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».

Правила безопасности, соблюдение которых позволит избежать обмана при совершении онлайн-покупок.

- Не давайте никому логин и пароль от личных кабинетов магазинов и маркетплейсов, банков и так далее.
- Не переходите по внешним ссылкам: заходите на страницу и в личный кабинет только с оригинального сайта компании.
- Общайтесь со службами поддержки только на официальных сайтах или в приложениях.
- Не называйте никому коды по телефону.
- Не сохраняйте для оплаты в личных кабинетах кредитные карты и карты с овердрафтом.
- Заведите отдельную карту для маркетплейсов и вносите на нее сумму, которой хватает только для оплаты самой покупки.
- Если вы сомневаетесь, что вам звонят представители компании, положите трубку и сами позвоните в поддержку магазина по номеру, который указан на сайте.
- Не храните в мессенджере и не выкладывайте в открытый доступ копии документов, удостоверяющих личность.
- Перед оформлением заказа, проверьте отзывы и рейтинг продавца, аккаунт и условия оплаты.
- Подключите двухфакторную аутентификацию для всех своих аккаунтов.

Будьте бдительны и осторожны при любых финансовых операциях в интернете. Если что-то кажется подозрительным, лучше перестраховаться и проверить информацию. Защита ваших денег и данных — это ваша ответственность!

Больше информации в телеграм-канале «КИБЕРКРЕПОСТЬ». Осуществить подписку на телеграм-канал можно с использованием QR-кода, а также путем введения в поисковую строку мессенджера «Telegram» «КИБЕРКРЕПОСТЬ».