Как защитить себя от кибермошенничества!

Кибермошенники постоянно совершенствуют методы обмана, используя новые технологии и социальную инженерию (методы манипуляции людьми). Ваша задача — быть в курсе актуальных схем мошенничеств.

Основные схемы кибермошенничества

Мошенничество под видом работников коммунальных служб и государственных органов. Злоумышленники выдают себя за сотрудников коммунальных служб (энергонадзора, водоканала, газовой службы), а также представителей правоохранительных органов, банков или других государственных структур. Они могут звонить по телефону, в том числе по стационарной линии, или использовать мессенджеры (Viber, Telegram, WhatsApp). Цель — под любым предлогом получить личные данные, реквизиты банковских карт или вынудить перевести деньги на «безопасные» счета. Часто работают в паре: один представляется сотрудником коммунальной службы, другой – правоохранительных органов или банка, убеждая жертву, что ее данные скомпрометированы, и для «спасения» средств необходимо оформить кредит или перевести деньги.

Мошенничество с использованием мобильной связи. Мошенники представляются сотрудниками операторов сотовой связи (А1, МТС). Под предлогом окончания срока действия договора или необходимости обновления услуг они убеждают жертву перейти по ссылке из мессенджера и скачать поддельное приложение. Такие приложения дают злоумышленникам полный доступ к данным на смартфоне, включая коды из SMS, логины и пароли к онлайн-банкингу. Важно помнить: безопасное скачивание приложений возможно только из официальных магазинов, таких как Google Play, App Store, App Gallery. Никогда не устанавливайте приложения, переходя по сомнительным ссылкам.

Использование дипфейков и нейросетей. Киберпреступники активно применяют нейросети для создания поддельных голосовых сообщений и видео (дипфейков) с использованием голоса или изображения родственников и знакомых жертвы. Затем такие фальшивые сообщения рассылаются контактам жертвы с просьбами о материальной помощи на лечение или другие нужды, часто с указанием реквизитов банковской карты или просьбой передать деньги через «знакомого».

Психологическое давление и угрозы. Мошенники, выдавая себя за сотрудников правоохранительных органов или даже вашего руководителя, пишут в мессенджерах, сообщая о якобы совершенном вами преступлении или соучастии в нем. Они могут угрожать обыском, изъятием имущества или денежных средств. Для «сохранения» денег предлагают перевести их на «защищенный» счет или передать курьеру, который на самом деле является их пособником. В таких случаях мошенники могут даже «переключать» жертву на подставных «сотрудников» различных ведомств (милиции, Следственного комитета, КГБ, ДФР, КГК).

Финансовые пирамиды и лжеинвестиции. Это одна из наиболее опасных схем. Мошенники, представляясь брокерами или трейдерами торговых площадок, предлагают жертвам быстрый и высокий доход от инвестиций. Они создают фейковые веб-сайты несуществующих бирж с имитацией графиков и диаграмм, регистрируют «личные кабинеты» и демонстрируют «прибыль». Могут даже позволить вывести небольшую сумму, чтобы убедить жертву в реальности заработка. Цель — вынудить человека вложить как можно больше денег, включая заемные средства или деньги от продажи имущества. После получения крупной суммы мошенники исчезают.

Гродненский РОВД

КАК ОТСЕЧЬ ЗВОНКИ МОШЕННИКОВ: ПРОСТАЯ ИНСТРУКЦИЯ

Защитите себя, настроив популярные мессенджеры так, чтобы звонить вам могли ТОЛЬКО люди из вашей телефонной книги. Это займет меньше минуты!

📱 В Viber:
Откройте Viber →
вкладка «Ещё» (внизу справа)→
⚙️ Настройки →
💬 Вызовы и сообщения.
Включите опцию ✅ «Защита от лишних звонков».

📱 В Telegram:
Откройте Telegram → «Настройки» (шестеренка в меню) →
Конфиденциальность → Звонки →
«Кто может звонить мне?».
Выберите вариант «Контакты».

📱 В WhatsApp:
Откройте WhatsApp → вкладка «⋮» (три точки, Android) или «Настройки» (iOS) → Конфиденциальность → Вызовы.
Активируйте опцию «Тихие вызовы от неизвестных».

Помните:

1. Официальные структуры НИКОГДА не запрашивают по телефону коды из СМС, CVV-коды карт, пароли от интернет-банка или предложат установить посторонние программы.
2. Банки НЕ БЛОКИРУЮТ карты, предварительно не уведомив клиента через официальное приложение банка или СМС на короткий номер банка (который всегда одинаков и указан на обороте карты).
3. Любой звонок о проблемах с родственником ТРЕБУЕТ ПЕРЕПРОВЕРКИ. Немедленно положите трубку и самостоятельно позвоните родным или их близким знакомым по известным вам номерам.

Если вы пострадали от мошенничества:

1. Немедленно позвоните в свой банк по официальному номеру (с сайта или оборота карты), чтобы заблокировать карту (если сообщали реквизиты или коды).
2. Позвоните в межбанковскую систему идентификации по короткому номеру – 141! (заблокируют переводы ваших денежных средств).
3. Немедленно сообщите о происшествии в милицию по телефону 102! Чем быстрее вы обратитесь, тем выше шансы задержать преступников.