



# Не позволяйте себя обмануть

## Правила безопасности, которые уберегут вас от мошенников

В социальных сетях и мессенджерах активизировались мошенники: новые изобретательные схемы и уловки могут лишить вас не только денег, но и сделать соучастником уголовного преступления.

Будьте бдительны при общении с незнакомыми людьми в соцсетях и мессенджерах, не переходите по подозрительным ссылкам и не скачивайте приложения из неизвестных источников. Никому не сообщайте ваши пин-, CVC- или CVV- коды банковской карты и одноразовые пароли в СМС.

«Анти-террор Урал»

## ПРАВИЛА БЕЗОПАСНОСТИ, КОТОРЫЕ УБЕРЕГУТ ВАС ОТ МОШЕННИКОВ

Как защитить себя от злоумышленников? Рассказываем в деталях о новых схемах и уловках преступников.

Будьте бдительны при общении с незнакомыми людьми, не переходите по подозрительным ссылкам и не скачивайте приложения из неизвестных источников.

Никому не сообщайте ваши пин-, CVC- или CVV-коды банковской карты и одноразовые пароли.

Сообщите о случае мошенничества по номерам:

- 02
- 102
- 112

### НОВЫЕ СХЕМЫ МОШЕННИЧЕСТВА

#### ■ Подработка с целью получения страховых выплат при пожаре

В мессенджерах и социальных сетях жертву убеждают, что за денежное вознаграждение нужно поджечь «заброшенные» офисные здания или автомобили. Деньги обещают выплатить в криптовалюте или переводом после выполнения задания.

Не верьте мошенникам. Помните, что поджог — это уголовное преступление.

### НОВЫЕ СХЕМЫ МОШЕННИЧЕСТВА

#### ■ Продление просроченных документов

Телефонные мошенники сообщают, что срок действия документа истекает, его нужно срочно продлить. Как правило, предлагают «продлить» ОСАГО, СНИЛС, сим-карту, банковскую карту. Таким образом мошенники крадут личные данные и конфиденциальную информацию.

Никому не сообщайте по телефону ваши личные данные.

### ВИРУСЫ

#### ■ Сообщения от имени банка о якобы введении в России сбора денег на нужды спецоперации

Чтобы отменить так называемый «ежемесячный взнос на нужды СВО», гражданину предлагают пройти по ссылке.

При переходе вирус загружается в телефон, и мошенники получают полный доступ к устройству.

### ВИРУСЫ

#### ■ Новый вирус «Мамонт»

Мошенники в мессенджерах и социальных сетях отправляют файл с текстовым сообщением «Это ты на видео?». При открытии такого файла вирус попадает на телефон, и мошенники получают полный доступ к устройству.

Иногда для взлома используют украденные аккаунты в мессенджерах и социальных сетях или копируют фотографию и имя реального человека из интернета.

### ВИРУСЫ

#### ■ Новый вирус Firescat для телефонов на платформе Android

Распространяется через приложение, внешне похожее на мессенджер Telegram, и поддельный магазин приложений, идентичный RuStore.

Опасный вирус крадет платежную информацию, перехватывает СМС и уведомления на телефоне. Так мошенники получают полный доступ к устройству.

### НОВЫЕ СХЕМЫ МОШЕННИЧЕСТВА

#### ■ Мошенники обманывают граждан, ищущих работу и подработку

Аферисты представляются в мессенджерах работодателями известных маркетплейсов и служб доставки. Будущим жертвам предлагают работу и присылают ссылку на вакансию, а затем просят скачать приложение для работы.

При скачивании приложения или переходе по ссылке телефон жертвы взламывают и списывают деньги со счета.

### ЛЖЕБРОКЕРЫ

#### ■ Звонки пожилым гражданам от мнимых сотрудников брокерских компаний

Жертве сообщают о крупных денежных суммах на брокерских счетах и предлагают восстановить к ним доступ через личный кабинет или СМС.

Не сообщайте незнакомым людям СМС-пароли и не переходите по ссылкам.

### ПРИЗНАКИ МОШЕННИЧЕСТВА

Насторожитесь, если вам в мессенджере:

- направляют ссылки и файлы
- просят предоставить личные данные и документы
- требуют сообщить приходящие СМС
- пугают штрафами
- оказывают психологическое давление

# Внимание: участились случаи мошенничества!

**Компания «ЭнергосбыТ Плюс» настоятельно рекомендует соблюдать меры информационной безопасности, чтобы защитить ваши данные и средства**

Обратите внимание на следующие схемы мошенничества:

Поддельное приложение: злоумышленники звонят через мессенджеры, представляются сотрудниками «ЭнергосбыТ Плюс» и предлагают установить поддельное приложение «Энерго+» или похожее на ваш смартфон. Установка этого приложения от-

крывает полный доступ к вашему устройству для мошенников, включая банковские приложения, и делает невозможным удаление программы.

Фальшивые квитанции: мошенники рассылают поддельные счета с ложными QR-кодами, которые могут привести к установке вредоносных программ и компрометации ваших данных.

Чтобы избежать обмана мошенниками, оплачивайте услуги только через Личный кабинет на официальном сайте Компании [www.esplus.ru](http://www.esplus.ru) или в приложении «ЭнергосбыТ+», доступном исключи-

тельно в Google Play, AppStore и RuStore. Помните, что сотрудники «ЭнергосбыТ Плюс» никогда не запрашивают данные банковских карт, пароли или СМС-коды, а также не звонят через мессенджеры (WhatsApp, Viber, Telegram). Официальные звонки поступают только через телефон.

Если вам предлагают установить поддельное приложение через сторонние ссылки, прервите разговор и не переходите по таким ссылкам.

Поделитесь данной информацией с родными и близкими!

«Энергосбыт»



**ОСТОРОЖНО:**

**МОШЕННИКИ**