ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

Согласно статистике, 80% хищений средств происходит дистанционно, более того ежегодно растет не только количество преступлений, но и объем похищенных средств

ПРАВИЛА БЕЗОПАСНОСТИ

- используйте двухфакторную аутентификацию
- храните резервные копии в безопасных местах
- используйте сложные пароли
- желательно использовать отдельное устройство только для доступа к кошелькам
- регулярно обновляйте программное обеспечение
- позаботьтесь о защите своего устройства
- не афишируйте в публичных местах наличие большого количества криптовалюты на ваших кошельках

ПРАВИЛА БЕЗОПАСНОСТИ

- не откликайтесь на вакансии с легким заработком. когда обещается легкий и при этом высокий заработок, то это точно мошенническая схема
- потенциального работодателя проверяйте на предмет наличия отзывов в интернете
- никогда и никому не оставляйте данные своей банковской карты, тем более не передавайте ее третьим лицам (во многих банках передача карт третьим лицам запрещена)
- регулярно обновляйте пароли к своим банковским приложениям, личному кабинету портала «госуслуги» и прочим финансово значимым приложениям
- не переходите по ссылкам из неизвестных источников, во избежание взлома доступа к банковскому личному кабинету
- всегда повышайте свою финансовую грамотность – читайте новости о новых видах мошенничества, ведь «предупрежден – значит вооружен»
- если вас попросят вернуть случайный перевод денег, совершенный на ваше имя, не соглашайтесь на это, обратитесь с этим вопросом в ваш банк

ОСНОВНЫЕ ТИПЫ ПРЕСТУПЛЕНИЙ С КРИПТОВАЛЮТАМИ

МОШЕННИЧЕСТВО

В Управление поступило обращение гражданки «М», денежные средства которой похитили преступники. С использованием одной из социальных сетей с гражданкой «М» связалась девушка, которая, используя методы социальной инженерии убедила «М» приобрести криптовалюту и инвестировать её на бирже «С». В ходе финансового расследования МРУ Росфинмониторинга по СКФО установило, что сайт биржи был подделкой, а криптовалюта, вложенная потерпевшей, выводилась преступниками на одну из известных криптобирж, обменивалась на стэйблкойны и в дальнейшем переводилась на анонимные криптокошельки

ПРОГРАММЫ-ВЫМОГАТЕЛИ (RANSOMWARE)

Одна из крупнейших атак осуществлена на компанию Colonial Pipeline. в 2021 году. Вымогатели потребовали оплату в биткойнах на сумму около 4,4 млн долларов. После получения выкупа преступники пытались скрыть свои средства, разбивая транзакции на мелкие части и переводя их через различные криптовалютные кошельки для запутывания следов

КИБЕРПРЕСТУПЛЕНИЯ И ВЗЛОМЫ

Наиболее известные случаи взлома криптовалютных бирж, такие как взлом Mt. Gox в 2014 году и взлом Bitfinex в 2016 году, привели к огромным потерям.

НАРКОТОРГОВЛЯ И ИНАЯ НЕЛЕГАЛЬНАЯ ТОРГОВЛЯ

В качестве примера можно привести платформу Hydra, деятельность которой была пресечена в 2022 году. По имеющимся данным Hydra контролировала более 90% незаконной торговли в даркнете, где за все товары и услуги, включая наркотики, оружие и поддельные документы, оплачивались криптовалютой

ФИНАНСИРОВАНИЕ ТЕРРОРИЗМА

Криптовалюты также используются для финансирования террористических организаций, так как они позволяют совершать анонимные переводы без необходимости использовать традиционные банковские системы.

ОСНОВНОЕ ПРАВИЛО ФИНАНСОВОЙ БЕЗОПАСНОСТИ ДОСТАТОЧНО ПРОСТОЕ:

НЕ ОТВЕЧАТЬ НА ЗВОНКИ С НЕЗНАКОМЫХ НОМЕРОВ