

Что нужно знать, чтобы не стать жертвой мошенников!

1. «Взлом личного кабинета в Госуслугах».

Мошенники звонят гражданам от имени оператора связи или сотрудника портала «Госуслуги» убеждают гражданина, что действие его sim-карты заканчивается или неизвестные пытаются взломать его личный кабинет и получить кредит используя его учётную запись на портале. Затем выясняют у гражданина пароли, поступающие по СМС от портала «Госуслуги».

2. «Ваша банковская карта заблокирована / прекращение ложной транзакции или оформление онлайн кредита».

Мошенники звонят гражданам используя популярные мессенжеры и от имени службы безопасности и сотрудников полиции или следственного комитета убеждают гражданина, что по его банковской карте произошло несанкционированное списание или неизвестные, пытаются получить кредит. Затем выясняют у гражданина реквизиты банковских карт и пароли, поступающие по СМС либо просят перевести деньги якобы на безопасный счет.

3. «Родственник попал в беду».

Преступники находят потерпевших путем случайного набора абонентских номеров городских телефонов. Затем мошенник представляется потерпевшим от имени родственника, либо сотрудником полиции, сообщая собеседнику заведомо ложную информацию о том, что его родственник (чаще всего это сын, либо внук) совершил преступление и с целью освобождения его от ответственности, просит перечислить на его счет необходимую сумму денег либо передать деньги курьеру.



#КодБезопасности #УловкиЛовки

Что нужно знать, чтобы не стать жертвой мошенников!

1. «Взлом личного кабинета в Госуслугах». Мошенники звонят гражданам от имени оператора связи или сотрудника портала «Госуслуги» убеждают гражданина, что действие его sim-карты заканчивается или неизвестные пытаются взломать его личный кабинет и получить кредит используя его учётную запись на портале. Затем выясняют у гражданина пароли, поступающие по СМС от портала «Госуслуги».

2. «Ваша банковская карта заблокирована / прекращение ложной транзакции или оформление онлайн кредита». Мошенники звонят гражданам используя популярные мессенжеры и от имени службы безопасности и сотрудников полиции или следственного комитета убеждают гражданина, что по его банковской карте произошло несанкционированное списание или неизвестные, пытаются получить кредит. Затем выясняют у гражданина реквизиты банковских карт и пароли, поступающие по СМС либо просят перевести деньги якобы на безопасный счет.

3. «Родственник попал в беду». Преступники находят потерпевших путем случайного набора абонентских номеров городских телефонов. Затем мошенник представляется потерпевшим от имени родственника, либо сотрудником полиции, сообщая собеседнику заведомо ложную информацию о том, что его родственник (чаще всего это сын, либо внук) совершил преступление и с целью освобождения его от ответственности, просит перечислить на его счет необходимую сумму денег либо передать деньги курьеру.



#КодБезопасности #УловкиЛовки