ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

начинается с вас

КОНФИДЕНЦИАЛЬНОСТЬ

Не пересылайте конфиденциальную информацию (номер банковской карты, ПИН-код, паспортные данные) через мессенджеры социальных сетей

СПАМ

Не переходите по ссылкам в сообщениях от незнакомых людей. Да и от знакомых проверять тоже нужно

ЗАШИФРОВАННОЕ СОЕДИНЕНИЕ

Страницы ввода конфиденциальной информации любого серьезного сервиса всегда защищены, а данные перемещаются в зашифрованном виде. Адрес сайта должен начинаться с «https://», рядом с которым нарисован замок зеленого цвета

сертификационный центр

АДРЕС СТРАНИЦЫ

Обращайте внимание на адрес страницы, где вы оказались. Если он отличается хотя бы на один символ, например ca-kk.info вместо ca-kk.ru, введите его вручную самостоятельно

СЛОЖНЫЕ ПАРОЛИ

Придумайте сложные пароли, не менее 8 символов и используйте специальные символы, цифры, буквы разных регистров. Используйте различные пароли на различных ресурсах, регулярно меняте их

ДОВЕРЕННЫЕ СЕТИ

Не доверяйте непроверенным Wi-Fi соединениям, которые не запрашивают пароль. Чаще всего именно такие сети злоумышленники используют для вовровства личных данных пользователей

ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ

В СИТУАЦИИ, КОГДА ЕСТЬ ПОДОЗРЕНИЕ ИЛИ ДОКАЗАТЕЛЬСТВА ФАКТА МОШЕННИЧЕСТВА, НЕОБХОДИМО НАПИСАТЬ ЗАЯВЛЕНИЕ В ПРАВООХРАНИТЕЛЬНЫЕ ОРГАНЫ.

В 2024 году свыше 200 млн рублей не попали в лапы мошенников. Граждане вовремя одумались и не стали переводить деньги аферистам. Некоторых «счастливчиков» остановили сотрудники банка или полицейские, заподозрившие сомнительные операции.

Кому-то помогли неравнодушные граждане, вовремя проходившие мимо банкомата и обратившие внимание на тревожного человека, постоянно с кем-то говорящего по телефону.

ЕСЛИ МОШЕННИКИ КАКИМ-ЛИБО СПОСОБОМ ВЫНУДЯТ ВАС ПЕРЕВЕСТИ ИМ ДЕНЬГИ, ВЕРНУТЬ ИХ БУДЕТ КРАЙНЕ СЛОЖНО. ТАК ЧТО БУДЬТЕ НАЧЕКУ!

3 миллиона рублей — самая большая сумма в этом году, которую пытались выманить аферисты у пенсионерки под предлогом спасения родственника, «попавшего в ДТП».

МЫ ПРИЗЫВАЕМ ВАС ОСТАВАТЬСЯ БДИТЕЛЬНЫМИ:

- ✔ Если ваш родственник виноват в ДТП — он ответит по закону!
- ✔ Полицейские не просят принять участие в изобличении группы мошенников, взявших по доверенности кредит на ваше имя! Они справятся сами!
- ✔ Сотрудники банка не требуют перевода денег на безопасный счет!
- ✔ Начальник вряд ли попросит вас взять кредит!
- ✔ Не устанавливайте никакие приложения по требованию звонящих «специалистов»!
- ✔ Не называйте никому свои персональные данные, а также поступившие по СМС коды, кем бы незнакомец не представлялся!

КРАСНОЯРСКИЙ КРАЙ
МИНИСТЕРСТВО ФИНАНСОВ

КРАСНОЯРСКИЙ КРАЙ
АГЕНТСТВО ПЕЧАТИ И МАССОВЫХ КОММУНИКАЦИЙ

БЕРЕГИСЬ МОШЕННИКОВ!

ЧТО ДЕЛАТЬ?

ПОМНИТЕ! У МОШЕННИКОВ МНОГО ЛИЦ И СОТНИ ОБРАЗОВ, А ЦЕЛЬ ТОЛЬКО ОДНА — ВЫМАНИТЬ ВАШИ ДЕНЬГИ!

ВАМ ПОЗВОНИЛИ С НЕЗНАКОМОГО НОМЕРА И ПОЧТИ СРАЗУ ОТКЛЮЧИЛИСЬ

Чаще всего это происходит с целью заставить вас выполнить обратный звонок. Нередко на том конце провода могут быть рекламные менеджеры, которые хотят навязать вам покупку, а могут быть и мошенники.

Сотрудниками полиции постоянно ведется работа по выявлению способов мошеннических схем.

Приводим самые распространенные сценарии, которые используют злоумышленники.

Схема 1 ОПЕРАТОРЫ СОТОВОЙ СВЯЗИ

«Действие вашей сим-карты заканчивается», «Какой у вас оператор связи?», «Продиктуйте код из СМС».

Схема 2 ПРЕДЛОЖЕНИЯ ОТ ЛЖЕБРОКЕРОВ

«Откроем брокерский счет для получения прибыли», «Оплатите страховой взнос за инвестиции», «Продиктуйте свои данные для регистрации в нашей брокерской компании».

Схема 3 ЗВОНКИ И СООБЩЕНИЯ ИЗ БАНКА

«На вас кто-то прямо сейчас оформляет кредит», «Прямо сейчас у вас списываются деньги», «Замечаем в последние дни странные операции по вашей карте», «Вам надо опередить мошенников и спрятать свои средства на безопасном счете».

Схема 4 ЗВОНКИ ИЛИ СООБЩЕНИЯ ОТ ЗНАКОМЫХ

«Я в беде, связи нет, говорить не могу, нужны деньги», «Проголосуйте за мою племяшку вот по этой ссылке», «Посмотри хороший материал — пройди по ссылке».

Схема 5 ОПЛАТА УСЛУГ ПО ФЕЙКОВОМУ QR-КОДУ

Человеку предоставляют QR-код с неофициального сайта и предлагают оплатить услугу «через камеру гаджета».

Схема 6 ОБЩЕНИЕ С РАБОТОДАТЕЛЕМ

«Заполните анкету в ходе нашего онлайн-общения», «Укажите данные банковской карты для перечисления будущей зарплаты», «Предоставьте персональные данные для бухгалтерии/кадровика».

Схема 7 ЗВОНКИ И СООБЩЕНИЯ ОТ ГОСУДАРСТВЕННЫХ ВЕДОМСТВ

Вам звонит следователь/дознаватель/судебный пристав/оперативник ФСБ: «На вас заведено уголовное дело», «Продиктуйте ваши данные, я все проверю».

УСЛЫШАЛИ ПО ТЕЛЕФОНУ ТАКИЕ СЛОВА? ПОЛОЖИТЕ ТРУБКУ. СКОРЕЕ ВСЕГО, ВАМ ЗВОНИТ МОШЕННИК!