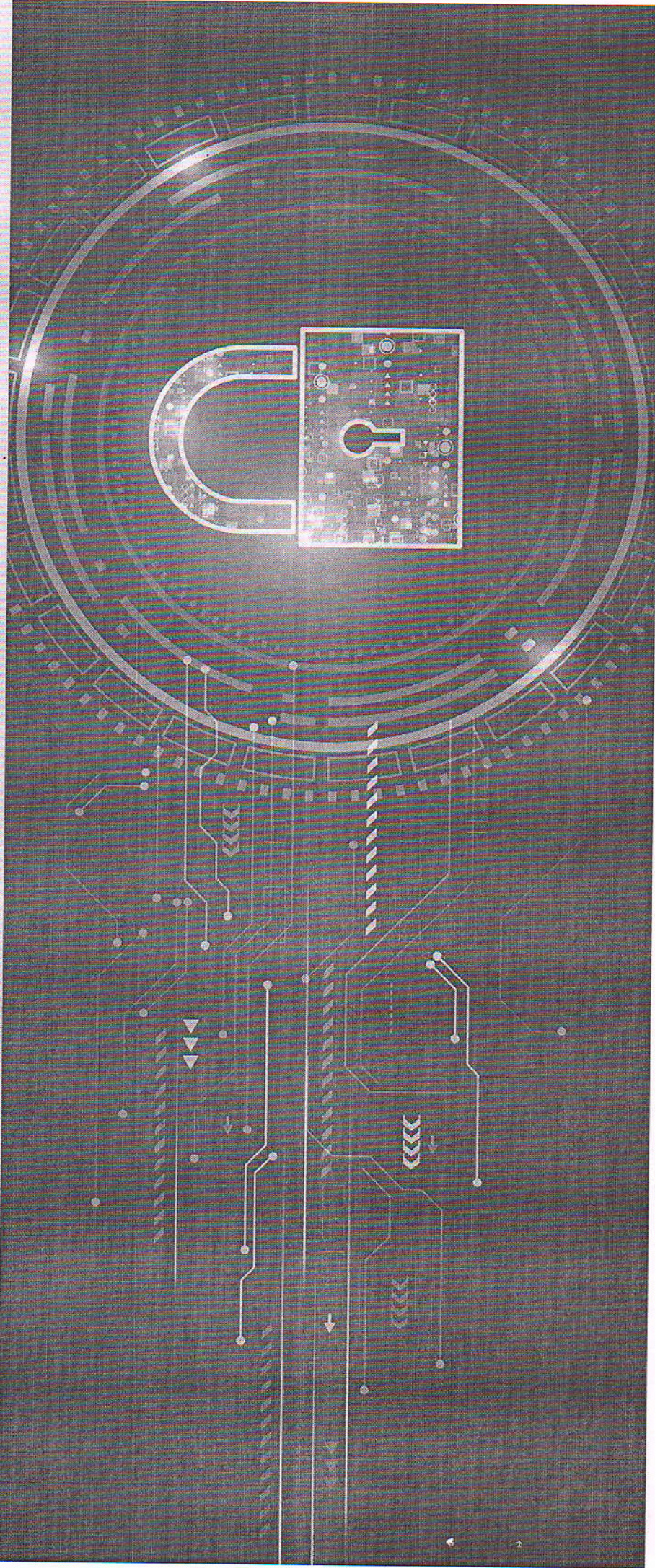
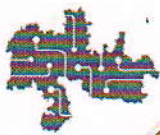




ПАМЯТКА О СПОСОБАХ СОВЕРШЕНИЯ ПРАВОНАРУШЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ И НЕОБХОДИМЫХ МЕРАХ БЕЗОПАСНОСТИ



НОВЫЕ СООБЩЕНИЯ МОШЕННИКОВ



1

Перевод денег на безопасный счет потому что:

- банк под санкциями
- отключение банков от системы SWIFT

2

Требования немедленно погасить несуществующий кредит от лица одного из крупнейших российских банков

3

Предложения от лжеброкеров по инвестиционным инструментам или имитация рекламы известных российских инвестиционных и финансовых компаний

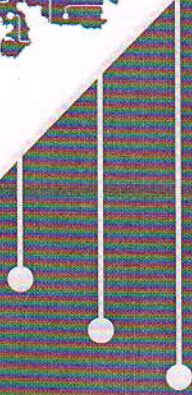
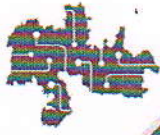
4

Тезисы о поддержке украинской армии и призывы к протестной активности среди матерей российских солдат-срочников

5

Ссылки на зараженные сайты российских компаний с сообщениями о якобы полученных начислениях или выигрыше ценных призов

РАССЫЛКА ПИСЕМ И СООБЩЕНИЙ ОТ ИМЕНИ ОРГАНОВ ВЛАСТИ



КАК ОРГАНИЗОВАНО

Приходит сообщение на эл. почту или в соцсетях от лица российских органов власти:

- предупреждение о незаконности использования запрещенных в России веб-сайтов, соцсетей, мессенджеров и VPN-сервисов;
- информация о новых совыплатах

Приложение к письму: файл RTF

КАК НА САМОМ ДЕЛЕ

При открытии документа скачивается вредоносный файл

Активируется скрипт, с помощью которого мошенник получает удаленный доступ к данным вашего устройства

Мошенник переводит денежные средства с банковских счетов или копирует персональную информацию

КАК ПОСТУПИТЬ

Не торопитесь!

Не открывайте файлы и не переходите по ссылкам, особенно в случае призыва к срочным действиям

Проверьте файлы активирисом

Все сомнительные файлы проверяйте антивирусными программами или на сервисах (пример orentip.kaspersky.com)

Проверьте адрес сайта

Проверьте написание адресов сайтов, прежде чем переходить по ним и вводить на них данные

МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ



КАК ОРГАНИЗОВАНО

Приходит сообщение или звонок о том, что банковская карта заблокирована либо идет попытка перевода денежных средств

Предлагается совместно с банком уточнить детали, чтобы предотвратить блокировку карты или перевод средств.

Мошенники по телефону просят сообщить номер карты/счета, свс-код с оборота карты, сумму средств на счете, код из смс

КАК НА САМОМ ДЕЛЕ

После сообщения номера карты или счета, свс-кода или кода из смс злоумышленники снимают деньги с вашего счета

КАК ПОСТУПИТЬ

Не торопитесь!

Не сообщайте реквизиты вашей карты (никто не вправе требовать данные карты)

Проверьте информацию

Чтобы проверить информацию о блокировании или списании с карты, позвоните в службу поддержки банка

Номер телефона службы поддержки банка указан на обороте карты, мобильном приложении или официальном сайте

ОПЛАТА В ПОДДЕЛЬНОМ ИНТЕРНЕТ-МАГАЗИНЕ



КАК ОРГАНИЗОВАНО

- Злоумышленники создают фальшивый интернет-магазин
- Пользователей привлекают на сайт низкие цены, дефицитные товары и услуги
- Человек оформляет заказ
Спойлер: но не получает желаемый товар или услугу

КАК НА САМОМ ДЕЛЕ

- Поддельные сайты копируют дизайн оригинального сайта и агрессивно продвигаются на онлайн-сервисах
- Человек вводит данные банковской карты
- Информация попадает злоумышленникам
- Деньги будут украдены

КАК ПОСТУПИТЬ

- Совершайте покупки только в проверенных интернет-магазинах
- Будьте внимательны при оплате
- Проверяйте, чтобы окно ввода данных карты было открыто в защищенном режиме
- На защищенный режим указывают замок в адресной строке, <https> в адресе

ОБМАН ПО ТЕЛЕФОНУ: ТРЕБОВАНИЕ ВЫКУПА



КАК ОРГАНИЗОВАНО

- Поступает звонок с незнакомого номера
- Мошенник представляется знакомым, сообщает, что задержан полицией и обвинён в преступлении
- В разговор вступает якобы сотрудник полиции. Сообщает, для решения вопроса нужна не раз помогал людям. Для решения вопроса нужна определенная сумма денег

КАК НА САМОМ ДЕЛЕ

- В организации обмана участвуют несколько преступников.
- Ваш номер набран наугад, фраза мошенника - заготовлена, его действия – по обстоятельствам
- Если жертва поддалась на обман ей называют адрес, куда приехать, или счет для перевода денег. Запугивают до получения денег

КАК ПОСТУПИТЬ

Прервите разговор

Позвоните тому, в ком идет речь.

Если телефон отключён - свяжитесь с его коллегами, друзьями, уточните информацию

Незнакомец требует деньги – мошенник

Задайте уточняющие вопросы «знакомому»

Примеры вопросов: Как я выгляжу? Когда мы виделись последний раз?

Уточните у полицейского номер отделения.

После наберите «02», узнайте у дежурного, действительно ли ваш родственник задержан

SMS-ПРОСЬБА О ПОМОЩИ



КАК ОРГАНИЗОВАНО

Абонент получает смс: «У меня проблемы, кинь 900 рублей на этот номер. Мне не звони, перезвоню сам»

Нередко добавляется обращение «мама», «друг» или другие

КАК НА САМОМ ДЕЛЕ

В роли вымышленного друга или родственника выступает мошенник

В зоне особого риска: пожилые или слишком юные владельцы телефонов

КАК ПОСТУПИТЬ

Проинформируйте близких

Пожилым людям, детям и подросткам следует объяснить, что на SMS с незнакомых номеров реагировать нельзя, это могут быть мошенники

ТЕЛЕФОННЫЙ НОМЕР-ГРАБИТЕЛЬ



КАК ОРГАНИЗОВАНО

- Приходит SMS с просьбой перезвонить на указанный номер телефона
- Просьба обоснована разными причинами – помощь другу, изменение тарифов связи, проблемы со связью и др.
- После того, как вы перезваниваете, вас долго держат на линии. Когда это надоедает, вы отключаетесь. Со счёта списываются крупные суммы

КАК НА САМОМ ДЕЛЕ

- Существуют сервисы с платным звонком. Например, для развлечения. Плата взимается дополнительно за сам звонок
- Мошенники регистрируют сервис и распространяют номер без предупреждения о снятии платы за звонок

КАК ПОСТУПИТЬ

- Не звоните по незнакомым номерам
- Это единственный способ обезопасить себя от телефонных мошенников

ТЕЛЕФОННЫЕ ВИРУСЫ



КАК ОРГАНИЗОВАНО

- В смс или в соцсетях приходит сообщение: «Вам направлена информация. Для получения пройдите по ссылке...»
- При переходе по адресу на телефон скачивается вирус и происходит списание денежных средств с вашего счета
- С вашего номера рассылаются подобные сообщения по адресной книге

КАК ПОСТУПИТЬ

- **Не переходите по незнакомым ссылкам**
Не переходите по ссылкам даже, если номер знакомый (его могли взломать)
- **Пользуйтесь официальными источниками**
Для скачивания приложений используйте только официальные источники
- **Проверьте настройки приложений в телефоне**
Не давайте лишних разрешений приложениям в настройках телефона

ВЫИГРЫШ В ЛОТЕРЕЕ



КАК ОРГАНИЗОВАНО

- На телефон приходит сообщение или звонок от якобы ведущего популярной радиостанции
- Ведущий поздравляет вас с крупным выигрышем в лотерее (телефон, ноутбук, автомобиль и др.)
- Чтобы получить приз просят представиться, назвать год рождения, данные карты и просят сообщить код из SMS для подтверждения выигрыша

КАК НА САМОМ ДЕЛЕ

- Полученной информации о ФИО, банковской карте достаточно, чтобы мошенники списали деньги с вашего счета.
- Код из SMS-сообщения нужен для подтверждения списания денежных средств

КАК ПОСТУПИТЬ

- Прекратите общение
- Игнорируйте сообщения с такой тематикой