Памятка по профилактике мошенничества в интернете

Мошенники постоянно совершенствуют схемы обмана, чтобы заполучить ваши деньги. Для связи кроме интернет-звонков в мессенджерах, таких как Viber, Telegram или WhatsApp, могут использовать стационарную телефонную и мобильную связь, а также интернет-видеосвязь. Чаще всего они представляются сотрудниками правоохранительных органов, работниками операторов сотовой связи, государственных или банковских организаций, реже – вашим родственником или руководителем, брокером или трейдером криптобиржи.

Правоохранительные органы НИКОГДА:

1. Не привлекают граждан к содействию посредством телефонных переговоров.
2. Не требуют перевода денежных средств с целью их декларирования или проверки на легальность заработка.
3. Не запрашивают конфиденциальные данные, такие как пароли, номера карт или другие личные сведения по телефону.
4. Не требуют немедленной денежной выплаты за «избежание ареста» или «решение проблем».
5. Не отправляют фотографии служебных удостоверений посредством мессенджеров.

Любые телефонные звонки такого рода являются противоправными и направлены на хищение денежных средств!

Наиболее распространенные фразы, используемые мошенниками!

«Ваш аккаунт будет заблокирован, если вы не ответите прямо сейчас».

«Ваши деньги пытаются похитить, зафиксирована подозрительная операция».

«Ваш аккаунт был взломан. Пожалуйста, подтвердите свои данные, чтобы восстановить доступ».

«У нас есть информация о том, что ваши личные данные были украдены. Мы можем помочь вам защититься».

«Пожалуйста, подтвердите свою личность, чтобы избежать блокировки вашего аккаунта».

«Вас беспокоит специалист финансовой безопасности, сотрудник службы безопасности банка».