

ЦИФРОВАЯ ГИГИЕНА МОЛОДОГО СПЕЦИАЛИСТА

Практическое руководство по кибербезопасности на старте карьеры

Начало профессиональной деятельности — это не только новые задачи, но и высокий уровень ответственности за данные.

Мошеннические схемы становятся изощреннее, и вчерашний студент, не знакомый с правилами корпоративной безопасности, часто становится главной целью киберпреступников.

Данный чек-лист поможет защитить личные данные, сохранить конфиденциальность рабочей информации и сформировать культуру осознанного поведения в цифровом пространстве.

1. Личные и корпоративные аккаунты: разделение сред

- **Исключите смешивание почтовых ящиков.** Никогда не используйте личную почту для регистрации на рабочих корпоративных ресурсах, и наоборот — не привязывайте рабочую почту к личным сервисам (магазинам, соцсетям, подпискам).
- **Внедрите менеджер паролей.** Забудьте про хранение паролей в текстовых файлах на рабочем столе или в блокнотах. Используйте локальные или облачные менеджеры паролей с шифрованием.
- **Применяйте правило уникальности.** Один аккаунт — один сложный пароль. Длина пароля должна составлять не менее 12 символов, включая строчные и прописные буквы, цифры и специальные знаки.
- **Активируйте двухфакторную аутентификацию (2FA).** Это базовый и самый надежный барьер. Защитите двухэтапной проверкой все доступные сервисы: от рабочих мессенджеров до личных аккаунтов в банках и социальных сетях. При возможности используйте приложения-аутентификаторы (например, Яндекс Ключ или Google Authenticator) вместо SMS-кодов.

2. Защита от социальной инженерии и фишинга

- **Проверяйте контекст при общении в мессенджерах.** Популярный сценарий сегодня — сообщения в Telegram или VK от профиля «руководителя» или «отдела кадров» с требованием

срочно предоставить данные или выполнить финансовую операцию. При малейшем сомнении перепроверьте информацию по другому каналу связи (личный звонок, очная встреча).

- **Развивайте цифровую бдительность при работе со ссылками.** Перед переходом по любой ссылке из писем или сообщений внимательно проверяйте доменное имя в адресной строке. Разница в одну букву (например, замена «i» на «l») — классический признак фишингового сайта, созданного для кражи платежных данных или корпоративных доступов.
- **Контролируйте вложения.** Не открывайте файлы с расширениями .exe, .scr, .bat, а также заархивированные документы от внешних или неизвестных отправителей без предварительной проверки антивирусным ПО.

3. Безопасность мобильных устройств и работы «на удаленке»

- **Откажитесь от публичных Wi-Fi сетей для работы.** Открытые сети в кафе, коворкингах и на вокзалах уязвимы для перехвата трафика злоумышленниками. При необходимости поработать вне дома или офиса используйте режим модема на собственном смартфоне или подключайтесь исключительно через защищенное VPN-соединение, предоставленное организацией.
- **Контролируйте физический доступ к устройствам.** Установите автоматическую блокировку экрана смартфона и ноутбука при отсутствии активности (оптимальное время — 1 минута). Внедрите привычку блокировать экран сочетанием клавиш при каждом отходе от рабочего места.
- **Соблюдайте правила использования съемных носителей.** Внешняя флешка, найденная на парковке или полученная в подарок на конференции — это прямой источник заражения системы вредоносным кодом. Использование личных флеш-карт на рабочих устройствах должно быть полностью исключено.

4. Управление цифровым следом и биометрия

- **Защитите свой голос и лицо.** С развитием технологий искусственного интеллекта мошенникам достаточно короткой аудиозаписи вашего голоса, чтобы сгенерировать поддельное сообщение (дипфейк) для ваших близких или коллег. Ограничьте круг лиц, имеющих доступ к вашим аудиосообщениям в мессенджерах, с помощью настроек приватности.
- **Проведите аудит личных публикаций.** Оценивайте контент, который вы публикуете в открытом доступе. Фотографии рабочих

документов, экранов мониторов, пропусков или внутренних помещений компании — это прямая угроза безопасности бизнеса и вашей деловой репутации.

- **Регулярно очищайте неиспользуемые доступы.** Раз в полгода проверяйте список разрешений для сторонних приложений и сайтов, которым вы предоставляли доступ к своим аккаунтам, и отзывайте права у тех, которыми больше не пользуетесь.

Помните: кибербезопасность — это не статичное состояние, а ежедневный процесс. Внедрение этих простых правил в рутину позволит минимизировать до 95% рисков в цифровой среде.