

ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВУ И КИБЕРПРЕСТУПЛЕНИЯМ



ПРИЁМЫ ВОЗДЕЙСТВИЙ



ДОВЕРИТЕЛЬНОЕ ОБРАЩЕНИЕ

ПО ИМЕНИ И ОТЧЕСТВУ



СРОЧНОСТЬ

«НУЖНО ПРЯМО СЕЙЧАС»



СТРАХ ПОТЕРИ

ДЕНЕГ, СВОБОДЫ, БЛИЗКИХ



ЗВОНКИ ОТ ЗНАЧИМОГО ЛИЦА

БАНКИ, ПОЛИЦИЯ, ЦБ

КАНАЛЫ И СПОСОБЫ



ВКОНТАКТЕ



MAX



ОДНОКЛАССНИКИ



ТЕЛЕГРАММ



VIBER



WHATSAPP*

* — Соцсеть принадлежит компании Meta, деятельность которой запрещена на территории РФ



**Операторы
сотовой связи**

Выманивание кодов доступа к «Госуслугам» и личным кабинетам под предлогом продления договора или смены тарифа



**НЕ СООБЩАЙТЕ НИКОМУ
ПЕРСОНАЛЬНЫЕ
ДАННЫЕ, ПАРОЛИ,
КОДЫ ИЗ СМС**



**Фейковые
работодатели**

Сбор данных банковских карт и личной информации во время «собеседования»



**НАСТРОЙТЕ
СЛОЖНЫЕ ПАРОЛИ
И ДВУХФАКТОРНУЮ
АУТЕНТИФИКАЦИЮ**

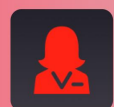


**Поддельные
QR-коды**

Перенаправление на фейковые сайты для кражи денег и данных карты



**НЕ ПЕРЕХОДИТЕ
ПО ПОДОЗРИТЕЛЬ
НЫМ ССЫЛКАМ,
ДАЖЕ ЕСЛИ
ИХ ПРИСЛАЛИ
ЗНАКОМЫЕ**

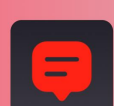


**«Сотрудники»
банка**

Ложные звонки о подозрительных операциях, предложение перевести деньги на «безопасный» счёт



**ПЕРЕЗВОНите В БАНК
ПО ОФИЦИАЛЬНОМУ
НОМЕРУ С САЙТА
ИЛИ НА ОБРАТНОЙ
СТОРОНЕ КАРТЫ**



**Сообщения
от знакомых**

Просьбы о деньгах через взломанные аккаунты или с имитацией голоса с помощью ИИ



**ПОЗВОНите
ЧЕЛОВЕКУ
САМОСТОЯТЕЛЬНО —
НЕ ПЕРЕВОДИТЕ
ДЕНЬГИ
ПО ПЕРЕПИСКЕ**



**«Сотрудники»
госорганов**

Сообщения о выплатах или штрафах с требованием передать данные или «безопасный» счёт



**ИСПОЛЬЗУЙТЕ
ОТДЕЛЬНУЮ
БАНКОВСКУЮ КАРТУ
ДЛЯ ОНЛАЙН-
ПЛАТЕЖЕЙ**

АЛГОРИТМ ДЕЙСТВИЙ ПРИ ПОДОЗРИТЕЛЬНОМ ЗВОНКЕ

1



ПРЕКРАТИТЕ РАЗГОВОР — ПОЛОЖИТЕ ТРУБКУ

2



**ПЕРЕЗВОНите В ОРГАНИЗАЦИЮ
ПО ОФИЦИАЛЬНОМУ НОМЕРУ**

3



**НЕ ВЫПОЛНЯЙТЕ НИКАКИХ ДЕЙСТВИЙ,
ПОКА НЕ ПРОВЕРИТЕ ИНФОРМАЦИЮ**

4



**ЕСЛИ ВЫ УЖЕ СООБЩИЛИ ДАННЫЕ
ИЛИ ПЕРЕВЕЛИ ДЕНЬГИ — СРОЧНО ОБРАТИТЕСЬ
В БАНК ИЛИ ПОЛИЦИЮ**