«Жертву обвиняют в госизмене за денежные переводы в пользу ВСУ, либо звонки от сотрудников правоохранительных органов пытающихся предотвратить незаконное оформление кредита.»

Мошенники звонят клиенту и представляются сотрудниками полиции, следственного комитета, прокуратуры или ФСБ. Сообщают, что сотрудник банка, в котором обслуживается клиент, украл его персональные данные и осуществляет с его счета переводы в пользу армии Украины. А так же ответственность лежит на владельце карты, клиент может быть обвинен в государственной измене, за что ему грозит до 20 лет лишения свободы.

Затем мошенники представляются службой безопасности банка и убеждают клиента переводить деньги на их счета и даже брать кредиты, мотивируя это тем, что так они смогут вычислить преступника внутри банка.

Сотрудники правоохранительных структур никогда не звонят гражданам с целью обезопасить их банковские счета.

«Заработок на различных интернет-площадок (Биржа, Газпроминвестиции и т.д.)»

Граждане самостоятельно, через интернет либо, через звонок осуществляемый злоумышленниками, становятся участниками различных инвестиционных проектов. Их убеждают поучаствовать в выгодных инвестициях и получить огромную прибыль, зарегистрировав аккаунт на электронной торговой площадке (бирже), которая якобы имеет официальный статус, однако является эмулятором. Так же сотрудники организации убеждают гражданина, что будут консультировать его в ходе торгов и говорить, когда совершить покупку или продажу активов, чтобы сделки гарантировано приносили прибыль. В процессе торгов гражданину дают возможность немного заработать и вывести на свой банковский счет, небольшую сумму денег. После чего, с целью получения еще более высоких дивидендов предлагают перевести на подконтрольные счета злоумышленников крупные суммы денег. Когда человек намерен вывести полученную прибыль, ему под различными предлогами отказывают и убеждают совершить еще несколько гарантированно выгодных сделок, в результате которых ничего не подозревающий гражданин, под полным контролем брокеров, совершает заведомо убыточные операции и теряет все накопления с лицевого счета.

При обнаружении в сети интернет рекламы по дополнительному заработку на различных биржевых платформах, знайте это мошенники. Не переходите на данные сайты, чтобы не стать жертвой мошенников.

«Сообщение о взломе Единого портала государственных и муниципальных услуг»

Одним из распространенных способов хищений денежных средств в последнее время является получение несанкционированного доступа к личному кабинету пользователя сервиса «Госуслуги». Жертве поступает звонок от злоумышленника, который представляется оператором службы поддержки Единого портала государственных и муниципальных услуг, где сообщается о том, что произошел неправомерный доступ к личному кабинету, и для предотвращения необходимо сообщить поступающие на телефон гражданина соответствующие коды. При сообщении кодов злоумышленники получают доступ ко всем сервисам портала с аккаунта жертвы и имеют возможность подать заявку на оформление и получения кредита с последующим переводом денежных средств на подконтрольные счета. **Сотрудники Единого портала государственных и муниципальных услуг(Госуслуги) никогда не звонят гражданам с целью несанкционированного доступа к личному кабинету. Согласно инструкции и предоставляемых услуг, пользователь сам осуществляет звонки в службу поддержки портала.**

«Жертве звонят представляясь сотрудниками операторов сотовой связи «Билайн, Теле2, МТС, Мегафон и т.д.».

Мошенники представляясь сотрудниками оператора сотовой связи и сообщают, что необходимо обновить приложение оператора связи или улучшить тарифный план, для этого необходимо скачать программу которая позволит внести вышеуказанные изменения. Для этого предлагается установить на мобильный телефон приложения «RustDesk» и

«Zoom». Приложения «RustDesk» и «Zoom» позволяют мошенникам дистанционно управлять мобильным телефоном жертвы, и открывать приложения «Онлайн банка», с целью хищения денежных средств.

Сотрудники операторов сотовой связи не звонят клиентам с предложениями установить программное обеспечение на телефон. При поступлении таких звонков необходимо отклонить вызов, чтобы не стать жертвой мошенников.