|  |
| --- |
|  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | | |  |  |
|  | | | | |  |
|  | |  | |  |  |
| **На №** |  | | | | |
|  |  | |  | |  |  |

**ИНФОРМАЦИЯ**

для размещения на официальном сайте

**«Как смена номера мобильного телефона может стать ловушкой мошенников».**

Злоумышленники научились получать доступ к личным кабинетам на портале «Госуслуги», банковским счетам, электронной почте через сим-карты, которые ранее принадлежали другим лицам.

Номера мобильных телефонов повторно поступают в продажу в том виде, в каком их оставили прежние владельцы с сохранением привязки к аккаунтам в социальных сетях и различным приложениям. В продажу в салоны сотовой связи такие сим-карты выпускаются операторами мобильной связи через 1-2 месяца после расторжения договора с абонентом – пользователем услуг сотовой связи.

При этом, оператор мобильной связи самостоятельно отключить доступ к таким сведениям не может, а прежний владелец теряет доступ к ним.

В целях получения доступа к персональным данным, злоумышленники пытаются восстановить доступ к различным аккаунтам, в том числе в личном кабинете «Госуслуги», в целях оформления кредитов и микрозаймов от имени жертвы (путем сброса пароля на мобильный телефон, находящийся в пользовании мошенника).

Будьте внимательны при смене номера мобильного телефона! Чтобы не стать жертвой мошенников необходимо следить за актуальностью привязки важных аккаунтов, установить дополнительную защиту (например, уведомление о входе в аккаунт).