

Самые «популярные» сценарии звонков и обращений:

- «Вам полагается прибавка к пенсии» за неучтенный стаж - из Социального фонда России;
- «Получите новые льготы» за ЖКУ для записи на прием в МФЦ;
- «Срочно переводите все средства на безопасный счет» - из «банка», «МВД», «ФСБ»;
- «Новый полис ОМС», «Провайдер ускорит интернет», «Выгодные инвестиции», «Истекает срок действия SIM-карты», «QR код домового чата», «Мама, я попал в аварию».

С недавнего времени начали поступать звонки от якобы сотрудников Федеральной налоговой службы «Вы не подали сведения о доходах за 2024 год в форме 3-НДФЛ». При этом для записи на прием требуют сообщить паспортные данные или ИНН.

Поступают письма от «Госуслуг» о попытках входа в аккаунт с других устройств с указанием в сообщении поддельного номера телефона службы поддержки.

Мошенники представляются сотрудниками «жилищной инспекции» и угрожают изъятием домашних животных, если не будут переведены денежные средства. Предварительно они выясняют количество домашних питомцев и требуют оплату за «разрешение» на их содержание. Злоумышленники отправляют ссылки на поддельный сайт «Госуслуг», чтобы украсть личные данные.

Аферисты, представляясь инженерами оператора связи, под предлогом «проверки телефонной линии» просят набрать комбинации вроде #90, #09 или других. Нажатие этих цифр может передать управление SIM-картой аферистам, что позволяет им совершать звонки за счет абонента и получать доступ к банковским приложениям.

Общие признаки мошеннических схем:

- Звонок или СМС поступает с незнакомого номера телефона.
- Следует запрос персональных данных (паспорт, ИНН, банковские реквизиты, коды СМС). Звонок сопровождается просьбой сообщить код из СМС и/или скачать приложение по ссылке.
- Требование срочно перевести деньги.
- Давление, угрозы или предложение слишком выгодных условий.

Данный перечень признаков не является исчерпывающим.

Главное правило: никогда не переводите деньги и не сообщайте конфиденциальные данные (пароли, коды из СМС, паспортные данные, данные карты) по просьбе незнакомых лиц по телефону, в СМС или письмах!

По просьбе незнакомых лиц не заходите на сайт, не регистрируйтесь, не делайте заказы; не пишите администратору ресурса «Вы не мошенники?».

Рекомендации по безопасности по распознаванию Интернет-злоумышленников:

1. Общие правила:

- Никогда и никому не сообщайте коды из СМС, пароли, полные данные паспорта, банковской карты или ИНН по телефону, в ответ на СМС или письмо.
- Никогда не переводите деньги по требованию незнакомых лиц, особенно под давлением или спешкой.
- Не отвечайте на сомнительные письма или звонки с незнакомых номеров. Просто положите трубку.
- Не торопитесь выполнять любые инструкции, полученные от неизвестных лиц.

2. Работа с почтой и СМС:

- Не переходите по ссылкам в письмах и СМС от неизвестных отправителей.
- Не скачивайте вложенные файлы от неизвестных отправителей.
- Не вводите никаких данных (логины, пароли, персональные данные) в формы, открывшиеся по подозрительным ссылкам.
- Не пересылайте подозрительные письма другим.
- Удаляйте подозрительные письма из почтового ящика и очищайте корзину.

3. Защита аккаунтов и мессенджеров:

- Всегда используйте сложные уникальные пароли и двухфакторную аутентификацию (например: ввод пароля и подтверждение смс) везде, где это возможно;
- Выставляйте корректные настройки приватности и конфиденциальности в соцсетях и мессенджерах.

Советы по настройке безопасности WhatsApp:

1. Включите двухшаговую проверку (Настройки - Аккаунт - Двухшаговая проверка). Укажите адрес электронной почты для восстановления PIN-кода.
2. Ограничьте добавление в группы: «Настройки» - «Конфиденциальность» - «Группы» - Выберите «Мои контакты».
3. Отключите звонки от неизвестных номеров: «Настройки» - «Конфиденциальность» - «Звонки» - «Личные звонки» - Выберите «Мои контакты».

4. Регулярно проверяйте список связанных устройств (Настройки - Связанные устройства): убедитесь, что там нет неизвестных вам устройств. Отвязывайте ненужные.
5. Установите код доступа (PIN) на само приложение WhatsApp, если ваш телефон поддерживает блокировку приложений.
6. Для продвинутых: Изучите настройки в разделах «Конфиденциальность» - «Расширенные настройки» и «Проверка конфиденциальности».

Советы по настройке безопасности Telegram:

1. Регулярно проверяйте, на каких условиях активен ваш аккаунт (Настройки - Устройства) если находите аномалии - сразу удаляйте подозрительный сеанс.
2. Скрывайте свои фото (Настройки - Конфиденциальность - Фотографии профиля) настраивайте так, чтобы их никто не видел.
3. Включите код-пароль (Настройки - Конфиденциальность - Код-пароль (включите и не забывайте)) можно включить облачный пароль.
4. Запретите добавлять себя в групповые чаты и каналы (Настройки - Конфиденциальность - Приглашения) настраиваете так, чтобы никто не мог приглашать.
5. Скрывать свой номер телефона (Настройки - Конфиденциальность - Номер телефона) настраиваете так, чтобы его никто не видел.
6. Установить запрет на звонки посторонних (Настройки - Конфиденциальность - Звонки) PEER-TO-PEER (анонимные звонки) вообще отключаем, а обычные - по своему усмотрению, но точно не «для всех».