ПАМЯТКА

о противодействии мошенничеству
в социальных сетях, мессенджерах
и по телефону

Мошенники могут выдавать себя за:

- Сотрудников правоохранительных органов и иных силовых структур (МВД, СК, ФСБ, прокуратуры и др.)
- Представителей контрольно-надзорных органов
- Руководителей органов власти и государственных учреждений
- Представителей банков, служб безопасности или техподдержки
- Известных публичных лиц
- Коллег, руководителей, подчиненных
- Друзей, родственников и знакомых

Мошенники применяют:

телефонные звонки (в том числе с подменой номера и имитацией голоса)

видеозвонки (с применением «дипфейков» для создания поддельного видеоизображения)

фейковые или взломанные аккаунты электронной почты, социальных сетей и мессенджеров

поддельные групповые чаты якобы с коллегами или другими лицами (где все участники, кроме вас, являются мошенниками)

Мошенники пытаются:

получить доступ к информации ограниченного доступа (персональным данным, служебной тайне и иной), банковским данным

убедить **перевести деньги** или передать иные ценности

склонить к **совершению противоправных действий** (например, поджоги, диверсии и т.п.)

Сообщения и звонки часто содержат:

просьбы об оказании содействия в решении «важного» или «секретного» вопроса (например, в **расследовании преступления, в проведении проверки** контролирующего органа, **выявлении экстремистов** и т.п.)

предупреждения о скором звонке уполномоченного сотрудника из профильного ведомства (например, МВД, ФСБ, прокуратуры)

просьбы **дать комментарии** о чрезвычайном происшествии (о площади возгорания, числе пострадавших, размере ущерба и т.д.) и ином событии

поручения **направить информацию** или документы

Сообщения и звонки часто содержат:

поручения или просьбы **установить приложение или открыть файл**

просьбы **перейти по ссылке, пройти регистрацию или сообщить код**

имитации рабочих ситуаций (поручения от «руководства» или «коллег»)

«выгодные» предложения бесплатных услуг и товаров, высокооплачиваемой подработки, получения выигрыша или иной прибыли

элементы **запугивания и шантажа**

В почте и мессенджерах необходимо:

Проверять имя домена отправителя электронного письма (не служебные почтовые ящики должны насторожить, например: @mail.ru, @gmail.com и другие)

Не открывать и не загружать почтовые вложения (файлы) писем с тематикой, **не относящейся к деятельности** органа (организации)

Не открывать и не загружать почтовые вложения (файлы) писем **от неизвестных отправителей**

Не открывать и не загружать почтовые вложения (файлы) писем, которые **не ожидаемы или не запрошены вами**

Не открывать и не загружать **потенциально вредоносные вложения (файлы)** с расширением .zip, .exe, .vbs, .js, .pdf.exe, .doc.exe, .docm, .xlsm, .bat, .cmd, .hta, .scr, .msi и прочие

Что должно насторожить:

просьбы никому не сообщать о факте разговора или сообщения

давление на срочность («нужно немедленно», «времени нет»)

сообщения от лиц, с которыми **ранее не было общения**

просьбы и поручения, которые **не входят в ваши должностные обязанности**

необычные просьбы (участие в следственных действиях или проверках)

Что должно насторожить:

разговоры о деньгах (в любой форме – о счетах, комиссиях, предоплате, выигрыше, доходе, инвестициях, долге, и т.д.)

использование неофициальных каналов связи (важный вопрос решается не лично и не через официальные документы, а через мессенджеры)

просьбы **раскрыть личные, конфиденциальные данные** (ваши или чужие) (требуют сообщить пароли, коды из SMS/CVC, паспортные данные)

попытки **запугивания** (срочная помощь родственнику, угрозы финансовых потерь, уголовного преследования, проверок контролирующих органов, прямой шантаж)

Как правильно действовать:

прервите беседу, положите трубку

спокойно обдумайте ситуацию

не совершайте поспешных действий и не выполняйте требований мошенников

проверьте информацию: перезвоните по знакомому номеру, обратитесь в официальную службу (банка, магазина, госоргана и т.д.)

обсудите лично с близкими людьми или коллегами и руководителем (если вопрос по работе)

Кого информировать:

О попытках совершения мошеннических действий необходимо незамедлительно **информировать непосредственного руководителя и правоохранительные органы**

Ответственность:

Административная: штрафы по статье 13.11 КоАП РФ за действия (бездействие), повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей персональные данные.

Дисциплинарная: замечание, выговор, лишение премии или увольнение по статье 81 ТК РФ за разглашение охраняемой законом тайны.

Уголовная:

по ст. 275 УК РФ за оказание финансовой, материально-технической, консультационной или иной помощи иностранному государству, международной либо иностранной организации или их представителям в деятельности, направленной против безопасности Российской Федерации;

по ст. 275.1 УК РФ за сотрудничество на конфиденциальной основе с иностранным государством, международной либо иностранной организацией.