Мошенничество в социальных сетях

Персональные данные – это источник богатства. Ваши предпочтения, любимые места, близкие люди или любые другие подробности о вас являются ценной информацией.

1. Опросы, тесты и конкурсы для сбора данных

Часто можно увидеть призывы пройти платный опрос, по итогам которого нужно оставить данные банковской карты и оплатить комиссию для получения вознаграждения. Это мошенничество.

В «шуточных» тестах также могут использоваться уловки, заставляющие поделиться определенной информацией: датой рождения и местом проживания. Так злоумышленники выманивают информацию о вас и ваших друзьях. Не переходите по ссылке на такие тесты и не делитесь ими.

2. Кликбейт

Злоумышленники тратят много сил на создание ярких заголовков, по которым хочется перейти. Чем больше у злоумышленников ваших данных, тем проще им создать заголовок, который вас привлечет. Если вы на него нажмете, скорее всего, откроется страница входа на сайт через аккаунты в социальных сетях. Если вы введете свои учетные данные, они станут известны мошенникам и те завладеют вашей страницей.

3. Просьбы одолжить денег

Взломав чью-то учетную запись, злоумышленники первым делом пытаются разослать сообщения друзьям жертвы со срочной просьбой одолжить деньги. Получив подобную просьбу в социальных сетях или по электронной почте, всегда уточняйте у знакомого лично, не взломан ли его аккаунт.

4. Подозрительные запросы на добавление в друзья

Получив запрос на добавление в друзья от незнакомца, всегда спрашивайте себя, зачем это ему нужно. Если причина вам непонятна, а страница вызывает подозрения, проигнорируйте подобный запрос.

5. Запросы от людей, которые уже были в списке друзей

На первый взгляд может показаться, что друг создал новую страницу или произошел странный сбой в системе, а потому запрос на «дружбу» можно безбоязненно принять. На деле это прием социальной инженерии, рассчитанный на то, что вы сами добавите мошенника, не подозревая об этом.

6. Сообщения о чрезвычайных ситуациях

Это «срочные» предупреждения от имени ваших друзей или какого-либо сервиса, содержащие якобы срочную и важную информацию о вашей учетной записи.

Например, вы можете получить письмо от вашего банка, в котором говорится, что карта заблокирована из-за подозрительных операций, и для верификации необходимо ввести ее данные (или перейти по ссылке на поддельную страницу интернет-банка и войти в свой аккаунт).

Злоумышленники вводят вас в состояние паники, чтобы вы опрометчиво предоставили доступ к вашим персональным данным или счетам. Никогда не доверяйте ссылкам в личных сообщениях, публикациях и электронных письмах.

Это самые распространенные уловки Интернет-аферистов. Запомните их и поделитесь с близкими. А обо всех фактах мошенничества сообщайте в ближайший отдел полиции или по телефону «02» («102» – с мобильного).