

Цифровой след человека: что остается в сети после каждого клика

Утро для многих начинается не с завтрака, а со смартфона. Проверить сообщения, почту и соцсети, посмотреть баланс карты, оплатить покупку, вызвать такси. В течение дня к этому добавляются рабочие документы, онлайн-сервисы, маркетплейсы, банковские приложения, а вечером фильмы, игры и общение в мессенджерах.

Значительная часть нашей повседневной жизни переместилась в онлайн. Вместе с удобством туда же переместились деньги, документы, фотографии, переписка, рабочая информация и множество других данных.

Поэтому кибербезопасность давно перестала быть исключительно задачей IT-специалистов. Сегодня она начинается с повседневных привычек каждого из нас.

Один пароль на все – удобно, но рискованно

Почта, социальные сети, маркетплейсы, государственные сервисы - аккаунтов сегодня становится все больше. Поэтому знакомая ситуация: один удобный пароль используется сразу в нескольких местах, иногда годами.

Проблема возникает, если данные одного из сервисов окажутся скомпрометированы. Получив логин и пароль, злоумышленники могут попробовать эту же комбинацию для входа в другие аккаунты.

Для важных сервисов используйте **разные сложные пароли**, а где возможно - двухфакторную аутентификацию.

Особенно внимательно **стоит защищать электронную почту**. Именно через нее часто восстанавливается доступ к другим сервисам. Получив контроль над почтовым ящиком, злоумышленник может попытаться получить доступ и к связанным с ним аккаунтам.

«Вам пришла посылка». А вы точно ее ждали?

Кибератака не всегда начинается со взлома устройства. Иногда гораздо проще заставить человека самого предоставить необходимые данные.

«Ваша посылка задержана». «На ваше имя оформлен кредит». «Проголосуйте за моего ребенка». «Руководитель просит срочно открыть документ». «Покупатель уже оплатил товар — получите деньги по ссылке». Сценарии постоянно меняются, но цель остается прежней: заставить человека **перейти по ссылке, открыть файл, установить программу, ввести данные или сообщить код подтверждения**.

Поэтому полезно выработать простую привычку: сначала проверить, потом действовать.

Если сообщение пришло якобы из банка - самостоятельно откройте банковское приложение или позвоните по официальному номеру. Пишет служба доставки - проверьте заказ через ее официальный сервис. Знакомый пишет и просит деньги - свяжитесь с ним самостоятельно.

В цифровой среде несколько секунд на проверку иногда имеют гораздо большую ценность, чем кажется.

Социальные сети знают о нас больше, чем кажется

Мы ежедневно **оставляем цифровой след** и часто сами предоставляем значительную часть информации о себе. Дата рождения, место работы, фотографии из отпуска, геолокация, школа ребенка, автомобиль, круг общения - по отдельности эти сведения могут казаться совершенно безобидными.

Но собранные вместе они способны дать достаточно подробное представление о человеке. Этим могут воспользоваться мошенники, чтобы сделать звонок или сообщение более убедительными.

Иногда полезно открыть свой профиль и посмотреть на него глазами незнакомого человека: что он сможет узнать о вас, вашей семье, работе, привычках и текущем местонахождении?

Это не означает, что нужно отказываться от социальных сетей. Достаточно осознанно выбирать, **какой информацией вы делитесь, с кем и в какой момент**

«Разрешить доступ?»: не нажимайте автоматически

Камера, микрофон, контакты, фотографии, геолокация: приложения регулярно запрашивают доступ к данным и функциям смартфона. Мы настолько привыкли к кнопке «Разрешить», что иногда нажимаем ее автоматически. Но приложению-фонарику вряд ли нужны ваши контакты, а простой игре - постоянный доступ к геолокации.

Поэтому, периодически **проверяйте разрешения установленных приложений** и отключайте те, которые не нужны для их работы. Сами приложения лучше устанавливать из официальных источников, а операционную систему и программы своевременно обновлять.

Обновление - это не только новые функции и дизайн. Оно может содержать исправления выявленных уязвимостей.

На работе личная невнимательность может стать общей проблемой

Рабочая кибербезопасность **начинается с таких же повседневных действий.**

Пришло необычное письмо от руководителя. Коллега просит пароль. Рабочий документ удобнее переслать на личную почту и закончить дома. Компьютер остается разблокированным, пока вы вышли за кофе. Каждая ситуация по отдельности кажется мелочью. Но рабочий аккаунт может **открывать доступ к документам**, внутренним системам, переписке и данным других людей.

Поэтому рабочие документы лучше не переносить в личные сервисы без необходимости, учетные данные никому не передавать, а компьютер блокировать, когда отходите от него.

И особенно внимательно относиться к необычным просьбам, сопровождаемым словами «срочно», «никому не говорите», «откройте сейчас», «пришлите код».

Даже если сообщение выглядит так, будто его отправил руководитель или коллега, необычную просьбу лучше дополнительно проверить.

Бесплатный Wi-Fi тоже требует осторожности

Аэропорт, торговый центр, гостиница, кафе: бесплатные сети удобны, особенно когда мобильный интернет недоступен. Но проводить через открытую сеть важные финансовые операции или работать с конфиденциальными документами не стоит.

Если необходимо открыть банковское приложение или передать чувствительные данные, безопаснее использовать мобильный интернет или доверенную сеть.

Полезно также **отключить автоматическое подключение смартфона** к незнакомым Wi-Fi-сетям. Само название сети еще не гарантирует, что она действительно принадлежит кафе, гостинице или аэропорту.

Смартфон: ключ от вашей цифровой жизни

Когда-то потеря телефона означала потерю контактов. Сегодня в смартфоне могут находиться банковские приложения, электронная почта, документы, фотографии, рабочие чаты и доступ к десяткам сервисов.

Поэтому устройство должно быть защищено блокировкой экрана, а важные данные резервными копиями. Полезно также заранее знать, как дистанционно заблокировать или найти свое устройство.

Если смартфон потерян или украден, действовать нужно быстро: заблокировать SIM-карту и устройство, завершить активные сеансы в важных аккаунтах и при необходимости связаться с банком.

Несколько простых правил, которые стоит сделать привычкой

Для базовой кибербезопасности не нужно быть специалистом по технологиям. Гораздо важнее регулярно соблюдать несколько правил:

- используйте **разные пароли и двухфакторную аутентификацию**;
- никому **не сообщайте пароли**, SMS-коды, PIN, CVV/CVC и данные для входа в приложения;
- **проверяйте неожиданные ссылки**, файлы и просьбы о переводе денег;
- устанавливайте приложения **из официальных источников** и своевременно обновляйте устройства;
- контролируйте **разрешения приложений и настройки приватности**;
- не проводите **важные финансовые операции** через открытые Wi-Fi-сети;
- соблюдайте **правила защиты рабочей информации**;
- делайте **резервные копии** важных данных.

И еще одно правило, которое объединяет практически все остальные: **не действуйте автоматически**, если вас просят предоставить данные, открыть доступ или совершить финансовую операцию.

Если ошибка все-таки произошла, не стоит надеяться, что «ничего не случится». При риске списания денег сразу свяжитесь с банком, при компрометации аккаунта смените пароль и завершите посторонние сеансы, а если столкнулись с мошенничеством, то обязательно сохраните подтверждающие материалы и незамедлительно обратитесь в правоохранительные органы.