Какие схемы используют мошенники?

- **«Представители социальных служб»** сообщают о доплатах и надбавках
- **«Медицинские работники»** предлагают пройти обязательное обследование или купить лекарства
- **«Сотрудники банка»** говорят о подозрительных действиях с картой и просят предоставить конфиденциальные данные
- **СМС о выигрыше денег** или другого ценного приза
- **Звонок от «сотрудника полиции»** с сообщением, что близкие попали в ДТП и срочно нужны деньги
- **Звонок от «сотрудника МФЦ»** с сообщением, что ваш личный кабинет атакуют мошенники и что прямо сейчас злоумышленники пытаются изменить номер телефона, привязанный к «Госуслугам»

Что делать? Поговорите с родственниками

- Расскажите, какие схемы используют мошенники
- Попросите, чтобы они никому не сообщали данные паспорта, карты или пенсионного
- Договоритесь, что деньги в банкомате вы будете снимать только вместе
- Регулярно звоните родным и навещайте их

Защитите деньги на карте

- Установите лимит на снятие наличных
- Оформите зачисление пенсии на карту
- Привяжите свой номер к карте, чтобы получать уведомления
- Большую часть денег храните на накопительном счете
- Запомните CVV-код на обратной стороне карты и никому его не сообщайте

Опасность! вредоносные программы

- **Вредоносные программы -** это программы, которые созданы для нанесения вреда вашему компьютеру или кражи вашей личной информации.
- Они могут проникнуть на ваш компьютер/смартфон при скачивании файлов или переходе по мошенническим ссылкам
- Вредоносные программы могут вызывать различные проблемы, такие как потеря данных или даже кража вашей личной информации, например, паролей или банковских данных.

Опасность! вредоносные программы

- **Вирусы:** программы, которые могут размножаться и прикрепляться к другим файлам на вашем компьютере/смартфоне. Они могут нанести ущерб вашей системе, удалять файлы или заражать другие компьютеры.

- **Шпионские программы:** следят за вашей активностью в интернете и собирают информацию о вас без вашего согласия, могут перехватывать пароли, банковские данные или другую личную информацию

- **Рекламное ПО (adware)**: программы, которые показывают назойливую рекламу. Они могут появляться в виде всплывающих окон или рекламных баннеров и замедлять работу вашего гаджета.

Опасность!
вредоносные программы

- **Расшифровщики и шифровальщики**: программы, которые захватывают ваши файлы и шифруют их, делая их недоступными для вас. Злоумышленники требуют выкуп за расшифровку ваших файлов.

- **Джекеры (keyloggers):** программы, которые записывают все, что вы вводите на клавиатуре, включая пароли и личную информацию. Злоумышленники могут использовать эту информацию для мошенничества или кражи личности.

Опасность!
Фишинг

- **Фишинговый сайт** – сайт подделка!

- Ссылка на такой сайт выглядит как настоящая.
- **Но**, в такой ссылке пропущены или добавлены символы, допущена ошибка в названии или указан другой домен.

- Интерфейс страницы тоже выглядят натурально, есть поля для ввода логина и пароля, только это форма отправки логина и пароля злоумышленникам. А ещё там может быть форма для ввода платёжной информации.

- Мошенники рассчитывают на то, что вы не заметите сайт-подделку и оставите на странице свои личные данные: логин, пароль, реквизиты карты.

Опасность!
Фишинг

- Поддельные «Официальные» электронные письма. **Это работает так**: на вашу почту приходит якобы официальное письмо от банка, интернет магазина или госуслуг или от любой другой компании, которой вы пользуетесь.

- **Адрес или название электронного ящика содержит ошибку**, письмо оформлено правдоподобно, но в нём содержится странная просьба. Например, перейти по ссылке для подтверждения учётной записи.

- Сделав так, вы рискуете потерять учётную запись и ваши персональные данные.

Что делать?
Быть внимательным

- **Внимание на адресную строку:** значок «замочек» должен быть закрыт, если открыт, значит отсутствует безопасное соединение
- **Подозрительный домен сайта:** домен, где не существует ограничений для регистрации (например: .org, .net, .info, .biz, .top, .in, .cc, .com.ua, .in.ua, .pp.ua, .kiev.ua, .dp.ua, .te.ua) или используется домен конструктора сайтов (например, Jimdo, Heroku);
- **Сайт из другого государства, хотя не должен быть (**например веб-сайт платежного сервиса России расположен в Германии, США, Латвии, Китае, Перу, Зимбабве)
- Много «несостыковок» или грамматических и синтаксических ошибок.
- **Сообщение об отказе в проведении банковской операции** (например, «Операция отменена банком! Возможные причины: …»), реже – сообщение об успешной операции, но при этом оплаченные услуги держателю не предоставляются.

Что делать?
Используйте сложные пароли

- Создайте пароль по формуле (его легко создать и запомнить, меняется только 3 часть формулы)
- **Простое слово**. Желательно, чтобы это слово легко переводилось на английский и содержало не меньше 5 символов. Для примера возьмем слово пианино. И пишем так, будто оно расположено в начале приложения, с большой буквы: **Pianino**
- **Комбинация из цифр, 2-3 достаточно.** Возьмите счастливое число или важное для вас число, чтобы легче запоминать. Например **951**
- Просто берем **первые 3 символа того сайта**, куда заходим. К примеру, мы регистрируемся на yandex.ru, значит берем **YAN**
- Выбирайте **любой спецсимвол**, который вам нравится, пусть будет знак вопроса **?**

- **Pianino951YAN?**

Что делать?
Установить антивирус

- На все свои гаджеты: компьютер, ноутбук, планшет и смартфон — **нужно установить антивирус**.
- Хороший антивирусный пакет включает защиту от спама и фишинговых писем. Он сам распознает подозрительных адресатов.
- Антивирус защитит от программ, которые воруют данные карт, получают доступ к онлайн- и мобильным банкам, перехватывают СМС и push-сообщения с секретными кодами.
- Важно регулярно обновлять защиту!

Помните!

- **Будьте осторожны в социальных сетях:** Не делитесь личной информацией в социальных сетях. Злоумышленники могут использовать ее против вас!
- Не заходите на сомнительные сайты и не открывайте письма с незнакомых адресов. Они могут содержать **вредоносные программы**.
- Используйте **сложные пароли** для своих аккаунтов и не повторяйте их. Это поможет защитить ваши данные.
- Установите **антивирусную программу**: Это специальная программа, которая поможет обнаружить и удалить вредоносные программы.
- Чаще звоните родным и близким!