ЗАЩИТА ОТ КИБЕРУГРОЗ

ВИДЫ КИБЕРУГРОЗ

- Киберпреступление – действия, направленные на кражу данных, обман, сбой работы сервисов.

- Кибератака – действия, направленные на информационную систему, цель которых получить несанкционированный доступ к системам и украсть, изменить или уничтожить данные.

- Кибертерроризм – действия, направленные на дестабилизацию систем, цель которых вызвать страх или панику у населения.

- Кибербезопасность – совокупность методов и приемов по защите компьютеров, серверов, мобильных устройств, приложений и электронных систем от действий злоумышленников

СРЕДСТВА СВЯЗИ МОШЕННИКОВ

- Телефонные звонки с незнакомых номеров.
- «Звонки-призраки». Звонки сбрасываются до того, как был принят вызов, если на них перезвонить – спишутся деньги.

- Письма по электронной почте.
- SMS-сообщения.

- Сообщения в социальных сетях и мессенджерах.

- Вредоносные программы, приложения и расширения.

КАК ДЕЙСТВУЮТ КИБЕРМОШЕННИКИ

Представляются:

- Сотрудниками правоохранительных и государственных органов
- Работниками организаций с подменных номеров
- Специалистами служб безопасности банков
- Руководителями
- Потенциальными покупателями
- Людьми, которые говорят об ошибочном переводе денег; сообщают о попавшем в беду родственнике; уведомляют о выигрыше в лотерею

Просят:

- Сообщить личные данные
- Перевести деньги для решения ситуации (например, на безопасный счет, или чтобы «отмазать»)
- Взять кредит, чтобы защитить ваши средства
- Установить приложения для защиты (через которые передаются сведения мошенникам)
- Перевести деньги для решения ситуации
- Сообщить коды подтверждения

КАК ДЕЙСТВУЮТ КИБЕРМОШЕННИКИ

Работают в команде.

В рамках одной «истории» с жертвой могут связываться несколько «специалистов»: сотрудник банка, правоохранительных органов, специалист из госуслуг.

Используют нейросети.

Для подделки голоса или изображения может использоваться искусственный интеллект.

Используют фишинг.

Вредоносные ссылки маскируются под настоящие.

Используют вирусы.

Это могут быть вложения в виде документов. Также мошенники используют уязвимости устройств (отсутствие антивируса, двухфакторной аутентификации, легкие пароли и т.д.)

Апеллируют к эмоциям. Перегружают информацией. Требуют срочных действий.

ЧТО НЕЛЬЗЯ ПУБЛИКОВАТЬ

- Фото или сканы паспорта, водительского удостоверения, ИНН, СНИЛС, договоров и др.
- Банковские реквизиты, номера карт, пин-коды и др.
- Личный номер, электронную почту, отметки о геолокации, фотографии близких.

! Не верьте мошенникам и сохраняйте спокойствие.

- Не продолжайте разговор.

Не совершайте действий, о которых просят мошенники.

КУДА ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ

Если вам угрожает опасность.

112

Если у вас подозрения об актах мошенничества.

Горячая линия МВД России

8 800 222 74 47

Телефон доверия МВД России по РБ

8 (347) 279-32-92

Если от имени банка запрашивают персональные сведения.

Горячая линия Центробанка РФ для физ. лиц

8 800 300 30 00