Уважаемые вкладчики!

В современном мире мошенники используют телефонные звонки, SMS, электронную почту и социальные сети, чтобы получить доступ к личным и финансовым данным. Защита этих данных помогает сохранить вашу информацию и предотвратить финансовые потери.
Ниже представлены рекомендации, которые помогут снизить риски и избежать мошенничества.

1. На что обращать внимание

Телефонные звонки:

- Звонки якобы от имени пенсионного фонда, банков или государственных органов с просьбой сообщить коды, пароли или реквизиты карт.
- Создание чувства срочности: «Необходимо срочно подтвердить операцию», «Ваш счет заблокирован».

SMS и мессенджеры:

- Сообщения с ссылками на поддельные сайты для ввода личных данных.
- Уведомления о «подозрительных списаниях» или «необычной активности».

Электронная почта:

- Письма с просьбой оплатить услуги, скачать вложения или проверить документы.
- Ссылки могут вести на мошеннические сайты.

Социальные сети:

- Поддельные аккаунты знакомых или официальных лиц.
- Запросы о переводе средств или предоставлении конфиденциальной информации.

2. Какие данные нельзя передавать

Ни при каких обстоятельствах не сообщайте:

- Коды подтверждения из SMS, push-уведомлений или приложений.
- Полные данные банковских карт: номер, срок действия, CVV/CVC.
- Логины и пароли от личных или рабочих аккаунтов.
- QR-коды и одноразовые токены.
- Персональные данные, информацию о доходах и другую конфиденциальную информацию.

3. Практические рекомендации

1. **Проверяйте источник запроса.** Если звонок или письмо вызывает подозрение, свяжитесь с организацией напрямую через официальные контакты.
2. **Не переходите по сомнительным ссылкам.** Введите адрес сайта вручную в браузере.
3. **Используйте безопасные каналы связи.** Не передавайте конфиденциальные данные через личные мессенджеры или социальные сети.
4. **Обновляйте пароли и используйте сложные комбинации.** Не используйте одинаковые пароли для разных сервисов.
5. **Следите за обновлениями ПО и антивирусов.** Актуальные версии снижают риск заражения вредоносными файлами.
6. **Не подключайте неизвестные устройства.** USB-флешки и внешние диски могут содержать вредоносное ПО.
7. **Будьте осторожны с вложениями и файлами.** Открывайте их только после подтверждения источника.

4. Действия при подозрительных событиях

Если вы получили подозрительный звонок, письмо или сообщение:

- Прекратите общение с неизвестным лицом.
- Не вводите данные и не открывайте вложения.
- Сообщите о ситуации в службу поддержки.
- При необходимости заблокируйте карты или доступ к онлайн-сервисам.

Соблюдение простых правил информационной безопасности помогает защитить личные данные, избежать финансовых потерь и сохранить репутацию. Быстрая проверка источников, осторожность при передаче информации и использование безопасных каналов связи ключевые меры защиты.