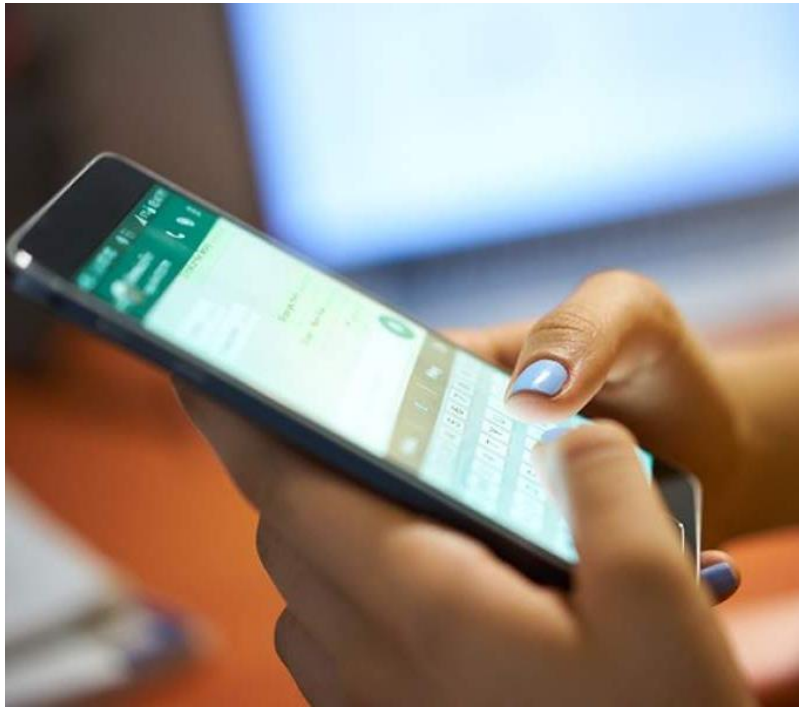
Мошенничество в сети «Интернет». Новые схемы

I. Переадресация звонков и SMS

- Телефонные мошенники в целях получения доступа к данным абонента стали использовать переадресацию звонков и SMS для взлома Госуслуг.
- Мошенническая схема заключается в следующем: на телефоне жертвы удаленно без ее ведома устанавливается переадресация звонков либо пользователь сам установил вредоносное приложение. После этого все звонки и сообщения поступают непосредственно аферистам, которые взламывают аккаунты на «Госуслугах».



II. Имитация разоблачения

- Мошенники усложнили стандартную схему обмана. Сначала они звонят от имени курьеров, делая вид, будто они неопытные аферисты. В последующем они, якобы забыв сбросить вызов, обсуждают план обмана жертвы.
- После этого с жертвой связываются от имени Роскомнадзора либо правоохранительных органов и уже звучат более убедительно. Посредством этого они выманивают настоящий код для входа в онлайн-банк.

III. «Ответы» на ЕГЭ, ОГЭ и госэкзаменах.

- Мошенники создают группы в социальных сетях (ВКонтакте, Телеграм и др.), сайты, где предлагают продажу ответов.
- Под видом файла с ответами они распространяют программу, с помощью которой похищают денежные средства и личные данные.

- Мошенники начали массово обманывать студентов, представляясь сотрудниками деканатов.
- Злоумышленники звонят и утверждают, что срочно нужно закрыть ведомость по госэкзаменам, а затем просят зайти в личный кабинет и продиктовать SMS-код.
- В таком случае жертва может потерять все деньги с банковских счетов.