

ПАМЯТКА

Как обезопасить себя в интернете



Правила безопасного поведения в интернете должен знать каждый!

Стать жертвой мошенников может любой человек. По данным Центробанка, в 2024 году 30% россиян столкнулись с мошенничеством в сети

200 млрд ₽

общая сумма ущерба от киберпреступлений в 2024 году

Частые схемы обмана

Звонки и сообщения под видом сотрудников банков или полиции

73%

Предложения по инвестициям

62%

Сообщения об отмене и подтверждении операций

54%

Наиболее уязвимы для мошенников люди, которые активны в интернете, часто общаются с незнакомцами и публикуют личную информацию в открытом доступе

Распространённые схемы мошенничества



Общение от имени банка, службы доставки или полиции

Во время разговора мошенники пытаются получить личные данные, конфиденциальную информацию и коды доступа к аккаунтам

Взлом аккаунтов и рассылка сообщений от лица знакомых

В этом случае мошенники просят перевести деньги или перейти по ссылке



Фишинговые ссылки

Обычно такие ссылки ведут на установку вирусных и шпионских приложений. Они крадут данные и могут навредить самому устройству

Способы обмана и защиты от него

Запугивание

Вам сообщают о потере денег, доступа или безопасности

Примеры:

- Вас взломали!
- С карты списывают деньги!

Решение

- Не торопитесь
- Не предпринимайте действий по инструкции из сообщения и проверьте информацию — позвоните в банк по номеру, указанному на карте

Обещание лёгких денег

Вам предлагают быстро и без усилий заработать

Примеры:

- Вы выиграли iPhone!
- Кредит под 0%

Решение

- Помните: бесплатный сыр бывает только в мышеловке
- Проверяйте любые акции на официальных сайтах и игнорируйте сомнительные сообщения

Упор на доверие

С вами общаются от имени друзей, родственников или официальных лиц

Примеры:

- Звонок «сотрудника банка»
- Сообщение от «друга»

Решение

- Положите трубку и перезвоните на официальный номер
- При общении со знакомыми перезвоните на известный вам номер или используйте проверочный вопрос

Ограничение по времени

Вас заставляют принять решение срочно, не дают обдумать ситуацию и проверить факты

Примеры:

- У вас 5 минут!
- Нужно срочно!
- Акция только сегодня!

Решение

- Помните: настоящие проблемы не решаются за 5 минут в разговоре с незнакомцем
- Возьмите паузу и проверьте информацию. Попытка вас торопить — признак мошенничества

Правила безопасности в мессенджерах

1

Используйте двухфакторную аутентификацию

Обязательно установите пароль и подключите двухфакторную аутентификацию, чтобы мошенники не могли получить доступ к вашему аккаунту

2

Не публикуйте личные данные

Этой информацией могут воспользоваться мошенники, причём не только против вас, но и против ваших знакомых

3

Не отвечайте на звонки и сообщения от незнакомцев

Все важные контакты записаны в телефонной книге, а звонки и СМС с незнакомых номеров можно спокойно игнорировать и даже блокировать

Если вы случайно ответили на звонок, как можно скорее завершите разговор — не дожидаетесь разрешения и не оправдываетесь, иначе мошенники могут записать слепок вашего голоса и использовать его в своих целях

4

Не переходите по ссылкам и не скачивайте файлы

Переходить по ссылкам и устанавливать незнакомые приложения опасно — там может быть вирус или программа для кражи данных

Лучше ограничиться приложениями, которые рекомендованы правительством — такими как Госуслуги, MirPay, RuStore, ВКонтакте, МАХ и др.

5

Не доверяйте информации в сети

В интернете встречаются фейковые и провокационные новости и посты. В них может содержаться ложная, а порой и откровенно вредная информация

Любую информацию важно проверить в нескольких официальных источниках и убедиться в её достоверности. Если возникают сомнения, лучше уточнить у знакомых и доверенных лиц



Сферум в МАХ — безопасное пространство для общения



Настройки приватности



Позволят скрыть вас из поиска и выбрать, кто может вам звонить, добавлять в чаты и видеть в сети. Безопасный режим защитит вас от сообщений и звонков от незнакомцев

Проверенные контакты



В Сферуме можно проверить собеседника, посмотрев его профиль и роль в организации в личном кабинете. Педагоги отмечены академической шапочкой

Центр безопасности



Можно пожаловаться на нежелательный контент и сообщения от незнакомых пользователей. Все обращения оперативно рассматриваются

Безопасный контент



В настройках приватности можно скрыть контент с маркировкой 16+. Функция позволяет исключить чувствительную и нежелательную информацию

Защищённые чаты



В учебных чатах состоят только пользователи из вашей образовательной организации — учащиеся, педагоги и родители

Защита близких



Родитель может настроить приватность на телефоне ребёнка и создать для него безопасную цифровую среду

Сферум стоит на страже ваших данных и переписок

Используйте для общения только
проверенные сервисы, чтобы
защитить себя и своих детей



Установить Сферум в МАХ

