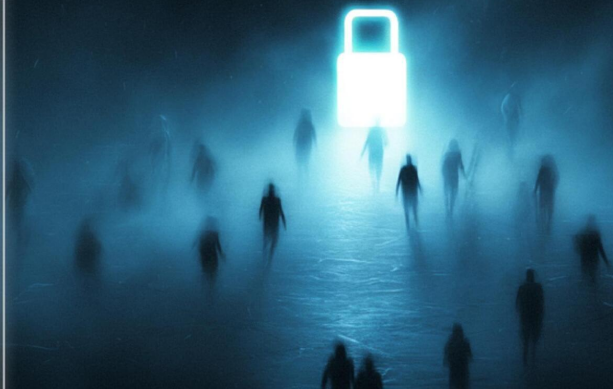
Личная кибербезопасность



Как не стать жертвой онлайн-мошенников

Артем Демиденко ии

Артем Демиденко

Личная кибербезопасность: Как не стать жертвой онлайн-мошенников

http://www.litres.ru/pages/biblio_book/?art=71979472
SelfPub; 2025

Аннотация

«Личная кибербезопасность: Как не стать жертвой онлайн-мошенников» – это ваш надежный путеводитель в мире цифровых опасностей. От социальных инженерных атак и фишинга до безопасности мобильных устройств и защитных механизмов банковских данных – эта книга откроет вам секреты эффективной защиты в интернете. Вы узнаете, как создавать надежные пароли, настроить многофакторную аутентификацию, обезопасить личные данные в социальных сетях и уберечь детей от киберугроз. Практические советы и разъяснения сложных понятий помогут сформировать крепкие привычки цифровой гигиены, чтобы онлайн-пространство стало действительно безопасным и комфортным. Не позволяйте мошенникам управлять вашей жизнью – вооружитесь знаниями и защитите себя! Обложка: Midjourney – Лицензия

Содержание

Введение в основы личной кибербезопасности	4
Социальная инженерия: манипуляции и способы распознавания	8
Фишинговые атаки: как их определить и обезопаситься	12
Надежные пароли: создание, хранение, использование	17
Многофакторная аутентификация: почему это важно	21
Безопасность электронной почты и вложенных файлов	24
Опасности при работе с публичными Wi-Fi сетями	28
Безопасность мобильных устройств и приложений	32
Конец ознакомительного фрагмента.	36

Артем Демиденко
Личная кибербезопасность: Как не стать жертвой онлайн-мошенников

Введение в основы личной кибербезопасности

Начинать разговор о личной кибербезопасности стоит с понимания, что это не абстрактные правила, а набор конкретных действий, которые мы выполняем ежедневно – чаще всего даже не замечая этого. Представьте, что ваша цифровая жизнь – это дом. Ключ, окно, почтовый ящик и сигнализация – все это элементы вашей защиты в интернете. Каждый из них требует внимания. Например, если вы используете простой пароль, словно прячете ключ под коврик – злоумышленник его обязательно найдет.

Один из главных принципов – правильное управление паролями. Всегда создавайте уникальные пароли для разных аккаунтов. Известны случаи, когда один простой пароль открывал мошенникам доступ к сотням учетных записей – от почты до онлайн-банка. Чтобы этого избежать, пользуйтесь

программами для хранения паролей, например, Bitwarden или 1Password. Они сгенерируют и сохранят сложные пароли, избавляя вас от необходимости держать их в памяти. Совет на практике: придумайте главный пароль из фразы длиной минимум 12 символов – например, возьмите любимую цитату и используйте первые буквы каждого слова, добавив цифры и знаки.

Двухфакторная аутентификация – вторая линия защиты. Исследования Google показывают, что её включение снижает риск взлома почти на 100%. Используйте приложения-аутентификаторы (Google Authenticator, Authy), а не только СМС – они уязвимы к подмене SIM-карты. Конечно, двухфакторная проверка не даёт стопроцентной гарантии, но значительно укрепляет ваши аккаунты. К примеру, когда мошенник попытался войти в почту известного блогера, именно она помешала взлому, хотя пароль был верным.

Еще одна важная тема – обновление программ. Новые версии часто закрывают критические уязвимости, которыми пользуются злоумышленники. Вспомните вирус WannaCry в 2017 году, который заразил тысячи компьютеров из-за устаревших версий Windows, которые не обновляли вовремя. Чтобы не попасть в такую ситуацию, включите автоматическое обновление – так ваш браузер, система и антивирус всегда будут в актуальном состоянии. Не игнорируйте сообщения о безопасности – они редко бывают лишними.

Внимательность в повседневном использовании – ещё

один ключевой элемент. Если приходит подозрительное письмо или сообщение, даже если оно кажется официальным, лучше проверить источник. Быстрая проверка адреса отправителя или звонок в организацию поможет избежать обмана. Например, мошенники часто шлют «письма от банка», требуя срочно подтвердить личные данные. Настоящий банк не делает так. Используйте специальные расширения для браузера, например Netcraft Anti-Phishing – они автоматически блокируют подозрительные сайты.

Не менее важно правильно обращаться с устройствами и сетью. Обязательно пользуйтесь виртуальной частной сетью (VPN), когда подключаетесь к общественному Wi-Fi. Без VPN ваши данные могут перехватить, даже если сайт кажется безопасным. Если вы пользуетесь интернетом в кафе или аэропорту, подключайтесь к проверенным сервисам, например ProtonVPN или NordVPN – ваш трафик будет надёжно зашифрован, и никто не получит доступ к паролям или банковским данным.

Наконец, обратите внимание на мультимедийный контент и разрешения в приложениях. Многие устанавливают программы из официальных магазинов, не задумываясь, что доступ к камере, микрофону или контактам могут открыть злоумышленникам. Проверяйте хотя бы раз в месяц настройки на смартфоне: отключайте лишние разрешения, удаляйте ненужные приложения. Это значительно снижает риски. Современные технологии могут следить за местоположени-

ем или собирать данные без вашего ведома.

В итоге личная кибербезопасность – это сочетание технических решений и бдительности. Уникальные пароли, двухфакторная аутентификация, своевременные обновления и осторожность в действиях – вот что создаёт надёжную защиту. Каждый простой шаг укрепляет ваш цифровой иммунитет, объединяя все меры в одно прочное звено. Начните уже сегодня применять хотя бы три из этих советов – и кибермошенникам придётся несладко.

Социальная инженерия: манипуляции и способы распознавания

Когда речь заходит о личной кибербезопасности, важно понять: опасность исходит не всегда от хитрых взломов и автоматических атак. Гораздо чаще слабое звено – это человек. Именно на ваше доверие, рассеянность и спешку нацеливается социальная инженерия – умение манипулировать сознанием, чтобы выудить нужную информацию или получить доступ к охраняемым ресурсам. Разобраться, как действует этот механизм, и научиться его распознавать – значит сделать огромный шаг к собственной цифровой безопасности.

Социальная инженерия – это не просто обман в интернете. Вспомните типичный случай: вам звонят и называют себя сотрудником службы технической поддержки, быстро рассказывают про сбой в почте и просят срочно назвать пароль или перейти по ссылке для восстановления доступа. Вы думаете: «Это же наши, почему сомневаться?» Вот именно этот момент становится входом в вашу цифровую «крепость». На практике бывали случаи, когда один такой фальшивый звонок давал мошенникам полный доступ к рабочей почте. Поэтому главная рекомендация – никогда не сооб-

щайте пароли по телефону или в письме.

Ещё один распространённый приём – мошеннические письма, замаскированные под сообщения от ваших банков, компаний или государственных служб. Здесь особенно важно уметь отличать настоящие письма от подделок. Представьте: вы получаете письмо с просьбой подтвердить платёж и ссылкой на «банк». Внешне письмо выглядит официально, но если присмотреться, адрес отправителя отличается на несколько символов, или доменное имя содержит лишние элементы, например, «.ru» вместо «.com». Практически совет: проверяйте адрес сайта не бегло, а внимательно, буква за буквой. Лучше всего вводить адрес вручную в браузере, а не переходить по ссылкам из писем.

Опасность социальной инженерии в том, что она использует психологию. Мошенники часто играют на чувствах спешки и страха. Письмо с предупреждением: «Ваш аккаунт заблокируют через 10 минут, если не подтвердите данные!» вызывает молниеносную реакцию. Чтобы не попасться, сделайте паузу перед любым быстрым действием – звонком, переходом по ссылке или скачиванием вложений. Проверьте информацию на официальных сайтах. Если действительно нужно действовать срочно, там обязательно будет об этом сообщение.

Интересный пример из жизни: мошенник звонит по телефону, представляясь коллегой из другого отдела. Он говорит спокойно, чтобы вызвать доверие, а потом просит со-

общить уникальный внутренний код или отправить важный документ. Чтобы не попасться, в коллективе стоит договориться: для передачи конфиденциальной информации требуется подтверждение личности через официальный канал – например, личный звонок на служебный номер.

Отдельного внимания заслуживают «ловушки доверия» в социальных сетях. Мошенники создают фальшивые аккаунты, входят с вами в контакт, задают личные вопросы, знакомятся и ждут момента, чтобы косвенно выудить нужные данные. Если вы выкладываете слишком много личной информации – даты рождения, место работы, имена родных – вы облегчаете им задачу. Сведите к минимуму открытые данные и используйте настройки доступа: не все должны видеть всё. Совет – регулярно проверять настройки приватности и помнить: если что-то кажется слишком личным, возможно, не стоит делиться этим даже с близкими.

Как отличить фальшивое сообщение от настоящего? Забудьте о старом правиле «письмо с ошибками – мошенник». Сейчас мошенники хорошо владеют языком. Доверяйте не только внешнему виду, но и содержанию. Постоянно задавайте себе вопросы: «Что от меня хотят? Какова цель этого сообщения? Как проверить его подлинность?» Если есть хоть малейшие сомнения – сделайте скриншот и проверьте через специальные базы подозрительных сообщений или обратитесь в официальные службы поддержки.

В итоге: социальная инженерия – это, прежде всего, иг-

ра с психологией и поведенческими шаблонами. Чтобы не попасть в ловушку, меняйте привычки: вместо автоматической реакции включайте осознанный контроль над каждой информацией и каждым действием. Ведите дневник подозрительных контактов, если нужно – делитесь сомнительными письмами с другом или коллегой, разбирайтесь в каждой ситуации спокойно и чётко. Ваш цифровой щит – это не только технические средства, но и внимание, готовность не дать мошенникам ни единого шанса.

Фишинговые атаки: как их определить и обезопаситься

Фишинг – это не просто технический термин, а одна из самых коварных и серьёзных угроз, с которой сталкивается каждый, кто пользуется интернетом. В предыдущей главе мы говорили о социальной инженерии, и фишинг – отличный пример такого обмана, когда злоумышленники играют на наших психологических реакциях. Теперь перейдём к сути: как эти атаки выглядят на практике, как их распознать и, главное, как не попасться на уловки мошенников.

Фишинг – это целенаправленные попытки выведать вашу личную информацию: пароли, банковские данные, номера карт, коды подтверждения и доступ к учётным записям. Всё это происходит под видом сообщений от якобы проверенных и надёжных организаций. Чаще всего это письма на электронную почту, но всё чаще фишинг встречается в смс, мессенджерах и даже по телефону. Представьте: вы получаете письмо от будто бы вашего банка с сообщением, что карта заблокирована из-за подозрительной активности, и предложением срочно перейти по ссылке для подтверждения данных. Если перейти – попадёте на ложный сайт, который практически не отличается от настоящего, и рискованно оставите там свои данные.

Распознать такие письма можно по ряду признаков, но совет «проверьте адрес отправителя» уже не так прост. Мошенники научились маскировать адреса так искусно, что они выглядят практически настоящими. Важно смотреть не только на адрес, но и на содержание письма. Часто в фишинговых сообщениях встречаются грамматические ошибки и странные выражения: «Уважаемый клиент, ваше акаунт будет заблокирован». Но даже если текст написан без ошибок, стоит задуматься – если вам внезапно требуют срочно что-то сделать без предварительного предупреждения, это серьёзный повод насторожиться.

Один из надёжных способов – не кликать по ссылкам в письмах, а самостоятельно вводить адрес сайта в браузере или переходить через сохранённые закладки. Фишинг часто маскируется под акции или новости – например, «Вы выиграли приз! Нажмите здесь, чтобы получить». Настоящая компания не будет просить переходить по сомнительным ссылкам ради приза или чтобы решить проблемы с аккаунтом.

Обращайте внимание на адреса сайтов – мошенники подделывают их настолько, что они кажутся почти настоящими: bankofarnerica.com вместо bankofamerica.com или bank0famerica.com – с нулём вместо буквы. Внимательный взгляд на адрес перед вводом пароля может спасти вас от кражи данных.

Практический совет: включайте двухэтапную проверку

подлинности – это значительно снижает риск взлома даже при похищении пароля. Особенно опасны ситуации, когда на одном устройстве включён автозапуск логинов, и преступники получают доступ к почте, чтобы восстановить остальные пароли. Двухэтапная проверка требует дополнительного подтверждения – например, код из смс, уведомление в приложении или физический ключ.

Для дополнительной защиты установите специальные расширения для браузера, которые в реальном времени проверяют ссылки на фишинговые сайты. Например, расширения от Google Safe Browsing или Bitdefender TrafficLight анализируют адрес и предупреждают о подозрительных ресурсах. Современные почтовые программы, как Outlook и Gmail, тоже автоматически фильтруют фишинговые письма, но полностью полагаться на них не стоит.

Никогда не отвечайте на письма с подозрительными просьбами – не отправляйте пароли, коды подтверждения или другую личную информацию. Продвинутые мошенники могут просить об этом, выдавая себя за внутреннюю проверку. В реальной жизни ни одна серьёзная организация не станет требовать пароль по электронной почте.

Если возникли сомнения – связывайтесь напрямую с организацией по официальным телефонам или через проверенный сайт. Особенно это важно, когда речь идёт о банках, операторах связи или соцсетях. Такая простая проверка не раз спасала сотни тысяч людей от серьёзных потерь.

Вот пример: однажды человек получил письмо от «службы поддержки» своего интернет-провайдера с сообщением о повышении тарифа и просьбой перейти по ссылке, чтобы подтвердить новые условия. Письмо выглядело очень убедительно и было даже адресовано по имени. Но внимательный пользователь заметил лишние символы в ссылке, не нажал на неё и позвонил в службу поддержки. Там подтвердили, что ничего подобного не рассылали – это был фишинг.

Ещё одна распространённая опасность – вложения с вредоносными программами, которые запускаются при открытии файла, например, Excel с макросами. Чтобы не рисковать, не скачивайте и не открывайте такие файлы от незнакомцев или подозрительных отправителей. Если файл пришёл от знакомого, но без пояснений, лучше уточнить у него напрямую, что это и зачем.

И, наконец, учите себя и близких. Фишинг постоянно меняется, становится всё хитрее и изощрённее. Следите за новостями о новых методах мошенничества, проходите простые онлайн-курсы по цифровой безопасности, обсуждайте эти темы с друзьями и семьёй – так риски снижаются намного эффективнее, чем при отдельном чтении советов.

В итоге: всегда сомневайтесь, проверяйте адреса и ссылки, не вводите данные на подозрительных сайтах, используйте двухэтапную проверку и инструменты для автоматической проверки безопасности. Фишинг – это серьёзная угроза с реальными последствиями, и ваша бдительность – главный

щит в цифровом мире.

Надежные пароли: создание, хранение, использование

Мы все знакомы с понятием «надежный пароль», но как часто его действительно используют на практике? Отношение к паролям – это один из главных щитов, которые защищают ваш цифровой «дом» от злоумышленников. Если социальная инженерия и фишинг играют на психологии, то слабый пароль – простая техническая брешь, которую взломщики используют молниеносно и без лишних вопросов.

Давайте разберемся, как создаются пароли, которые действительно сложно взломать. Пример из жизни: многие выбирают что-то знакомое – дату рождения, имя питомца или просто слово «password». Атаки методом перебора по словарю, включающему миллионы таких общеизвестных слов, разрушают эти пароли за секунды. Сильный пароль – это сочетание случайных символов, цифр, заглавных и строчных букв, специальных знаков. Недостаточно просто «пароль123!», лучше взять что-то вроде «*7v$9mQrp*2f*. На реальном примере: после утечки данных крупной соцсети в 2019 году более 20% пользователей продолжали использовать пароли, которые можно было взломать за несколько секунд. Это говорит о том, что знание и осознанный подход к паролям пока не получили широкого распространения.

Второй важный момент – длина пароля. Чем длиннее, тем больше вариантов перебора придется перебрать злоумышленнику. Рекомендуется использовать пароли длиной не менее 12 символов. Почему? При атаках перебором время взлома экспоненциально растет с каждым дополнительным символом и превращается из часов и дней в годы и даже сотни лет. Например, пароль из 8 случайных символов можно взломать сравнительно быстро, а с каждым новым символом число возможных вариантов увеличивается примерно в 62 раза – если учитывать буквы и цифры. При добавлении специальных знаков эта цифра ещё больше растёт.

Как не запутаться в сотнях сложных паролей? Самое простое решение – использовать программы для хранения паролей. Это приложения или расширения для браузера, которые надёжно шифруют и хранят ваши пароли в одном месте. Например, такие программы, как Bitwarden, 1Password или Dashlane, позволяют создавать уникальные и случайные пароли для каждого аккаунта, а вам нужно запомнить только один «главный» пароль. Один знакомый IT-специалист рассказывал, что после перехода на менеджер паролей у него значительно снизился уровень стресса и улучшилась цифровая гигиена – ведь нет нужды записывать пароли на бумажках, которые потом часто теряются.

Однако важно помнить: никакой менеджер не защитит, если мастер-пароль будет слабым или если вы не включите двухэтапную проверку подлинности. Двухэтапная защита

– дополнительный уровень обороны, который, по статистике Microsoft, блокирует более 99,9% автоматических атак на аккаунты. При выборе менеджера обратите внимание, чтобы он поддерживал двухэтапную проверку и имел возможность работать с мобильными приложениями.

Особое внимание уделяйте паролям для важных сервисов: банковских аккаунтов, электронной почты и социальных сетей. Практика показывает, что взлом почты часто открывает доступ к восстановлению паролей во многих других сервисах, поэтому слабый пароль там – это огромный риск для всей вашей цифровой жизни. Совет простой: для каждой важной учётной записи используйте уникальный пароль и никогда не повторяйте его на разных сайтах.

Не забывайте регулярно менять пароли. При утечке данных или подозрении на взлом меняйте пароли сразу, не откладывайте. Многие думают: «Да это меня не коснется», но практика показывает обратное – сотни аккаунтов ежедневно становятся лёгкой добычей хакеров именно из-за промедления.

Наконец, помните: надежный пароль – это не обязательно случайный набор бессмысленных символов. Метод «фразового пароля» – длинной фразы из нескольких слов, которую легко запомнить, но которую сложно угадать – тоже работает отлично. Например, фраза «Завтрак_В_15_минут@Парк2024» сочетает в себе длину, разнообразие символов и личную значимость, что помогает запомнить и повышает без-

опасность. Главное – избегать очевидных фраз и клише, которые легко взламываются с помощью автоматического подбора или анализа профиля.

Итог прост: чтобы создать надежный пароль, нужно использовать длинные и разнообразные комбинации, включать специальные символы, не повторять пароли для разных сервисов, применять менеджеры паролей, менять их при подозрении на взлом и обязательно включать двухэтапную проверку. Тогда пароль перестанет быть просто набором символов и станет реальной защитой от большинства автоматических и целенаправленных атак. Такая практика спасает от ошибок в социальной инженерии и утечек, о которых мы говорили в предыдущих главах.

Многофакторная аутентификация: почему это важно

Если пароль – это ваша дверь, то многофакторная аутентификация (МФА) – это цепь и замок, которые делают эту дверь почти непроницаемой. Мы уже поняли, почему одних только надежных паролей часто мало. Теперь пришло время разобраться, как дополнительный уровень защиты меняет всю ситуацию.

Возьмём простой пример, чтобы показать преимущества МФА. Представьте, что злоумышленник каким-то образом получил ваш пароль – будь то через фишинговую ловушку или утечку данных. Без второго фактора он спокойно войдёт в ваши аккаунты и сможет навредить: украсть деньги, разослать спам от вашего имени. Но если у вас включена многофакторная аутентификация, то даже имея пароль, мошеннику придётся пройти ещё одно испытание, зачастую невозможное без вашего физического устройства или отпечатка пальца. Например, Google заявляет, что включение МФА снижает риск взлома аккаунта на 99,9%. Это не просто цифра – это разница между открытой дверью и надёжным замком.

Важно понять: МФА – это не одно универсальное решение, а целый набор методов, каждый со своими плюса-

ми и нюансами. Чаще всего используются три типа факторов: что-то, что вы знаете (пароль), что-то, что у вас есть (специальное устройство или приложение для кодов) и что-то, кем вы являетесь (биометрия). Такой подход называют «трёхфакторной аутентификацией». Например, приложения Google Authenticator или Authy каждую минуту создают одноразовые коды, которые нужно вводить вместе с паролем. Или аппаратные ключи, как YubiKey – эти устройства подключаются к USB-порту и работают по протоколам FIDO2/WebAuthn. Они особенно надёжны: украденный пароль или поддельный сайт тут не помогут.

Чтобы использовать МФА по максимуму, советую:

1. **Включайте МФА везде, где есть такая возможность.** Практически все популярные сервисы – почта, социальные сети, банки – уже поддерживают эту опцию. Обычно она спрятана в разделе «Безопасность» или «Учётная запись». Поставьте цель активировать МФА на всех важных платформах в течение недели – так вы сильно снизите риск взлома.

2. **Для особо ценных аккаунтов выбирайте аппаратные ключи безопасности.** Это надёжная защита. Банковские счета и рабочие учетные записи – идеальные кандидаты. В отличие от смс-кодов, которые можно перехватить, аппаратный ключ невозможно взломать удалённо.

3. **Настройте запасные способы доступа, но будьте осторожны.** Телефон или устройство могут потеряться –

на всякий случай сделайте резервные варианты, например, одноразовые коды. Но не используйте простые и ненадёжные методы вроде повторного приёма смс или восстановления через электронную почту – это слабые места.

4. **Обращайте внимание на уведомления о входе в аккаунт.** Многие сервисы присылают оповещения, если кто-то пытается войти, и просят подтвердить или отклонить попытку. Не игнорируйте такие сообщения – это ваше первое предупреждение о возможной угрозе.

Подводя итог, важно понять: многофакторная аутентификация – это не просто сложная технология и набор строгих правил безопасности. Это мощный инструмент, который уже сегодня может защитить вас от многих бед. Она сильно затрудняет жизнь злоумышленникам и часто становится последним рубежом, стоящим между ними и вашими данными. Настроить МФА занимает совсем немного времени, зато этот маленький шаг может уберечь вас от множества проблем – от обычных неудобств до серьёзных финансовых потерь и урона репутации.

В следующей главе мы поговорим о том, как правильно управлять своими устройствами и программами, чтобы не создавать новые уязвимости на телефоне, компьютере и домашней сети – ведь безопасность должна быть целостной. А пока не откладывайте настройку многофакторной аутентификации. Включить МФА сегодня – значит обеспечить себе спокойствие и уверенность завтра.

Безопасность электронной почты и вложенных файлов

Защита электронной почты – это не просто очередное правило из учебника по кибербезопасности. Это ваш главный рубеж, где борьба с угрозами начинается сразу после получения письма. Электронная почта – как парадная дверь в ваш цифровой дом, через которую пытаются проникнуть не только мошенники, но и вирусы, шпионские программы или трояны. Понимание того, как работают эти угрозы и как с ними справляться, поможет сделать вашу цифровую жизнь гораздо безопаснее.

Первое, на что стоит обратить внимание, – отправитель письма. Кажется очевидным, но именно здесь таится большая опасность. Мошенники давно научились подделывать адреса, делая их похожими на официальные контакты банков, служб доставки или даже ваших коллег. Простая проверка адреса, а не только поля «от кого» в заголовке, может спасти вас от неприятностей. Например, если письмо от банка приходит с домена вида banksecurety.com вместо banksecurity.com – это повод насторожиться. Настоятельно рекомендуем всегда сверять доменное имя, а при сомнениях – звонить в организацию напрямую. Никогда не переходите по ссылкам в таких письмах без проверки.

Вложения – отдельный источник опасности. Они могут содержать вредоносные программы, которые активируются при открытии. Особенно настороженно стоит относиться к файлам, которые приходят неожиданно или от малознакомых адресатов. Особое внимание уделяйте форматам .exe, .bat, .js, .scr, а также документам Office (.doc, .xls) с включёнными макросами. Макросы – старый, но всё ещё действенный способ запуска вредоносных программ. Например, одна крупная компания потеряла десятки тысяч долларов, когда сотрудник открыл файл с макросом, который установил программу для кражи нажатий клавиш. Чтобы избежать такого, отключите автоматический запуск макросов в офисных программах и открывайте вложения только после тщательной проверки.

Следующий шаг – использование антивирусных и антишпионских программ, которые интегрируются с почтовыми клиентами и автоматически проверяют входящие письма. Но не стоит полностью полагаться на них: новые виды атак бывают слишком изощрёнными для стандартных средств защиты. Поэтому комбинируйте технические инструменты с собственной внимательностью и осторожностью.

Если речь идёт о работе, часто применяются корпоративные почтовые системы с дополнительными уровнями защиты – например, шифрованием сообщений и вложений. Технологии типа S/MIME или PGP гарантируют, что даже если письмо попадёт к злоумышленнику, он не сможет прочитать

его без специального ключа. Важно, чтобы пользователь понимал, как пользоваться такими технологиями: ключи нужно хранить в надёжном месте, а при утрате ключа не следует пересылать важные документы без шифрования.

Особое внимание заслуживает фишинг, который чаще всего распространяется по электронной почте. Мошенники присылают письма с вложениями, будто это важные документы – счета, отчёты или квитанции. При этом само письмо часто написано наспех и с ошибками – сигнал беды. Учитесь распознавать стиль настоящих деловых писем: большинство компаний придерживается строгой формальности и не используют слишком общий или эмоциональный тон.

Практический совет на каждый день: привыкайте проверять письма в отдельном окне или в режиме чтения без возможности сразу запускать вложения. Многие почтовые сервисы, например Gmail, предлагают режим «только текст», который помогает избежать случайного запуска вредоносных программ.

Если часто открываете вложения на телефоне, помните: мобильные устройства менее защищены, и вредоносные программы могут проникнуть через них быстрее и незаметнее. В таких случаях лучше использовать специальные приложения для открытия документов, которые изолируют файлы от основной системы и не дают им излишних прав.

Наконец, не забывайте о резервном копировании. Даже при самой осторожной работе есть риск потери важных дан-

ных из-за вредоносного письма. Регулярные копии почты и ключевых файлов помогут быстро восстановиться и избежать серьёзных последствий.

В итоге, безопасность электронной почты – это цепочка из множества шагов: проверка отправителя, внимательная оценка вложений, использование защитных программ и шифрования, а также аккуратное обращение с письмами. Каждый такой шаг – маленький, но очень важный элемент, который вместе превращает вашу электронную почту из уязвимого канала связи в крепкую и надёжную защиту.

Опасности при работе с публичными Wi-Fi сетями

Публичные сети Wi-Fi – настоящая ловушка, маскирующаяся под удобство. В кафе, аэропорту или отеле вы подключаетесь к бесплатному интернету и чувствуете себя в безопасности, но на самом деле многие «бесплатные» точки доступа – золотая жила для мошенников. При работе с такими сетями важно помнить о рисках, которые новичкам часто остаются незаметными.

Главная опасность – так называемые атаки «человек посередине». Мошенник создаёт точку доступа с названием, похожим на официальное, например, «Cafe_Free_WiFi» становится «Cafe_Free_Wi-Fi» или «CafeFreeWiFi». Вы подключаетесь, думая, что пользуетесь настоящим интернетом, а весь ваш трафик проходит через злоумышленника. Вот пример из практики: в одном аэропорту мошенники развернули такую сеть и за несколько часов перехватили сотни учётных записей, включая пароли от банковских приложений. Чтобы избежать этого, всегда сверяйте название сети с информацией от сотрудников заведения, а лучше попросите пароль, если сеть защищена. Если же вы используете открытую сеть без пароля, стоит подумать о дополнительных мерах защиты.

В открытых Wi-Fi сетях трафик обычно не шифруется.

Без этого мошенник легко «подслушивает» ваши данные – от сообщений до реквизитов карты. Особенно уязвимы сайты и приложения на протоколе HTTP. Поэтому есть два простых правила: во-первых, используйте расширения для браузера, автоматически переключающие на защищённый протокол HTTPS. Во-вторых, всегда проверяйте адрес сайта – зелёный замок и начало с https:// должны быть на виду. Если их нет, не вводите личную информацию.

Для надежной защиты поможет виртуальная частная сеть (ВЧС, VPN). Она создаёт защищённый туннель, через который ваш трафик идёт в зашифрованном виде – атаки «человек посередине» теряют смысл. Но быть осторожным при выборе ВЧС очень важно. Бесплатные VPN часто сами следят за пользователями или продают их данные рекламе. Выбирайте проверенных провайдеров с хорошей репутацией и прозрачной политикой конфиденциальности. Отличный вариант – сервисы с открытым исходным кодом и аудитом безопасности.

Публичные Wi-Fi также используют для распространения вредоносных программ и фальшивых обновлений. Представьте: вы подключаетесь к сети, и вдруг система или браузер предлагает обновить Flash Player или антивирус – но на самом деле это замаскированные вирусы или майнеры. Известен случай, когда злоумышленники под видом обновлений заразили устройства и начали добывать криптовалюту. Решение – всегда загружайте обновления только с офици-

альных сайтов или через встроенные системные утилиты, а не из всплывающих окон в браузере.

Ещё один момент – автоматическое подключение устройств к знакомым сетям. Смартфоны и ноутбуки часто запоминают сети и подключаются к ним без вашего ведома. Это удобно, но даёт взломщикам возможность создать фальшивые точки доступа с теми же именами, чтобы ловить ваши данные. Чтобы защититься, отключите автоматическое подключение и сами выбирайте сеть, особенно в общественных местах.

Время подключения тоже играет роль. Многие остаются в сети после работы, забывая, что это оставляет путь для атак. Всегда отключайтесь от публичного Wi-Fi после использования и, если есть возможность, удаляйте эту сеть из памяти устройства. Так вы предотвратите случайное подключение и снизите риски.

Если пользование публичным Wi-Fi неизбежно, пересмотрите, какими приложениями пользуетесь. Не заходите в банковские и корпоративные сервисы напрямую через публичную сеть без ВЧС. Для важных операций лучше использовать мобильный интернет. Также включайте двухфакторную аутентификацию – даже если злоумышленник получит пароль, без дополнительного кода он не войдёт в аккаунт.

В итоге пренебрегать рисками публичного Wi-Fi – значит оставлять входную дверь в свой цифровой дом открытой. Вот простые правила:

1. Всегда уточняйте у сотрудников заведения название и параметры публичной сети.

2. Подключайтесь только к сетям с паролем и проверяйте адрес сайтов с HTTPS.

3. Используйте ВЧС только от надёжных провайдеров.

4. Никогда не запускайте обновления и не скачивайте файлы из непроверенных источников.

5. Отключите автоматическое подключение к сетям.

6. После использования удаляйте сеть из памяти устройства.

7. Ограничьте важные действия только надежными каналами и включайте двухфакторную аутентификацию.

Если следовать этим рекомендациям, вы значительно усложните жизнь мошенникам и сохраните контроль над своими данными, даже подключаясь к бесплатному Wi-Fi в любой точке мира.

Безопасность мобильных устройств и приложений

Мобильные устройства давно перестали быть просто средствами связи – сегодня это настоящие карманные компьютеры, в которых хранится огромное количество личной информации: переписки, банковские приложения, документы, фотографии. Соответственно, любая уязвимость телефона или планшета может стать лазейкой для мошенников. Начнём с основ: мобильная безопасность – это не кнопка «включить», а набор мер, адаптированных под ваш стиль использования. Рассмотрим ключевые моменты на конкретных примерах.

Первое и главное – защита доступа к устройству. Многие до сих пор используют только простой свайп или графический ключ, который легко подглядеть. В 2019 году исследование специалистов компании Zimperium показало, что более 30% пользователей Android применяют стандартные жесты или вовсе не блокируют экран. Решение очевидно: выберите надёжный PIN-код или современный биометрический способ – отпечаток пальца или сканирование лица. Но и тут есть нюанс: системы распознавания должны быть многоуровневыми. Например, Face ID на последних моделях Apple анализирует глубину и тепловой отпечаток лица, чтобы предотвратить подделку фотографией. Если ваше устрой-

ство поддерживает сканирование радужной оболочки глаза (как в некоторых моделях Samsung), лучше воспользоваться именно этим – это технологически более надёжный вариант.

Следующий важный момент – обновления операционной системы и программ. Пример из жизни: в 2021 году на Android появилась волна вредоносных программ, распространявшихся через поддельные обновления. Пользователи, игнорируя системные сообщения, скачивали апдейты из непроверенных источников, открывая путь троянам. Помните: официальные обновления не только приносят новые функции, но и устраняют уязвимости, которые находят злоумышленники. Автоматическая установка последних исправлений – ваша лучшая защита. Совет простой: отключите возможность установки приложений из сторонних источников и проверяйте обновления каждый день. Если устройство больше не получает обновления системы, задумайтесь о замене – устаревшая ОС становится лёгкой добычей для атак.

Теперь поговорим о приложениях – самой уязвимой части мобильной безопасности. Представьте: вам прислали ссылку на бесплатное приложение для управления финансами. Вы скачиваете, даёте все разрешения – камера, микрофон, доступ к контактам, а на деле программа шпионит и собирает ваши данные. В 2022 году аналитики Google Play выявили около 150 опасных приложений, замаскированных под привычные программы, которые воруют пароли и номера банковских карт. Чтобы не попасть в ловушку, избегайте

установки из непроверенных магазинов – Amazon Appstore, APKPure и им похожих. Если у вас Android, пользуйтесь только Google Play с включённой функцией Play Protect; для iPhone – только App Store. Перед установкой обратите внимание на количество скачиваний, рейтинг, отзывы и особенно на список запрашиваемых прав. Если калькулятор просит доступ к микрофону и геолокации – это повод насторожиться. Практический совет: зайдите в настройки устройства и отключите у приложений сомнительные разрешения. Запустите программу, затем в меню «Разрешения» или «Приложения» уберите лишние доступы.

Работа с банковскими приложениями требует отдельного внимания. По данным Федерального агентства по кибербезопасности, свыше 60% случаев финансовых мошенничеств связаны с взломом мобильных устройств. Например, мошенник может отправить SMS с подозрительной ссылкой для обновления мобильного банка или под видом уведомления попросить войти в аккаунт. Практика показывает: никогда не переходите по неизвестным ссылкам из сообщений и не вводите личные данные вне официального приложения или сайта. Пользуйтесь только проверенными каналами загрузки и настройками уведомлений – любые подозрительные запросы блокируйте. Кроме того, включите в смартфоне функцию оповещений о подозрительной активности – многие банки предлагают встроенную защиту или собственные антивирусные решения. Если возможно, установите лимиты на опера-

ции и активируйте одноразовые коды подтверждения.

Не менее важно настроить резервное копирование данных. Представьте, что вы потеряли или у вас украли телефон. Первое желание – мгновенно удалить всё, чтобы злоумышленник не получил доступ к вашим файлам. В Android и iOS это реализовано через удалённое стирание данных («Найти устройство» и «Найти iPhone»). Настройте эти функции заранее. Для резервных копий используйте облачные сервисы с многофакторной защитой, например Google Диск или iCloud. Но будьте внимательны: храните только самое необходимое и тщательно защищайте аккаунты.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, купив полную легальную версию на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.