«Осторожно мошенники!»

Мобильные телефоны стали для современного общества одним из самых ценных видов имущества, и **киберпреступники** об этом знают. К телефонным номерам привязан учетные записи от банков, электронная почта и другие конфиденциальные данные, что делает их идеальной мишенью для злоумышленников.

Задача мобильного мошенника – вынудить гражданина самостоятельно заразить свое устройство или передать ему конфиденциальную информацию.

К самым популярным видам мобильного мошенничества относятся:

1. **Сообщения о заражении мобильного телефона вредоносной программой.**

При этом виде мошенничества на экране телефонного устройства отображается поддельное сообщение об обнаружении вредоносной программы.

В сообщении говориться, что в ходе сканирования на телефоне было обнаружено вредоносное программное обеспечение и необходимо принять срочные меры.

Гражданину будет предложено загрузить «антивирус», который на самом деле является вредоносной или шпионской программой. После того, как вредоносный код внедриться в телефонное устройство, злоумышленники смогут получить к нему полный доступ или заразить другие устройства. Самый простой способ защититься от подобных атак – установить на телефон антивирусную защиту.

1. **Телефонный вишинг.**

Это вид мошенничества, при котором звонят гражданам, пытаясь побудить к какому-либо действию.

В данных случаях мошенники представляются реальными людьми или компаниями, чтобы завоевать доверие, могут сказать, что работают в реально существующей организации, чтобы убедить гражданина сообщить им свои личные данные или перевести деньги.

Действий от граждан ждут прямо **во время разговора.** Мошенники создают ощущение срочности, вызываю чувства паники, требуют заплатить или раскрыть данные прямо во время звонка, а не просят выполнить какое-то дополнительное действие позднее (по окончании разговора).

1. **SMS-фишинг.**

При SMS-фишинге или «смишинге», мошенники будут привязывать граждан к действию с помощью текстовых сообщений.

В таком сообщении может содержаться вредоносная ссылка, перейдя по которой в телефонное устройство загружается вредоносная или шпионская программа. Иногда мошенники вынуждают граждан совершить другие действия, например перезвонить на платный номер, оформить подписку или выдать личные данные.

1. **Сбрасывающиеся звонки.**

Это вызовы с неизвестных номеров которые **длятся всего пару секунд.**

Делается это для того, чтобы вынудить гражданина перезвонить на этот номер.

Как правило обратный звонок на подозрительный номер будет платным. Иногда мошенники оставляют сообщения в голосовой почте – это повышает шанс того, что гражданин решит перезвонить.

**Будьте бдительны и осторожны, принимая звонки, SMS сообщения или прослушивая голосовую почту с неизвестных номером**

**Азовская межрайонная прокуратура**