

Внимание! Распространенные схемы мошенничества

Фишинговые атаки через мессенджеры и социальные сети:

- Мошенники отправляют сообщения со ссылками, ведущими на сторонние ресурсы. Чтобы воспользоваться интересующей информацией предлагают внести персональные данные - логины, пароли, данные банковской карты.

Использование поддельных сайтов маркетплейсов:

- Создаются копии известных интернет-магазинов. Покупатели переводят деньги за несуществующий товар и не получают заказ.

Звонки от «сотрудников банка»:

- Лжесотрудники банков и правоохранительных органов сообщают о «подозрительных операциях» и предлагают перевести деньги на «безопасный» счет.

Поддельный QR-код:

- Мошенники размещают поддельные QR-коды в различных местах, например, на парковках или квитанциях об оплате услуг, сканирование которых может привести к установке вредоносного программного обеспечения, или утечке персональных данных.

Ложные сообщения о компенсациях и выплатах:

- «Жертве» предлагают компенсацию или социальные выплаты, требуя предварительный платеж «за оформление».

Взлом аккаунтов в социальных сетях и требование выкупа:

- Получив доступ к личным страницам пользователей сети «Интернет», злоумышленники требуют деньги за их восстановление. Однако, выплата денег не гарантирует восстановление доступа к аккаунтам.

Как защитить себя:

- Не переходите по подозрительным ссылкам.
- Проверяйте достоверность информации через официальные источники.
- Прежде, чем приобрести товар, убедитесь, что находитесь на официальном сайте организации путем сличения всех знаков его адреса в браузерной строке.
- Знакомьтесь с отзывами об организации.
- Не сообщайте личные данные незнакомцам, кем бы они не представились.
- Используйте для защиты сложные пароли и двухфакторную аутентификацию.
- Помните, что настоящие работники банков и правоохранительных органов не информируют граждан о финансовых угрозах и не предлагают перевести деньги на «безопасный счет».
- Знайте, социальные организации не требуют предоплату за выплаты.