БАЗОВЫЕ ПРАВИЛА ЛИЧНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:

ЗАЩИЩАЙТЕ СВОИ ПАРОЛИ:

Не используйте простые пароли, не делитесь ими ни с кем и регулярно меняйте.

БУДЬТЕ ОСТОРОЖНЫ С WI-FI СЕТЯМИ:

Избегайте использования общественных Wi-Fi сетей для оплаты или ввода конфиденциальных данных.

УСТАНАВЛИВАЙТЕ АНТИВИРУСНОЕ ПО:

Регулярно обновляйте антивирусное ПО и следите за его работой.

БЕРЕГИТЕ СВОИ ЛИЧНЫЕ ДАННЫЕ:

Не делитесь конфиденциальной информацией в социальных сетях и на других сайтах.

НЕ ПЕРЕХОДИТЕ ПО СОМНИТЕЛЬНЫМ ССЫЛКАМ:

Не открывайте письма и ссылки от незнакомых отправителей.

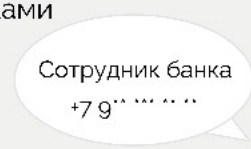
ПРОТИВОДЕЙСТВИЕ ТЕЛЕФОННЫМ МОШЕННИКАМ

НЕ ОТВЕЧАЙТЕ НА ЗВОНКИ С НЕЗНАКОМЫХ НОМЕРОВ

Если вам звонят
с незнакомого номера,
не отвечайте на него

БУДЬТЕ БДИТЕЛЬНЫ

Мошенники могут представляться
сотрудниками банков,
государственных органов
или родственниками



НЕ ПЕРЕВОДИТЕ ДЕНЬГИ ПО ПРОСЬБЕ НЕЗНАКОМЦЕВ

Никогда не переводите
деньги незнакомцам,
даже если они утверждают,
что находятся в беде

ПРОВЕРЬТЕ ИНФОРМАЦИЮ

Если вам поступил
подозрительный звонок,
проверьте информацию,
позвонив на официальный
номер организации

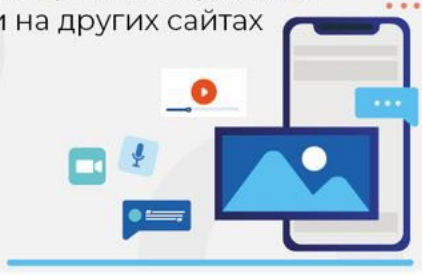
СООБЩИТЕ О МОШЕННИЧЕСТВЕ

Если вы стали жертвой
телефонного мошенничества,
сообщите в полицию

ЗАЩИТИТЕ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

БУДЬТЕ ОСТОРОЖНЫ С ТЕМ, ЧТО ВЫ ПУБЛИКУЕТЕ

Не делитесь конфиденциальной информацией в социальных сетях и на других сайтах



ИСПОЛЬЗУЙТЕ НАДЁЖНЫЕ ПАРОЛИ

Не используйте простые пароли, не делитесь ими ни с кем и регулярно меняйте

БУДЬТЕ БДИТЕЛЬНЫ ПРИ ИСПОЛЬЗОВАНИИ ПУБЛИЧНЫХ КОМПЬЮТЕРОВ

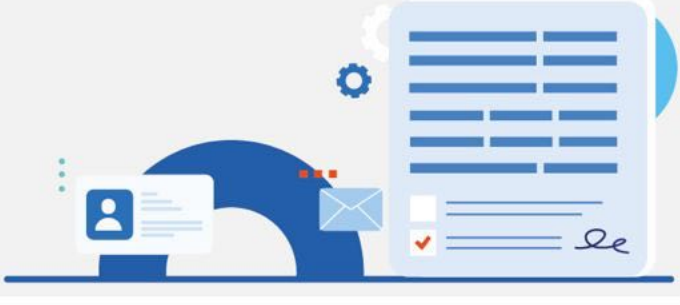
Не используйте публичные компьютеры для ввода конфиденциальных данных

УСТАНОВИТЕ АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Регулярно обновляйте антивирусное ПО и следите за его работой

ОЗНАКОМЬТЕСЬ С ПОЛИТИКОЙ КОНФИДЕНЦИАЛЬНОСТИ

Перед тем как поделиться своими данными на каком-либо сайте, ознакомьтесь с его политикой конфиденциальности



БУДЬТЕ ВНИМАТЕЛЬНЫ ПРИ РАБОТЕ С ПИСЬМАМИ

БУДЬТЕ ОСТОРОЖНЫ С ФИШИНГОВЫМИ ПИСЬМАМИ

Фишинговые письма могут содержать ссылки на поддельные сайты, которые выглядят как подлинные

НЕ ПЕРЕХОДИТЕ ПО СОМНИТЕЛЬНЫМ ССЫЛКАМ

Не открывайте письма и ссылки от незнакомых отправителей

НЕ ВВОДИТЕ СВОИ ДАННЫЕ НА ПОДОЗРИТЕЛЬНЫХ САЙТАХ

Если вы не уверены в подлинности сайта, не вводите на нем свои данные

УСТАНОВИТЕ АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Регулярно обновляйте антивирусное ПО и следите за его работой

СООБЩИТЕ О ФИШИНГОВЫХ САЙТАХ

Если вы обнаружили фишинговый сайт, сообщите о нём в соответствующие органы