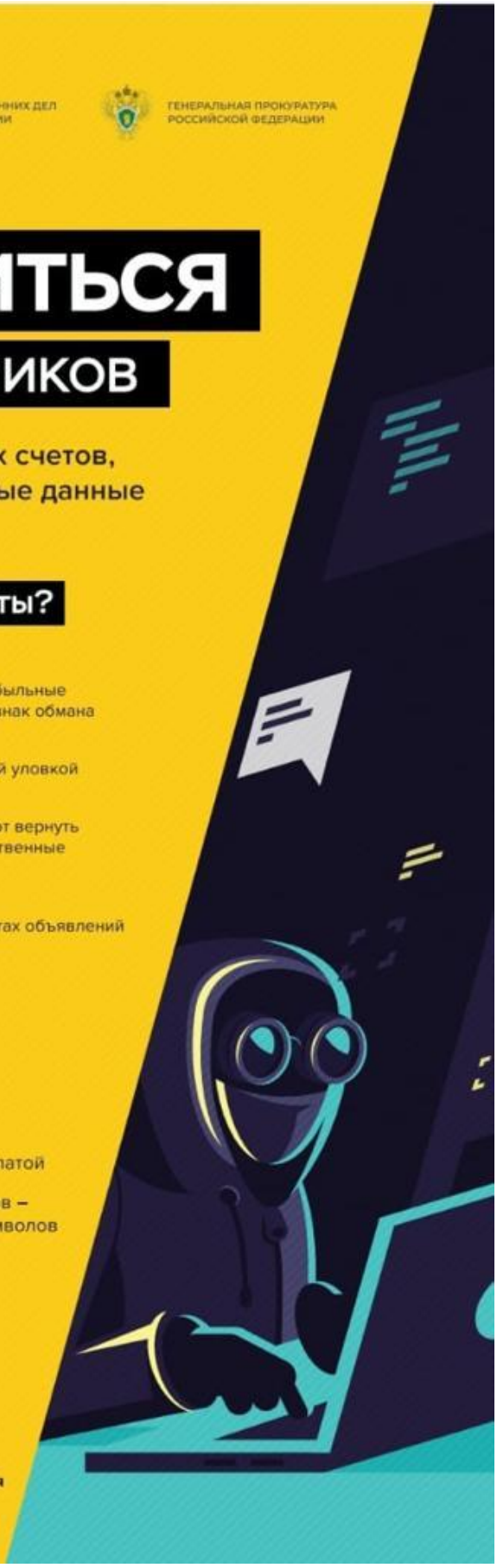
ЗАМАНИВАЮТ НА РАСПРОДАЖИ
Огромные скидки и низкие цены могут оказаться мошеннической уловкой

СПЕКУЛИРУЮТ НА ГРОМКИХ СОБЫТИЯХ
Например, объявляют сбор денег на разработку вакцин, обещают вернуть деньги за отмененные рейсы или предлагают получить государственные дотации

МАСКИРУЮТСЯ
Разыгрывают роль продавцов и покупателей на популярных сайтах объявлений

Как обезопасить свои деньги в интернете?

1. Установите антивирус и регулярно обновляйте его
2. Заведите отдельную дебетовую карту для платежей в интернете и кладите на нее нужную сумму перед оплатой
3. Всегда проверяйте адреса электронной почты и сайтов – они могут отличаться от официальных лишь парой символов
4. Не переходите по ссылкам от незнакомцев – сразу удаляйте сомнительные сообщения
5. Никому не сообщайте свои персональные данные



Подробнее о правилах кибергигиены читайте на fincult.info

Финансовая культура

Банк России

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ

ОСТОРОЖНО: ТЕЛЕФОННЫЕ МОШЕННИКИ!

5 ПРИЗНАКОВ ОБМАНА

1 НА ВАС ВЫХОДЯТ САМИ

Аферисты могут представиться службой безопасности банка, налоговой, прокуратурой

Любой неожиданный звонок, СМС или письмо — повод насторожиться

2 РАДУЮТ ВНЕЗАПНОЙ ВЫГОДОЙ ИЛИ ПУГАЮТ

Сильные эмоции притупляют бдительность

3 НА ВАС ДАВЯТ

Аферисты всегда торопят, чтобы у вас не было времени все обдумать

4 ГОВОРЯТ О ДЕНЬГАХ

Предлагают спасти сбережения, получить компенсацию или вложиться в инвестиционный проект

5 ПРОСЯТ СООБЩИТЬ ДАННЫЕ

Злоумышленников интересуют реквизиты карты, пароли и коды из банковских уведомлений

ВАЖНО!

Сотрудники банков и полиции НИКОГДА не спрашивают реквизиты карты, пароли из СМС, персональные данные и не просят совершать переводы с вашей карты

НИКОГДА НИКОМУ НЕ СООБЩАЙТЕ:

- коды из СМС
- трехзначный код на оборотной стороне карты (CVV/CVC)
- PIN-код
- пароли/логины к банковскому приложению и онлайн-банку
- кодовое слово
- персональные данные

Как защитить свои финансы, читайте на fincult.info

Финансовая культура

Банк России

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ

ЧТО ДЕЛАТЬ, ЕСЛИ С КАРТЫ УКРАЛИ ДЕНЬГИ?

1 ЗАБЛОКИРОВАТЬ КАРТУ

- по номеру телефона банка на банковской карте или на официальном сайте
- через мобильное приложение
- через личный кабинет на официальном сайте банка
- в отделении банка

2 НАПИСАТЬ ЗАЯВЛЕНИЕ О НЕСОГЛАСИИ С ОПЕРАЦИЕЙ

Заявление должно быть написано:

- в течение суток после сообщения о списании денег
- на месте в отделении банка

3 ОБРАТИТЬСЯ В ПОЛИЦИЮ

Чем больше людей подадут заявления, тем выше вероятность, что преступников поймают

КАК ОБЕЗОПАСИТЬ ДЕНЬГИ НА СЧЕТАХ?

НИКОМУ НЕ СООБЩАЙТЕ:

- срок действия карты и трехзначный код на ее оборотной стороне (CVV/CVC)
- пароли и коды из уведомлений
- логин и пароль от онлайн-банка

НЕ ПУБЛИКУЙТЕ

персональные данные в открытом доступе

УСТАНОВИТЕ

антивирусы на все устройства

КОДОВОЕ СЛОВО

называйте только сотруднику банка, когда сами звоните на горячую линию

Банк не компенсирует потери, если вы нарушили правила безопасного использования карты

Подробнее о правилах безопасности читайте на fincult.info

Финансовая культура

ВИШИНГ: НОВЫЙ ВИД МОШЕННИЧЕСТВА НАБИРАЕТ ОБОРОТЫ

ЧТО ТАКОЕ ВИШИНГ?

(англ. vishing — от voice phishing)

Это вид мошенничества, когда аферисты используют телефонную связь, представляются кем-либо (например, сотрудниками банков, сотовых операторов) и выманивают у владельцев банковских карт конфиденциальную информацию.

КАК ЭТОМУ ПРОТИВОСТОЯТЬ?

Вам позвонил сотрудник банка и сказал, что мошенники пытаются похитить ваши деньги? Без паники! Просто:

КЛАДИТЕ ТРУБКУ. Это и есть МОШЕННИКИ!

Незнакомцы просят назвать код из смс-сообщений? Прочитайте внимательно СМС. В СМС написано "НИКОМУ НЕ НАЗЫВАЙТЕ КОД". Не нарушайте это правило, чтобы сохранить свои деньги.

БУДЬТЕ УМНЕЕ АФЕРИСТОВ!

МВД России

ОСТОРОЖНО МОШЕННИКИ

3 МИНУТЫ ОБЩЕНИЯ
КРЕДИТ НА ВСЮ ЖИЗНЬ!

НЕ СОГЛАШАЙТЕСЬ!
НИ НА ЧТО! НЕ НАЗЫВАЙТЕ ДАННЫЕ
НЕ БЕРИТЕ КРЕДИТЫ, НИКАКИХ
ДЕЙСТВИЙ НЕ ВЫПОЛНЯЙТЕ!

НЕ ВЕРЬТЕ!
ПОХОЖИМ НА БЛИЗКИХ
ГОЛОСАМ! КРИКАМ И
ПРОСЬБАМ О ПОМОЩИ

НЕ ПАНИКУЙТЕ!
СРАЗУ ЖЕ СБРОСЬТЕ ЗВОНОК!
И ПОЗВОНИТЕ СВОИМ БЛИЗКИМ!

НЕ ОТКРЫВАЙТЕ!
ДВЕРЬ И НЕ ВПУСКАЙТЕ В ДОМ
НЕ ПОД КАКИМ ПРЕДЛОГОМ!

ЧТО ДЕЛАТЬ

- СБРОСИТЬ ЗВОНОК
- ПОЗВОНИТЬ БЛИЗКОМУ
- ПОЗВОНИТЬ В ПОЛИЦИЮ

РАССКАЖИ БЛИЗКОМУ

МВД России

ОСТОРОЖНО МОШЕННИКИ

3 МИНУТЫ ОБЩЕНИЯ КРЕДИТ НА ВСЮ ЖИЗНЬ!

РОДСТВЕННИК ПОПАЛ В БЕДУ!

Вам звонит родственник и тревожным голосом просит уладить вопрос с полициейза крупную сумму денег

НЕ ПАНИКУЙТЕ! СБРОСЬТЕ ЗВОНОК!
Перезвоните своим близким сами или в полицию!

ПОЗВОНИЛИ ИЗ «СЛУЖБЫ БЕЗОПАСНОСТИ» БАНКА

И сообщают что ваши деньги в опасности и нужно их перевести на «безопасный счет»

СБРОСЬТЕ ЗВОНОК!
Служба безопасности никогда не звонит!

СОБРАЛИСЬ КУПИТЬ ПРОДАТЬ ЧТО-ТО НА АВИТО ИЛИ ЮЛЕ

НЕ ПЕРЕХОДИТЕ В VIBER, WHATS APP И ПО ССЫЛКАМ!
Будьте осторожны это мошенники, не вводите нигде данные своей карты

ПОЗВОНИЛИ ИЗ «БАНКА» ИЛИ СОТРУДНИКИ «ПОЛИЦИИ»

Говорят что на вас берут кредит сторонние люди или просят о помощи в задержании преступника и просят взять кредит вас

СБРОСЬТЕ ЗВОНОК!
Сами позвоните в банк по номеру, указанному на карте, близким или полицию

МВД России

НЕ УВЕРЕН? ЗВОНИ БЛИЗКИМ ИЛИ В ПОЛИЦИЮ!

ТЕЛЕФОН: 02 ИЛИ 102

3 МИНУТЫ ОБЩЕНИЯ С МОШЕННИКОМ - КРЕДИТ НА ВСЮ ЖИЗНЬ!

РОДСТВЕННИК ПОПАЛ В БЕДУ!

Вам звонит родственник и тревожным голосом просит уладить вопрос с полицией за крупную сумму денег

НЕ ПАНИКУЙТЕ! СБРОСЬТЕ ЗВОНОК!
Перезвоните своим близким сами или в полицию!

ПОЗВОНИЛИ ИЗ «СЛУЖБЫ БЕЗОПАСНОСТИ» БАНКА

И сообщают что ваши деньги в опасности и нужно их перевести на «безопасный счет»

СБРОСЬТЕ ЗВОНОК!
Служба безопасности никогда не звонит!

ПОЗВОНИЛИ ИЗ «БАНКА» ИЛИ СОТРУДНИКИ «ПОЛИЦИИ»

Говорят что на вас берут кредит сторонние люди или просят о помощи в задержании преступника и просят взять кредит вас

СБРОСЬТЕ ЗВОНОК!
Сами позвоните в банк по номеру, указанному на карте, близким или полицию

СОБРАЛИСЬ КУПИТЬ ПРОДАТЬ ЧТО-ТО НА АВИТО ИЛИ ЮЛЕ

НЕ ПЕРЕХОДИТЕ В VIBER, WHATS APP И ПО ССЫЛКАМ!
Будьте осторожны это мошенники, не вводите нигде данные своей карты

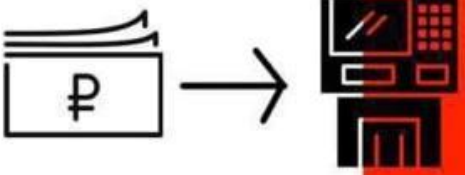
Подробнее на сайте:

И в Teegram-канале “Мы вместе”:

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

ЗВОНЯТ ИЗ БАНКА И СООБЩАЮТ О ПОПЫТКАХ КРАЖИ ДЕНЕГ СО СЧЕТА

ЗВОНЯЩИЙ ПРОСИТ СООБЩИТЬ ИНФОРМАЦИЮ О КАРТЕ



ИЛИ ПЕРЕВЕСТИ ДЕНЬГИ НА «БЕЗОПАСНЫЙ СЧЕТ»

НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

1. НЕ ВЫПОЛНЯЙ НИКАКИХ ТРЕБОВАНИЙ!

2. ЗАВЕРШИ ТЕЛЕФОННЫЙ РАЗГОВОР, ПОЛОЖИ ТРУБКУ!

3. ОБРАТИСЬ В БЛИЖАЙШИЙ ОФИС СВОЕГО БАНКА!