Памятка и рекомендации по соблюдению личной цифровой гигиены и информационной безопасности

I. Фундаментальные правила, основы кибергигиены

1. Надежные, а значит сложные и уникальные пароли
Длина и сложность: минимум 12-15 символов. Используйте комбинацию строчных и заглавных букв, цифр и специальных символов, например, GroN!t7aa@13N#WA$).

Рекомендую использовать генераторы паролей, которых на просторах интернета достаточное количество.
Уникальность: никогда не используйте один и тот же пароль для разных сервисов! Если взломают один, взломают все.

Менеджер паролей: Используйте надежный менеджер паролей, он создаст, запомнит и безопасно сохранит сложные уникальные пароли за вас. Запомните только один «очень сильный» мастер-пароль.

Рекомендую менеджеры паролей от российских производителей, для любых устройств, например, Kaspersky Password Manager, который помимо хранения паролей имеет еще ряд полезных функций, таких как защищенное хранение фотографий, банковских карт, документов и т.п.
Парольные фразы: Рассмотрите использование длинных, легко запоминающихся фраз, например, «Я_очень_люблю_НАКД!», которая в английской раскладке будет выглядеть как «Z_jxtym_k.,k._YFRL!».

Рекомендую брать фразы из стихов и песен, но что бы ни кто не смог догадаться, лучше не из ваших самых любимых. Такие пароли не возможно угадать и очень сложно взломать методом подбора — брутфорсом.

2. Двухфакторная Аутентификация (2FA/MFA)
Включайте двухфакторную аутентификацию везде, где это возможно!Это второй уровень защиты после пароля.

Рекомендую для аутентификации, помимо иностранных аналогов, обратить внимание на «Яндекс.Ключ» вместо SMS. SMS потенциально можно перехватить.
Аппаратные ключи, типа USB-токен Рутокен — самый надежный вариант для критически важных аккаунтов (почта, банк и т.п).
Резервные коды: Храните резервные коды для аутентификации в безопасном месте (менеджер паролей или распечатанные в сейфе).

3. Регулярное обновление программного обеспечения
Система и программы: Включайте автоматическое обновление операционной системы, браузеров, антивируса и всех установленных программ.

Обновления часто закрывают критические уязвимости безопасности.

Прошивки: Обновляйте прошивки телефонов, роутеров, камер, умных устройств (IoT) и т.п.

Защита устройств и сетей

4. Антивирус и брандмауэр (файрвол, межсетевой экран)
Используйте надежное антивирусное программное обеспечение с активной защитой в реальном времени. Регулярно обновляйте его базы.

Убедитесь, что встроенный брандмауэр операционной системы (при наличии) включен. Он контролирует входящий и исходящий сетевой трафик.

Рекомендую использовать продукты российских производителей и ни в коем случае не использовать бесплатные инструменты.
Используйте надежный и обновленный браузер, лучше со встроенными средствами защиты, в том числе от рекламы

Рекомендую браузер Brave — конфиденциальный и безопасный браузер для ПК, Mac и мобильных устройств.

5. Безопасность домашней сети Wi-Fi
Смените пароль по умолчанию на роутере на сложный, надежный и уникальный.

Используйте надежный протокол шифрования (WPA2 или WPA3). Избегайте устаревших WEP/WPA.

Смените имя сети (SSID) по умолчанию на что-то неочевидное (не указывайте свой адрес или фамилию, номер квартиры и название интернет-провайдера).

Отключите WPS (Wi-Fi Protected Setup — протокол полуавтоматического создания беспроводной сети Wi-Fi) — эта функция часто уязвима.

Регулярно обновляйте прошивку роутера.

Рекомендую заменять роутеры с периодичностью не менее 1 раз в 3 года, т.к., например, по информации с ресурса SecurityLab.ru от одного из российских лидеров в информационной безопасности Positive Technologies старые роутеры часто являются предметом особого внимания хакеров и имеют критические уязвимости.

6. Осторожность с публичными Wi-Fi
Избегайте ввода логинов, паролей, банковских данных в общественных сетях.

Отключайте автоматическое подключение к открытым сетям.

Рекомендую отказаться полностью или максимально минимизировать использование публичных сетей Wi-Fi, а также VPN

Поведение и осознанность

7. Осторожность с потенциальным фишингом
Не доверяйте слепо письмам и сообщениям! Проверяйте отправителя, адрес может быть подделан.

Рекомендую при поступлении сообщений, которые вы не ждете — их удалять, если же тематика сообщения потенциально важна, то стоит выйти на возможного отправителя письма по другим каналам, например, по телефону (ни в коем случае не используя телефонные номера из самих сообщений), что бы убедиться, что сообщение не вредоносное.
Не переходите по подозрительным ссылкам и не открывайте вложения от неизвестных отправителей или если письмо вызывает подозрения (срочность, угрозы, грамматические ошибки, необычные запросы).

Проверяйте URL: Наведите курсор на ссылку (не кликая!), чтобы увидеть реальный адрес. Остерегайтесь опечаток в доменах (g0suslugi.ru, gosuslugi1.ru и т.п.).

Официальные сайты: Вводите адреса важных сайтов (банк, почта) вручную или используйте сохраненные закладки. Не переходите по ссылкам из писем/сообщений.

Рекомендую, например, использовать проверку статуса сайта с помощью технологии Safe Browsing Яндекс.

8. Загрузка программного обеспечения и файлов
Скачивайте программы только с официальных сайтов разработчиков или надежных магазинов приложений (RuStore, App Store, Google Play и т.п.).

При использовании зарубежных источников рекомендую быть особенно внимательным, т.к. есть вероятность столкнуться с клонами приложений, даже таких как менеджер паролей.
Избегайте сомнительных сайтов и торрентов.

Проверяйте файлы антивирусом перед открытием, особенно .apk, .exe, .msi, .zip, .docm, .xlsm и т.п.

Рекомендую проверять файлы н вирусы, например, с помощью онлайн-сервиса Virustotal.

9. Безопасность в социальных сетях и онлайн

Настройки приватности: Регулярно проверяйте и ограничивайте круг лиц, видящих ваши посты, личную информацию (дата рождения, адрес, телефон), списки друзей.

Осторожность с информацией: Не выкладывайте в открытый доступ сканы документов, билетов, фотографии с полной информацией (паспорт, кредитная карта), точные даты отъезда в отпуск.

Осторожность с незнакомцами: Не принимайте запросы в друзья от незнакомых людей без веской причины. Будьте скептичны к слишком хорошим предложениям или просьбам о помощи/деньгах.

Рекомендую воздержаться при общении в соцсетях от обсуждений религиозных и политических тем, а также минимизировать публикации, которые могут потенциально негативно отразиться на вашей репутации, например с распитием алкоголя и т.п.

10. Регулярное резервное копирование

Имейте 3 копии данных (основная + 2 бэкапа), на 2 разных типах носителей (например, HDD + облако), и 1 копию храните вне дома/офиса (облако или внешний диск у родственников/в сейфе).

Для хранения данных на внешних носителях рекомендую использовать носители типа iStorage DatAshur — защищенные флешки с пин-кодом и аппаратным шифрованием.

Автоматизируйте: Используйте встроенные или сторонние инструменты для автоматического бэкапа.

Проверяйте восстановление: Периодически проверяйте, что из резервной копии можно восстановить файлы.

11. Защита мобильных устройств

Блокировка экрана: Используйте ПИН-код, пароль, графический ключ или биометрию (отпечаток/лицо).

Рекомендую оценить потенциальные риски связанные с использованием отпечатка пальца и лица т.к. этими способами могут воспользоваться третьи лица, принуждая вас, либо когда вы находитесь в расслабленном или уязвимом состоянии.
Также рекомендую не вводить пароли, ПИН-коды и т.п. в людных местах, где их могут подсмотреть.

Источники приложений: Устанавливайте приложения только из официальных магазинов (RuStore, App Store, Google Play и т.п.).

Права приложений: Внимательно проверяйте, к каким данным и функциям (камера, микрофон, геолокация, контакты) запрашивает доступ приложение. Отказывайте, если доступ неочевидно необходим для работы приложения.

Обновления: Регулярно обновляйте операционную систему и приложения.

При использовании банковских клиентов банка, в котором у вас сконцентрировано на счетах наибольшее количество средств, приложение банка на телефон не устанавливать, либо устанавливать только на момент использования, а для оплаты использовать отдельные карты и счета, с незначительным балансом.

Дополнительные меры повышенной безопасности

12. Шифрование Дисков

Включите полное шифрование диска на ноутбуках и смартфонах, хотя бы встроенное, встроенное шифрование на Android/iOS). Это защитит данные при потере или краже устройства.

Рекомендую с осторожностью подходить к данной рекомендации, взвесить все за и против т.к. при возможных сбоях, забытом пароле и т.п., помимо потери всех данных, ваше устройство превратиться в бесполезный полупроводниковый сувенир.

13. Осторожность с USB-устройствами

Не подключайте найденные флешки или внешние диски к своему компьютеру. Они могут содержать вирусы. Будьте осторожны с устройствами, полученными от незнакомых людей.

14. Цифровая «уборка»

Регулярно удаляйте неиспользуемые приложения и учетные записи.

Чистите кеш браузера и куки.

Проводите ревизию подписок и разрешений, данных сайтам и приложениям.

Важно:
Нет 100% защиты, но соблюдение этих правил значительно снижает риски и делает вас сложной мишенью для большинства злоумышленников. Начните с самых базовых (пароли, 2FA, обновления, фишинг) и постепенно внедряйте остальные. Безопасность — это процесс, а не разовое действие!