**Что такое мобильное мошенничество?**

Мобильные телефоны стали для нас одним из самых ценных видов имущества, и киберпреступники об этом знают. Мы всегда носим их с собой и используем для доступа к важнейшей информации. К нашим телефонам привязаны учетные записи от банков, электронная почта и другие конфиденциальные данные, что делает их идеальной мишенью для злоумышленников.

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

К самым популярным видам мобильного мошенничества относятся:

• Сообщения о заражении мобильного телефона вредоносной программой

• SMS-фишинг («смишинг»)

• Мошенничество с помощью телефонных звонков («вишинг»)

• Сбрасывающиеся звонки

Сообщения о заражении мобильного телефона вредоносной программой

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

Такое могло случаться с вами при просмотре интернет-страниц. В сообщениях обычно говорится, что в ходе сканирования на телефоне было обнаружено вредоносное ПО и вам необходимо принять срочные меры.

Вам будет предложено загрузить «антивирус», который на самом деле является вредоносной или шпионской программой. После того как вредоносный код внедрится в ваш смартфон, злоумышленники смогут получить к нему полный доступ или заразить другие устройства.

Телефонный вишинг

Вишинг – это вид мошенничества, при котором вам звонят, пытаясь побудить вас к какому-либо действию.

Обычно мошенники притворяются реальными людьми или компаниями, чтобы завоевать ваше доверие. Они могут сказать, что работают в реально существующей организации, чтобы убедить вас сообщить им свои личные данные или перевести деньги.

SMS-фишинг

При SMS-фишинге, или «смишинге», злоумышленники будут призывать вас к действию с помощью текстовых сообщений.

В таком сообщении может содержаться вредоносная ссылка, перейдя по которой вы загрузите на свое устройство вредоносную или шпионскую программу. Но иногда злоумышленники вынуждают жертву совершить другие действия, например перезвонить на платный номер, оформить подписку или выдать личные данные.

Сбрасывающиеся звонки

Сбрасывающиеся звонки – это вызовы с неизвестного номера, которые длятся всего пару секунд. Это сделано для того, чтобы вынудить вас перезвонить на этот номер. Как правило, такая схема срабатывает, если ваше любопытство перевешивает критическое мышление. Хитрость в том, что обратный звонок на подозрительный номер будет платным. На этом мошенники и зарабатывают. Обычно эти звонки совершаются с международных номеров, за что с вас и снимают деньги. Иногда мошенники оставляют сообщение в голосовой почте – это повышает шанс того, что вы решите перезвонить. Будьте осторожны, принимая звонки или прослушивая голосовую почту с неизвестного номера.