Номера телефонов вызовов экстренных служб:
Единая служба спасения - 112
Полиция – 102

Прокуратура Архангельской области
и Ненецкого автономного округа
Адреса:

г. Архангельск, пр. Новогородский, д. 15
Телефон: (88182) 410-208

г. Нарьян-Мар, ул. Ленина, д. 40
Телефон: +7-911-552-83-62

Прокуратура Архангельской области
и Ненецкого автономного округа

«Способы защитить себя от мошенников»

2025 год

БУДЬТЕ БДИТЕЛЬНЫ И ПОМНИТЕ:

Распространенные способы действий мошенников – получение обманным путем данных для доступа к личным кабинетам и приложениям. Злоумышленники могут использовать нейротехнологии, способные подделывать аккаунты и голоса, создавая видеосообщения от имени ваших знакомых и руководителей.

Вот несколько советов, которые помогут вам защититься от мошенников:

1) Если разговор кажется подозрительным, завершите его и перезвоните в организацию по официальным номерам;

2) Проверяйте способ связи: мошенники часто используют мессенджеры, тогда как настоящие представители не звонят через WhatsApp или Telegram;

3) Не сообщайте логины и пароли: читайте назначение смс-кодов и не делитесь ответами на контрольные вопросы;

4) Следите за актуальностью номера: убедитесь, что номер, к которому привязан аккаунт, актуален;

5) Используйте сложные пароли: меняйте их регулярно и подключайте двухфакторную аутентификацию;

6) Проверяйте адрес страницы: убедитесь, что сайт – это официальный ресурс (например, gosuslugi.ru).

Зачастую мошенники представляются сотрудниками различных служб или предлагают финансовые выигрыши.

Помните, что сотрудники финансовых организаций никогда по номеру телефона или в электронном письме

НЕ ЗАПРАШИВАЮТ:

1) персональные сведения (серия и номер паспорта, адрес регистрации, имя и фамилия владельца карты);

2) реквизиты и срок действия карты;

3) пароли или коды из СМС-сообщений для подтверждения финансовых операций или их отмены;

4) логин, ПИН-код и CVV (CVC)-код банковских карт.

НЕ ПРЕДЛАГАЮТ:

1) установить программы удаленного доступа на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки (например, удаление вирусов с устройства);

2) перейти по ссылке из СМС-сообщения;

3) включить переадресацию на телефоне клиента для совершения в дальнейшем звонка от его имени в банк;

4) перевести для сохранности денежные средства на «защищенный счет»;

5) зайти в онлайн-кабинет по ссылке из СМС-сообщения или электронного письма.

Банк может инициировать общение с клиентом только для консультаций по продуктам и услугам кредитно-финансового учреждения. При этом звонки совершаются с номеров, указанных на оборотной стороне карты, на сайте банка или в оригинальных банковских документах. Иные номера не имеют никакого отношения к банку.

При использовании мобильного телефона соблюдайте следующие правила:

1) при установке приложений обращайте внимание на полномочия, которые они запрашивают. Будьте особенно осторожны, если приложение просит права на чтение адресной книги, отправку СМС-сообщений и доступ к сети «Интернет»;

2) отключите в настройках возможность использования голосового управления при заблокированном экране.

3) применяя сервисы СМС-банка, сверяйте реквизиты операции в СМС-сообщении с одноразовым паролем от официального номера банка. Если реквизиты не совпадают, то такой пароль вводить нельзя.

4) в случае смены номера телефона или его утраты свяжитесь с банком для отключения и блокировки доступа к СМС-банку и заблокируйте сим-карту, обратившись к сотовому оператору.

При возникновении подозрений насчет предпринимаемых попыток совершения мошеннических действий следует незамедлительно уведомить об этом банк.