Приложение №3 к Письму
Министерства цифрового развития
и связи Кузбасса
от _____ № _____

Рекомендации по профилактике мошенничества с использованием методов социальной инженерии

1. Будьте осторожны с неожиданными сообщениями или звонками.

Обратите внимание на сообщения или звонки, которые поступают от незнакомых или подозрительных номеров или аккаунтов. Будьте особенно осторожны при получении запросов на конфиденциальную информацию, такой как пароли или данные банковских счетов.

2. Проверяйте подлинность сообщений.

Вместо того, чтобы незамедлительно действовать на сообщение с просьбой о предоставлении информации или осуществлении каких-либо действий, всегда проверяйте подлинность сообщения.

Внимание! Особо осторожно относитесь к звонкам и сообщениям в мессенджерах от аккаунтов, представляющихся контролирующими органами (например ФСБ России, ФСТЭК России, Прокуратуры), содержащих запросы сведений об отдельных категориях граждан, в рамках якобы ведущейся проверки! Кроме того, рассылка может осуществляться с взломанных аккаунтов в мессенджерах от лица руководителей органов (организаций) с указанием предоставить сведения и/или оказать содействие сотрудникам контролирующих органов (например ФСБ России, ФСТЭК России, Прокуратуры).

Ваши действия! Свяжитесь с отправителем через другой канал связи и убедитесь, что запрос действительно пришел от них, в том числе с официальными представителями контролирующих органов, руководителем органа (организации) или представителем банка.

Помните! В связи с повышенным риском мошенничества и утечки конфиденциальной информации, контролирующие органы и банки не осуществляют через мессенджеры запросы сведений или информирование клиентов!

3. Не доверяйте ненадежным ссылкам.

Будьте особенно осторожны с ненадежными ссылками, которые могут поступать через мессенджеры или электронную почту. Никогда не кликайте на подозрительные ссылки и не предоставляйте свои данные на ненадежных веб-сайтах. Это могут быть вредоносные программы или часть фишинговой атаки, направленной на получение ваших конфиденциальных данных. Важно

обеспечить надежную защиту своих устройств путем установки антивирусного программного обеспечения.

4. Обновляйте программное обеспечение.

Регулярно обновляйте программное обеспечение на своих устройствах. Обновления могут содержать исправления уязвимостей, которые могут быть использованы злоумышленниками при социальной инженерии.

5. Обучайте сотрудников.

Проводите тренинги и семинары по противодействию социальной инженерии для всех сотрудников, особенно тех, кто имеет доступ к конфиденциальной информации. Расскажите им о распространенных методах и тактиках социальной инженерии и научите их распознавать и предотвращать атаки.

6. Осознавайте риски и сохраняйте здравый смысл.

Всегда помните, что социальная инженерия направлена на манипуляцию ваших эмоций или создание ситуаций, которые могут выглядеть совершенно реальными. Осознавайте риски и сохраняйте здравый смысл, прежде чем предоставлять кому-либо конфиденциальную информацию или совершать какие-либо финансовые операции.

7. Используйте многофакторную аутентификацию.

Включите многофакторную аутентификацию в своих мессенджерах и других онлайн-платформах для дополнительной защиты своего аккаунта. Это может включать коды повторной проверки на других устройствах или с использованием биометрических данных, таких как отпечатки пальцев или распознавание лица. В случае, если злоумышленник попытается получить доступ к аккаунту, он столкнется с дополнительным уровнем защиты.

8. Проверяйте настройки конфиденциальности, чтобы убедиться, что ваша личная информация защищена.

Контролируйте, кто может видеть ваши данные и убедитесь, что доступ имеют только те, кому доверяете.

9. Используйте для каждой учетной записи уникальные пароли и не используйте общие пароли для разных сервисов.

Это поможет уменьшить риск взлома и сохранит вашу личную информацию в безопасности.