

ПАМЯТКА

как обезопасить себя от преступлений, совершаемых с использованием IT-технологий (телефонного мошенничества)

Установите самозапрет на получение кредита «на Госуслугах»

Функция самозапрета не позволит мошенникам оформить кредит на ваше имя в онлайн режиме.

Как подключить: войдите в личный кабинет «Госуслуг» на сайте или в приложении; в строке поиска введите «Самозапрет на кредит»; выберите услугу «Установление запрета на получение кредита»; укажите условия: полный запрет, либо частичный.

Также можно установить самозапрет в отделении МФЦ.

Защитите свой аккаунт «на Госуслугах» с помощью «Доверенного контакта»

Функция позволяет дополнительно обезопасить учётную запись «на Госуслугах», значительно снижает риски неправомерного доступа к ней.

Как это работает: в ситуации, когда потребуется восстановить доступ (пароль), SMS-код для подтверждения придёт на номер доверенного лица. При этом он не получает доступа к вашему личному кабинету и не может ничего делать от вашего имени.

Как подключить: зайдите в личный кабинет: Профиль → Безопасность → Доверенный контакт; выберите близкого человека с подтверждённой учётной записью «Госуслуг», укажите его номер телефона, использованный для регистрации «на Госуслугах».

Установите самозапрет на регистрацию новых СИМ-карт «на Госуслугах»

Функция не позволит преступникам оформить на ваше имя новый номер и использовать его.

Как это сделать: авторизуйтесь на портале «Госуслуги»; перейдите в «Профиль» → «Сим-карты»; нажмите «Установить запрет» в блоке «Запрет на оформление договоров связи».

Также можно лично обратиться в МФЦ, понадобятся паспорт и СНИЛС.

Защитите свой аккаунт в мессенджере Max

Что делать: перейдите в раздел «Профиль» – «Безопасность», включите «Безопасный режим».

Как это работает:

- ограничение звонков и приглашений в чаты (только контакты);
- ограничение круга общения (только доверенные лица);
- ПИН-код на настройки (предотвращает несанкционированное отключение безопасного режима в случае временного доступа злоумышленника к телефону).

Защитите свой аккаунт в мессенджере Telegram

Что делать: включите двухфакторную аутентификацию (Настройки - Конфиденциальность - Облачный пароль) (для входа в аккаунт, помимо номера телефона, потребует также ввод облачного пароля); разрешите звонки в мессенджере только своим контактам.

Защитите свой телефон от вирусов

Для получения доступа к телефону злоумышленники присылают сообщения, содержащие APK-файл (установочный пакет) с вредоносным программным обеспечением или ссылки на него.

Самые распространенные сценарии и приемы:

- под видом знакомого присылают ссылку или файл Фото.apk, утверждая, что внутри интересный или важный контент;
- под видом оператора утверждают, что из-за смены номера/тарифа срочно нужно внести изменения в банковское приложение, и для этого якобы требуется установить их «служебную» программу (Договор.apk, 5G.apk и т.п.).

Что необходимо делать:

- установить антивирусное программное обеспечение;
- не открывать подозрительные файлы из сообщений и не переходить по подозрительным ссылкам.

Если уже вы общаетесь по телефону или мессенджеру с подозрительными лицами помните:

Мошенники играют на чувствах, а не на глупости.

Страх: «Ваш счет/госуслуги заблокированы!», «За вами числится долг!», «Ваш родственник в беде!», «Твои фотографии по всему интернету!».

Жадность/Выгода: «Вы выиграли приз!», «Супер-скидка только сейчас!», «Инвестиции с гигантским доходом!».

Доверие: маскировка под ФСБ, полицию, Центробанк, банк, иные госорганы, мед. организации, родных, знакомых.

Помните, сотрудники вышеуказанных организаций не будут звонить вам по телефону, мессенджером.

Цель № 1 мошенников – моментальная реакция. Их задача – заблокировать критическое мышление, заставить действовать здесь и сейчас. Ключевая фраза для слушателя: «Если вас торопят – это 100% обман».

Если вы уже общаетесь с кем-то, и у вас есть малейшие сомнения, что они выдают себя за кого-то другого, **любое общение лучше сразу прекратить:** т.е. - не разговаривать, не переписываться. В любом случае, остановитесь, подумайте, проанализируйте – «что происходит». Есть сомнения – позвоните на горячую линию, той организации, с которой вам якобы звонили, посоветуйтесь с родными, друзьями. Не предпринимайте скоропалительных решений, действий. **Никогда не сообщайте кому-либо коды подтверждения.** Ни в коем случае **не выполняйте никаких поручений** таких лиц (что-то куда-то перевезти, забрать предмет, передать, сфотографировать объект, облить краской здание и т.п.). Это может привести к гораздо более тяжелым последствиям – гибели людей и привлечению вас к уголовной ответственности.

Более подробную информацию по данной теме можно посмотреть на официальном канале Управления по борьбе с киберпреступностью МВД России:

в Max: <https://max.ru/cyberpolice>; в Телеграмм: t.me/cyberpolice_rus