

ПАМЯТКА

как не стать жертвой киберферистов

Схемы, которые используют киберферисты

- ✓ звонки / звонки в мессенджерах (Телеграм, Вотсап, Вайбер) от лица операторов связи, сотрудников банка, правоохранительных структур, онлайн-портала «Госуслуги»;
- ✓ «безопасный» счет;
- ✓ взлом аккаунтов в социальных сетях и мессенджерах;
- ✓ покупка и продажа товаров на бесплатных сервисах объявлений;
- ✓ лжеброкерство;
- ✓ инвестиции в акции компании.

Как распознать мошенника?

- отвлекает объемом информации – звонящий много говорит, часто сложными и непонятными конструкциями, задает вопросы;
- торопит действовать – не дает времени подумать, подгоняет, просит, как можно скорее назвать код;
- пугает последствиями – звонящий говорит, что все плохо: деньги с карты уходят, счета замораживаются. Он предлагает быстрое решение, которое поможет все исправить.

!!Если вы стали жертвой мошенников, немедленно сообщите об этом в полицию либо по единому номеру 102 или обратитесь с письменным заявлением в ближайшее отделение полиции.

Услышали по телефону такие слова?

- ▼ «неизвестные сейчас оформляют на вас кредит»;
- ▼ «вам надо опередить мошенников и перевести свои средства на безопасный счет»;
- ▼ «вам звонит следователь/дознатель/судебный пристав/оперативник ФСБ»;
- ▼ «на вас заведено уголовное дело...»;
- ▼ «срок действия договора на пользование услугами мобильного оператора истек...».

КЛАДИТЕ ТРУБКУ

!!!При любых подозрительных звонках – КЛАДИТЕ ТРУБКУ!!!

!!! Не доверяйте незнакомцам, предлагающим легкий или быстрый заработок. Если Вам пишет знакомый с просьбой о займе денег, стоит лично перезвонить ему и убедиться, что его аккаунт не взломан неизвестными. Приобретая вещь или услугу, убедитесь, что это не мошенники – оплачивайте товар после получения, покупайте только у проверенного человека, у которого покупали ранее сами или кто-то из знакомых.

!!! В сети Интернет не переходите по ссылкам. Не устанавливайте на свой мобильный телефон неизвестные приложения.