**Ликбез по информационной безопасности**

Данные, которые нельзя сообщать никому и никогда! В киберпространстве действует простое правило: чем меньше личной информации вы раскрываете, тем труднее вас обмануть. Даже один невинный ответ может стать началом цепочки мошенничества. Ниже — перечень ключевых данных, которые всегда должны оставаться при вас.

Финансовая информация:

– номер карты, срок действия, CVC/CVV-код, логины и пароли от интернет-банка, коды из SMS, пуш-уведомления подтверждения.

Пример: вам заказное письмо, для подтверждения доставки, отправьте код из SMS.

Персональные документы:

– паспортные данные, ИНН, СНИЛС, фото документов. Пример: подтвердите личность для доставки — отправьте фото паспорта.

Аутентификационные коды:

– любые разовые пароли из SMS, push-коды, QR-коды подтверждения. Никому и ни при каких условиях.

Приватная информация:

- адрес, номера родственников, маршрут поездки, точное местоположение в режиме реального времени. Особенно — в открытых аккаунтах.

Комбинации данных:

– имя + дата рождения + номер телефона — уже достаточно для подбора пароля, входа в почту или оформления кредита.

Помните: никто из официальных структур — ни банк, ни «Госуслуги», ни полиция — не попросит у вас коды доступа или паспорт по телефону или в чате. Ваши данные — ваша зона ответственности. Бережное отношение к ним — лучший вклад в безопасность вас и ваших близких.