**Кибербезопасность – это важно!**

Интернет-мошенники регулярно изобретают новые схемы обмана. Однако соблюдая простые правила кибергигиены, вы сможете им противостоять. Проверьте свои навыки защиты от киберугроз и узнайте, как оградить от них себя и свою семью.

1. **Как создать надёжный пароль**

*Признаки надёжного пароля*

* Длинный и его трудно угадать

Надёжный пароль содержит 12 символов, включает буквы в разном регистре, цифры и специальные символы (~!@#$%^&\*+-/.,\{}[]();:|?<>=)

* В нём нет последовательных комбинаций клавиш

Не используйте последовательный набор клавиш, например «qwerty», — его легко взломать. Для надёжного пароля применяйте случайную комбинацию букв, цифр и других символов.

* Нет личных данных

Не используйте для паролей личные данные, например фамилию, дату рождения или кличку питомца. Такую информацию легко узнать, просмотрев ваши социальные сети

* Содержит фразу

Выбирайте за основу не слова, а фразы — они длиннее, их сложнее угадать или перебрать. Используйте для пароля смешное событие, забавную привычку, тайную мечту — такой пароль легко запомнить и трудно подобрать: «ГотовлюБорЩ\_на5+баллов!@», «РекордПрохождения$Цивилизации$-32часа», «\_Поеду1\_вРио-де-Жанейро-вБелыхШт@н@х»

* Уникальный

Придумайте пароль для каждого критичного аккаунта — интернет-банка, соцсетей и Госуслуг. Если один и тот же пароль используется в разных сервисах, взломав один, злоумышленники получат доступ ко всем вашим аккаунтам

Для аккаунтов, в которых не хранятся важные данные и не совершаются покупки, можно придумать простой и даже повторяющийся пароль

*Идеи для создания надёжного пароля*

Используйте генераторы паролей — программы, которые формируют случайные комбинации по заданным требованиям

*Как сохранить пароли в безопасности*

* Не сохраняйте пароли на смартфоне, планшете или компьютере

Если злоумышленники получат доступ к вашему устройству, они легко доберутся до паролей. Также небезопасно хранить пароли в браузерах — в них периодически находят уязвимости, которыми могут воспользоваться хакеры, чтобы добраться до ваших паролей

* Используйте двухфакторную аутентификацию (2FA)

Это метод защиты аккаунта не только посредством ввода логина и пароля, но и при помощи кода, известного только вам как владельцу аккаунта. Код может быть отправлен по смс или на электронную почту, а также создан специальным приложением-генератором одноразового кода: Twilio Authy, Duo Mobile и «Яндекс.Ключ»

2FA — дополнительный уровень безопасности, так вы усложните путь хакерам. Плюс 2FA помогает предотвратить взлом. Если вы получили смс с кодом, который не запрашивали, значит, аккаунт пытаются взломать, нужно срочно сменить пароль

В Госуслугах пользователи также могут настроить двухфакторную аутентификацию. Вход с подтверждением по смс нужен для безопасного доступа к личному кабинету и данным на портале. При каждом входе на Госуслуги будет приходить смс с одноразовым кодом подтверждения. Этот код нужно указывать после ввода пароля. Помните, что его никому нельзя сообщать

* Используйте менеджер паролей

Это специальные программы, которые генерируют, хранят и управляют вашими паролями в одном безопасном онлайн-аккаунте. Так, вам придётся запомнить только один сложный пароль — мастер-пароль от хранилища, где будут собраны все ваши пароли

* Храните пароли в тайне

Не сохраняйте их «на листочке» на видном месте, не отправляйте через текстовое сообщение или электронную почту. Даже если вы доверяете человеку, кто-то другой может завладеть и воспользоваться паролем в корыстных целях

1. **Как распознать звонок мошенника**

По данным МВД, за первое полугодие 2022 года телефонные мошенники похитили у россиян около 39 млрд ₽. Преступники постоянно придумывают новые способы обмана. Чтобы не попасться на их уловки, надо знать, как распознать мошенника и что делать при подобных звонках. Эти знания особенно важны для пожилых людей, поскольку именно они наиболее подвержены телефонному мошенничеству.

*Как распознать мошенников*

* Звонят со скрытого номера

Звонки из банка идут с официальных номеров, указанных на сайте или на банковской карте. Вам могут позвонить из конкретного отделения банка, номер будет федеральным или мобильным, но не скрытым.

* Спрашивают данные карты

Мошенники спрашивают конфиденциальные данные вашей карты: коды для подтверждения платёжных операций, CVC/CVV — три цифры с обратной стороны банковской карты, логины и пароли, код-пароль из смс к личному кабинету на сайте банка или в мобильном приложении

Настоящий сотрудник банка никогда не спросит секретные реквизиты карты, ПИН-коды и пароли, а номер карты и срок её действия знает из системы обслуживания клиентов

* Сообщают тревожную информацию

Мошенники нагнетают ситуацию, пытаясь вогнать жертву в панику, заставить действовать необдуманно, поспешно. В таком состоянии человек может поделиться с преступниками конфиденциальной информацией или перевести деньги на счёт обманщиков

Мошенники могут представиться сотрудниками банка и сообщить, что организация заблокировала счёт, начислила штраф за кредит или по карте проведена подозрительная операция. Представиться сотрудниками полиции, ФСБ, прокуратуры и запугать уголовным делом или сообщить о попавшем в беду родственнике. Под видом сотрудников Пенсионного фонда, Налоговой службы и даже Госуслуг запугивать отменой льгот, выплат и начислением штрафов

* Давят на вас

Мошенники всегда торопят, чтобы не дать жертве времени обдумать ситуацию. Чаще всего звонят поздно вечером, ночью или ранним утром в выходные дни, когда человек спит и не может быстро сориентироваться. В ходе звонка предостерегают от самостоятельных попыток разобраться с проблемой

* Сообщают о внезапном выигрыше

Мошенники сообщают о внезапном выигрыше в лотерею, предлагают прибыльную работу или беспроигрышные конкурсы. Взамен просят оплатить небольшой взнос — перевести на указанный счёт деньги или сообщить данные банковской карты

* Уговаривают открыть ссылку из смс

Во время разговора мошенники сообщают, что вам пришла ссылка в смс, и настойчиво уговаривают её открыть. Так злоумышленники хотят, чтобы под видом антивируса или другой полезной программы вы установили вредоносную программу. Это позволит мошенникам получить доступ к вашему смартфону и похитить данные или деньги, воспользовавшись мобильным банком, или подписать на платные рассылки

* Сбрасывают звонки

Мошенники звонят с неизвестного номера и сбрасывают звонок, чтобы вынудить жертву перезвонить на этот номер. Хитрость в том, что обратный звонок на подозрительный номер будет платным. Иногда мошенники оставляют сообщение в голосовой почте — это повышает шанс, что вы решите перезвонить

*Как защитить себя от мошенников*

* Не паникуйте
* Никогда не принимайте поспешных решений, особенно если они касаются ваших денег. Всегда берите паузу, чтобы разобраться в том, что происходит. Скажите, что перезвоните самостоятельно, и сразу завершите звонок. Иначе мошенники продолжат запугивать и давить на вас
* Если возникли сомнения в безопасности банковских счетов, позвоните в банк по номеру с официального сайта или с пластиковой карты. Обязательно расскажите оператору о звонке мошенника и о том, что вы ему сообщили. При необходимости оператор заблокирует вашу карту или приостановит возможность проведения операций в интернет-банке
* Не перезванивайте по номеру, с которого совершался звонок. Даже если он отображается как официальный номер организации, это может быть маскировка мошенников. Номер нужно набрать вручную
* Не сообщайте логины и пароли от аккаунтов, платёжные данные, одноразовые коды из смс
* Единственная ситуация, при которой требуется назвать устно одноразовый код, — личное обслуживание в банке или в магазине. Когда нужно подтвердить операцию, например выдачу банковской карты или списание бонусов программы лояльности
* Установите программу или подключите сервис определения номеров мошенников у мобильного оператора или в банковском приложении
* Эти сервисы распознают и блокируют звонки мошенников, в том числе замаскированные под официальные номера банков и ведомств. Номер проверяется в базе, и во время звонка высвечивается информация о том, кто вам звонит. Однако помните, что базы операторов не всегда обновляются автоматически, поэтому регулярно обновляйте их вручную и не теряйте бдительности
* Не переводите деньги на счета, номера которых вам называют по телефону
* Никакого «резервного счёта», который позволит спасти ваши деньги, не существует. Это счёт мошенников, и вы добровольно переведёте им свои деньги
* Нельзя переводить деньги «сотруднику полиции», который обещает решить проблемы попавшего в неприятную ситуацию родственника. Даже если у ваших родных действительно возникли проблемы с законом, решать их нужно легальным путём
* Не переходите по ссылкам, которые присылают во время звонка
* Не устанавливайте навязываемые приложения: никаких «специальных антивирусов» не существует. Всю необходимую информацию можно найти на официальных сайтах банков, а безопасные программы ищите в магазинах приложений — у них строгая модерация, рейтинг, статистика по количеству скачиваний и отзывы пользователей

1. **Как защитить мобильное устройство**

Киберпреступники постоянно охотятся за чужими личными данными. Часто их целью является секретная информация из смартфонов: номера карт, доступы к онлайн-банкам, домашний адрес, рабочие документы и личные фото. Рассказываем, как защитить свой телефон от действий злоумышленников

*Какие бывают угрозы*

* Случайный доступ

При использовании одного устройства несколькими членами семьи следует контролировать доступ к конфиденциальной информации. Не разрешайте ребёнку использовать устройство, на котором хранится важная информация, а также установлены приложения мобильного банка, почты и другие

* Кража

Если у вас украли смартфон, потери могут не ограничиться самим телефоном. Вор может получить доступ к вашим аккаунтам, которые привязаны к устройству. Воспользоваться мобильным банком и вывести с ваших счетов все доступные деньги. Использовать для шантажа и вымогательства вашу личную информацию — рабочие документы, фото, переписки в мессенджерах и соцсетях

* Действия хакеров

Киберпреступники атакуют смартфоны с помощью вредоносных программ или файлов с вирусами, получают удалённый доступ к гаджетам и крадут с них секретные данные. Такая ситуация опаснее реальной кражи устройства — человек может не подозревать, что его информацию похитили

*Как защитить устройство на случай кражи*

* Настройте блокировку экрана

Для защиты устройства включите автоматическую блокировку экрана. Для разблокировки используйте длинные пароли и сканер отпечатка пальца. Графический ключ легко подглядеть из-за плеча и несложно подобрать — люди рисуют слишком очевидные траектории

* Защитите паролем или отпечатком пальца важные приложения и файлы

Это станет дополнительным фактором защиты и не позволит вору быстро попасть в банковские приложения, диспетчер файлов, галерею, почту, ваши аккаунты в социальных сетях

* Настройте отслеживание

Установите программу, которая удалённо блокирует телефон. Такие приложения определяют местоположение устройства, включают сирену, фотографируют злоумышленника, а также стирают все личные данные

На мобильных устройствах по умолчанию установлена функция «Найти устройство», которая позволяет также удалённо заблокировать смартфон и удалить с него все данные. Убедитесь, что функция не отключена. Чтобы не потерять свои данные, регулярно делайте резервные копии. Важно, чтобы эти копии хранились в недоступном для злоумышленников месте, например на съёмном диске

* Скачивайте только проверенные приложения

Злоумышленники распространяют вредоносные программы под видом игр и полезных приложений. Загружайте приложения только из официальных магазинов: здесь строгая модерация, рейтинг, статистика по количеству скачиваний и отзывы пользователей

Если необходимо установить приложения банков, попавших под санкции, скачайте их с официальных сайтов организаций

* Не переходите по подозрительным ссылкам

Чтобы заразить телефон вирусом, злоумышленники часто рассылают письма и сообщения с информацией о выигрыше, выгодной акции. При переходе по ссылке из такого сообщения на смартфон может загрузиться вредоносная программа. Если случайно перешли и файл загрузился, ни в коем случае не открывайте его и удалите

* Установите антивирус на смартфон

Антивирусы смогут обнаружить вредоносную программу, если она уже оказалась на устройстве. Защитные системы блокируют переходы на заражённые сайты, проверяют ссылки, которые приходят в смс и мессенджерах, выявляют небезопасные настройки на смартфоне. Не забывайте периодически обновлять антивирус

* Не давайте приложениям лишних разрешений

Не разрешайте приложениям, например планировщику дел или фонарику, получать доступ к камере, файлам на устройстве, совершению звонков, отправке смс. Если приложение получает подобные разрешения, оно сможет пользоваться этими функциями без вашего ведома — отправлять ваши фотографии на сервер злоумышленников или подписывать на платные рассылки. Разрешения приложений можно проверить в общих настройках телефона

* Постоянно обновляйте систему

Киберпреступники ищут уязвимости в программном обеспечении и приложениях, поэтому разработчики программ регулярно выпускают обновления, исправляют ошибки и уязвимости. Включите автоматические обновления операционной системы в установленных приложениях. Если обновления не устанавливать, устройство будет хуже защищено от новых киберугроз

* По возможности откажитесь от бесплатного вайфая

Публичные сети могут быть недостаточно защищёнными. Злоумышленники взламывают и перехватывают трафик, который идёт с вашего устройства. В их руках окажутся секретные данные, в том числе логины и пароли от различных аккаунтов. Кроме того, мошенники могут сами размещать точки доступа и выдавать их за бесплатный вайфай в парках, кафе и торговых центрах.

Социальный педагог Д.Б. Заплавина