Контур Эгида

7 способов

защитить личное устройство
от взлома и атак

Про какие способы расскажем:

1. Включить двухфакторную защиту там, где она нужна.
2. Обновлять ПО по-умному.
3. Быть внимательнее в публичных сетях.
4. Правильно скачивать приложения и файлы.
5. Распознавать фишинговые атаки как профессионал.
6. Настроить резервное копирование, которое спасёт в критический момент.
7. Защищать устройство от доступа посторонних.

Способ 1. Включить двухфакторную защиту там, где она нужна

Пароль из 12 символов с заглавными буквами и специальными знаками может оказаться бесполезным — при утечке базы данных хэши сложных паролей расшифровываются за считанные часы. А если вы используете один и тот же пароль на разных сайтах, то взлом одного ресурса открывает двери ко всем остальным.

Двухфакторная аутентификация (2FA) должна быть настроена для:

— электронной почты, особенно если она привязана к финансовым сервисам,

— банковских приложений и платёжных систем,

— облачным хранилищам с рабочими документами,

— аккаунтов в социальных сетях, если вы ведёте через них бизнес.

При этом в малозначимых сервисах — новостных подписках, форумах по интересам или сайтах со статьями — 2FA может быть избыточной и только затруднит использование.

Важно понимать, что СМС как второй фактор аутентификации — самый уязвимый вариант. Перехват сообщений через подмену сим-карты или перенаправление — распространённая практика. Намного надежнее использовать приложения-аутентификаторы, например ID от Контур.Эгиды.

Способ 2. Обновлять ПО по-умному

Сообщения об обновлениях часто игнорируют, особенно когда они приходят в неподходящее время. Но именно обновления закрывают уже известные уязвимости, которыми могут воспользоваться злоумышленники. Не каждое обновление одинаково важно.

Косметические улучшения и новые функции можно отложить, если они не критичны для работы, а вот чему нужно отдавать приоритет:

- обновлениям безопасности операционной системы
- патчам для браузеров и почтовых клиентов
- исправлениям в приложениях с доступом к личным данным и финансам

Автоматические обновления стоит настроить на время, когда устройство меньше всего загружено — например, ночью для компьютера или во время обеденного перерыва для смартфона. В Windows 10/11 и macOS можно указать активные часы, когда система не будет запускать перезагрузку после установки обновлений. В Android и iOS имеет смысл включить опцию обновления только через Wi-Fi и при подключённой зарядке.

Способ 3. Быть внимательнее в публичных сетях

Беспроводные сети в общественных местах — аэропортах, кафе, отелях — могут представлять риск для пользователей. При подключении к публичному Wi-Fi старайтесь:

- Использовать VPN-сервис для шифрования всего интернет-трафика — это создаст защищённый туннель даже в ненадёжной сети;
- Проверять наличие HTTPS-соединения (значок замка в адресной строке браузера) перед вводом любых данных;
- Включить двухфакторную аутентификацию на важных сервисах — это защитит аккаунт даже при перехвате пароля;
- По возможности использовать мобильный интернет для банковских операций и других важных действий;
- Не передавать конфиденциальную информацию в незашифрованном виде.

VPN (виртуальная частная сеть) шифрует трафик и помогает защититься от перехвата данных в публичных сетях. Но не все VPN-сервисы одинаково полезны — бесплатные решения могут сами собирать ваши данные и продавать их третьим лицам. Выбирайте проверенные платные VPN-сервисы вместо бесплатных. Один из вариантов — Коннект от Контур.Эгиды.

Настройка домашнего роутера — тоже важный элемент безопасности. Что необходимо сделать в первую очередь:

- изменить стандартный пароль администратора,
- создать сложный пароль для Wi-Fi,
- отключить WPS (Wi-Fi Protected Setup) — эта функция повышает удобство подключения, но снижает безопасность,
- обновить прошивку роутера до последней версии,
- настроить гостевую сеть для случайных посетителей, чтобы они не получали доступ к вашим домашним устройствам.

Способ 4. Правильно скачивать приложения и файлы

Альтернативные магазины приложений и сайты с «бесплатными» версиями платных программ — прямой путь к заражению устройства. Экономия в несколько сотен рублей может обернуться потерей сотен тысяч. Официальные магазины (App Store, Google Play, Microsoft Store, Ru Store) проверяют приложения на вредоносный код, хотя и эта система не идеальна.

При установке приложений обращайте внимание на запрашиваемые разрешения. Приложение-фонарик, которое требует доступ к контактам, камере, микрофону и геолокации, определённо хочет больше, чем просто светить. Простое правило: если функционал приложения не связан с запрашиваемым разрешением — отказывайте.

Файлы, полученные через мессенджеры, заслуживают особого внимания. Даже от доверенных контактов могут прийти опасные вложения, если их аккаунт был взломан. Правило безопасности для мессенджеров:

- не открывайте неожиданные вложения (особенно с расширениями.exe,.bat,.cmd, apk) — лучше сначала спросите отправителя о содержимом файла перед открытием, убедитесь, что человек не взломан;
- проверяйте подозрительные файлы через онлайн-сканеры, например Касперский или Dr.Web, перед открытием.

Способ 5. Распознавать фишинговые атаки как профессионал

Фишинговые письма становятся все более правдоподобными. Современные мошенники используют точные копии сайтов банков, корректную грамматику и персонализацию обращений.

Чтобы распознать подделку:

- Проверяйте адрес отправителя полностью, а не только отображаемое имя. Мошенники используют домены, похожие на настоящие: вместо support@sberbank.ru может быть support@sber-bank.ru или support@sberbank.org.
- Наведите курсор на ссылку, не нажимая на неё — в большинстве почтовых клиентов это покажет реальный адрес, куда ведёт ссылка.
- Обращайте внимание на давление и срочность — требование «немедленно действовать» — обычно признак мошенничества.
- Помните, что банки никогда не запрашивают полные данные карт, CVV-коды или одноразовые пароли по электронной почте.

Распространённый в последнее время кейс: топ-менеджер крупной компании получает письмо якобы от коммерческого директора с просьбой срочно оплатить счёт нового подрядчика. Поддельная почта отличалась от настоящей одним символом, а спешка и авторитет «начальника» заставляют человека действовать без проверки. Результат — перевод значительной суммы мошенникам.

СМС часто используются для фишинга, так как выглядят более личными и вызывают меньше подозрений.

Правила безопасности:

- не переходите по ссылкам из СМС от незнакомых отправителей;
- если сообщение якобы от вашего банка или госоргана, проверьте информацию через официальное приложение или позвоните по номеру с официального сайта;
- проверяйте URL перед вводом любых данных — фишинговые сайты могут отличаться одной буквой или дополнительным дефисом.

Способ 6. Настроить резервное копирование, которое спасёт в критический момент

Резервное копирование — не просто удобство, а важнейший элемент безопасности. При заражении программами-вымогателями, которые шифруют данные и требуют выкуп, только резервная копия может спасти информацию без потерь.

Правило 3–2–1 для надёжного резервного копирования:

3 копии данных (оригинал + две резервные),

2 разных типа носителей, например, внешний жёсткий диск и облако,

1 копия хранится удалённо, например в другом помещении или облачном сервисе).

Необязательно самому регулярно создавать копии — настройте автоматическое резервирование на своём устройстве:

- На Windows — встроенную функцию «История файлов»
- На macOS — Time Machine с внешним накопителем
- На Android — резервное копирование в Google Drive или Яндекс.Диск
- На iOS — iCloud Backup или локальные копии через iTunes/Finder

Важно защитить резервные копии отдельным паролем — иначе злоумышленник, получивший доступ к вашим бэкапам, получит все данные.

Способ 7. Защищать устройство от доступа посторонних

Биометрическая защита удобна, но не всегда безопасна. Отпечаток пальца можно получить с поверхностей, которых вы касались, а распознавание лица в некоторых системах обманывается фотографией. Используйте отпечатки и FaceID для повседневной защиты, но для критически важных приложений (банковских, корпоративных) дополнительно требуйте ввод пароля.

Время автоблокировки устройства — важный параметр безопасности. Компромисс между удобством и защитой:

- для личного смартфона — 1-3 минуты
- для рабочего компьютера — 5-10 минут
- для устройств с конфиденциальными данными — не более 1 минуты

Что делать, если вас все-таки взломали

Если обнаружили взлом, не паникуйте — действуйте по плану:

1. Отключите устройство от интернета: включите авиарежим или отсоедините кабель.
2. Смените пароли к важным сервисам с другого, незараженного устройства.
3. Проверьте выписки по банковским счетам и историю операций.
4. Сообщите контактам о возможной компрометации, если через ваши аккаунты отправлялись сообщения.
5. Выполните полный сброс устройства до заводских настроек после сохранения важных данных.
6. Восстановите данные из резервной копии, созданной до взлома.

Три настройки, которые можно сделать прямо сейчас:

- Включите двухфакторную аутентификацию для электронной почты.
- Настройте автоматическое резервное копирование важных данных.
- Проверьте настройки конфиденциальности на смартфоне и отключите лишние разрешения для приложений.

Самое время защитить свой бизнес

kontur.ru/aegis →

16+. АО «ПФ «СКБ КОНТУР». ОГРН 1026605606620. 620144, ЕКАТЕРИНБУРГ, УЛ. НАРОДНОЙ ВОЛИ, 19А.