В рамках реализации программы кибергигиены, предусмотренной Федеральным Проектом «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации», АНО «Диалог Регионы» и Минцифры России подготовили для вас образовательный курс, который поможет вам узнать о **личной информационной безопасности.**

В сети можно встретить целые массивы данных, которые были получены в результате тех или иных утечек.

КРУПНЫЕ УТЕЧКИ ДАННЫХ

умышленные **случайные**

1. Инсайдеры и избыточные права
Сотрудники сами получают доступ к закрытой информации и добровольно выносят их за пределы компании

2. Утеря носителей данных*
*Флешки, ноутбуки, смартфоны

3. Кража информации извне
Например, при помощи вредоносных программ

4. Ошибочные действия сотрудников организации
Несоблюдение правил кибербезопасности

5. Взлом программного обеспечения
Слабые места в используемых приложениях и системах могут стать причиной утечки

6. Человеческий фактор
Например, сотрудник открывает доступ к документам в облаке для всех желающих

7. Вредоносные программы
«Троянские кони»: вирусы, которые могут полностью контролировать систему компьютера

Злоумышленник может воспользоваться вашими данными множеством разных способов:

1. Украсть деньги с ваших счётов или взять микрокредит на ваше имя

2. Шантажировать вас. Например, публикацией фото

3. От вашего имени дискредитировать организацию, в которой вы работаете

4.. Устроить кибербуллинг - интернет-травлю

5. Включить ваше устройство в ботнет* - «сеть компьютеров, зараженных вирусом»

*В этих сетях неправомерные действия могут совершаться от имени других пользователей