ЦИФРОВОЙ ЩИТ: ПРОФИЛАКТИКА КИБЕРМОШЕННИЧЕСТВА СРЕДИ МОЛОДЕЖИ

Разработано в рамках Всероссийского информационно-просветительского проекта "Будем рядом"

Памятка «Как защититься от кибермошенников»

1 Основные схемы мошенничества

● Фишинг – поддельные сайты и письма с просьбой ввести личные данные.
● Фальшивые звонки – мошенники представляются банком, полицией или службой поддержки.
● Вредоносные программы – вирусы, которые крадут пароли и данные карт.
● Обман в соцсетях – просьбы перевести деньги «за срочную помощь».

2 Как защитить себя

✅ Никому не сообщайте:

● Коды из SMS (даже если звонят «из банка»).
● Данные карты (CVV, срок действия, PIN).
● Пароли от интернет-банка и соцсетей.

✅ Проверяйте ссылки:

● Не переходите по подозрительным ссылкам в SMS или почте.
● Официальные сайты банков всегда начинаются с https:// и имеют замок в адресной строке.

✅ Установите защиту:

● Антивирус на телефон и компьютер.
● Двухфакторную аутентификацию (2FA) в важных сервисах.

3 Что делать, если вы стали жертвой мошенников?

1️⃣ Немедленно позвоните в банк и заблокируйте карту.
2️⃣ Подайте заявление в полицию (можно онлайн через сайт МВД).
3️⃣ Поменяйте пароли от почты, соцсетей и банковских аккаунтов.

4 Телефоны помощи

● Банк (блокировка карты): номер на обратной стороне карты.
● Полиция: 102 (с мобильного), 112 (экстренный номер).
● Горячая линия по кибермошенничеству: 8-800-250-25-25 (ЦБ РФ).

⚠️ Помните:

● Банки никогда не просят коды из SMS или перевод денег «для проверки».
● Если предложение кажется слишком выгодным – это обман.

Будьте бдительны и защитите свои деньги!