Общие инструкции:

1. Работа с ПК дома:
    1. Определить, какие данные для вас важны и критичны. То есть критичные или чувствительные данные - это те данные или информация, которую можно извлечь из данных, использование которой может причинить моральный, финансовый, физический или репутационный ущерб вам или работодателю.
    2. Поставить антивирус и регулярно обновлять антивирусные базы и программу антивируса, либо настроить автообновление антивируса. Антивирус подойдет любой из массовых: Kasper, Avast, Eset, если оперционка win10 и выше – то оптимально использовать базовый антивирус Windows Defender («Защитник Windows») – на данный момент работает не хуже внешних вендров.
    3. В периоды наименьшей рабочей активности за компьютером настроить автоматический запуск антивируса для полной проверки компьютера
    4. Никогда не работать под ролью Администратор, завести себе отдельную пользовательскую роль с ограничением на запуск и установку программного обеспечения (ПО,программы далее) при попытке установки ПО будет уведомление, которое вы можете отклонить или подтвердить паролем администратора. Если кроме вам кто-то работает на ПК - завести ему отдельную роль с ограничением действия по установке-запуску ПО
    5. Регулярно обновлять установленные программы. п.2-5 - основа безопасной работы
    6. Разделить жесткий диск на разделы - отдельно система, отдельно личные данные, отдельно - рабочие данные.
    7. Выделить критичные данные на отдельный раздел диска.
    8. Шифровать разделы с личными , критичными и рабочими данными - включить штатное шифрование средствами операционной системы, либо шифровать специальным ПО
    9. Регулярно выполнять сохранение данных с компьютера на внешний жесткий диск, в идеале пара usb-жестких дисков для дополнительного резервирования
    10. Отключить автораспаковку архивов, автозапуск внешних носителей
    11. При подключении внешних носителей, например usb - перед работой с файлами на носителе, проверить носитель антивирусом
    12. Блокировать компьютер, если нужно отойти и прервать работу
    13. Постараться не использовать нелегальное программное обеспечение (ПО), особенно программы генерации ключей, программы модернизации лицензии (crack), так как внутри этих программ могут быть встроены майнеры, вирусы, бэкдоры, трояны и прочее ПО, которые могут быть замаскированы от антивируса или созданы недавно и сигнатуры которых не успели попасть в вирусные базы антивирусов.
    14. Если нужно использовать нелегальное ПО, то отбросив этические и правовые моменты, нужно изолировать его использование в виртуальной машине и не обрабатывать в таком ПО персональные данные и критичные рабочие данные. Постараться найти бесплатный аналог или согласовать с работодателем-заказчиком покупку легальной лицензии.

15. При установке программного обеспечения обращать внимание на те разрешения и доступы, которые запрашивает ПО, если не знаете, что именно запрашивается - откажитесь от установки, уточните у кого-то где-то и вернитесь позже

2. Работа в сети:
    1. Использовать VPN при работе в сети и почте. Если сложно с настройками, то браузер Opera с белой буквой "O" - версия для разработчиков с встроенным VPN «Версия Opera для разработчиков» https://www.opera.com/ru/download
    2. Либо Tor Browser с оф ресурса https://www.torproject.org/ru/ , пока его использование не карается, но провайдеры могут понимать факт использования этого софта, но не могут видеть трафик. Рекомендуется именно браузер, не в коем случае не используйте ноды-узлы сети Тора на своих устройствах, особенно выходные в общую сеть, которые является точками раскрытия трафика, ибо: https://roskomsvoboda.org/27509/
    3. Если есть возможность - настроить firewall. При аккуратной работе и выполнении п.2-5 предыдущего пункта его наличие не критично.
    4. Всегда проверять антивирусом загруженные файлы из источников к которым нет доверия. В идеале не только установленным антивирусом, но и на VirusTotal https://www.virustotal.com/gui/
    5. Установить в браузеры блокировщики передачи снимков браузера - служебной информации о браузере, например Ghostery https://www.ghostery.com/ и https://chrome.google.com/webstore/detail/ghostery-%E2%80%93-privacy-ad-blo/mlomiejdfkolichcflejclcbmpeaniij?hl=ru
    6. Регулярно чистить кэш и cookie браузера, не хранить пароли в браузере
    7. Не использовать одинаковые пароли для разных ресурсов
    8. При работе в сети, с соц сетями, почтой помнить "заповедь": "Возможно именно сейчас меня хотят обмануть".
    9. При ответе на контрольные вопросы восстановления доступа не использовать ту информацию, которая доступна о вас в соц сетях: даты рождения, имена, клички домашних животных, географические названия. Пробовать придумывать нестандартные ответы на вопросы вида: "Где вы родились" - "В роддоме"
    10. При работе с чувствительными - критическими данными проверять, что есть защищенное подключение ssl - наличие в адресной строке https
    11. При переходе на ресурс обращать внимание на написание адреса в адресной строке - многие поддельные-фишинговые сайты создаются с созвучными названиями оригинальным ресурсам, но с опечатками-дополнениями в имени
    12. При звонках от кого-либо с просьбой под любым предлогом предоставить критичные, персональные, рабочие данные - обрывать разговор. Социальные инженеры могут быть очень талантливы в стратегии выпытывания данных.
    13. В сервисах и ресурсах при наличии двухфакторной аутентификации рекомендуется включить ее, например, как отправка доп кода на номер телефона
    14. Не переходить по подозрительным ссылкам, если есть сомнения можно использовать специальные сетевые сайты-песочницы для

открытия таких ссылок или использовать специальные защищенные браузеры, например бесплатный браузер Avast

3. Если компьютер ведет себя странно: зависания, медленная работа, странное поведение ПО:
    1. Обновить базы антивируса, если антивирус работает
    2. Отключить компьютер от сети интернет и локальной сети
    3. Запустить полную проверку
    4. Если антивирус не работает, то отключить компьютер от сети
    5. Выполнить перезагрузку и зайти в защищенном (или другом ограниченном) режиме
    6. Попробовать запустить антивирус и проверку
    7. Если не помогло - скачать бесплатную автономную версию антивируса и запустить ее, в том числе запустить с usb-флешки
4. Действия при потере-краже устройства:
    1. Заранее включить в настройках ПК опцию "Где мое устройство" - контроля устройства, многие производители предлагают такую опцию под разными названиями
    2. Добавить пароли для доступа к директориям, архивам с критичными данными
    3. Можно поискать специальный софт, на «Яблоке» это «Локатор», который контролирует последнюю геопозицию выхода в сеть устройства.
    4. Использовать спец ПО для удаленного контроля ПК или удаления данных, например: https://codeby.net/threads/udalenno-udaljaem-dannye-s-ukradennogo-noutbuka.67177/
    5. Регулярно сохранять критичные данные, как говорилось выше
    6. Если ПК украден войти в профиль устройства на сайте производителя для поиска геопозиции
    7. Если установлено ПО из п 3, то попробовать заблокировать-удалить данные
    8. Обратиться в правоохранительные органы с заявлением о краже, дополнив данными из п.1, п.4. Не всегда результативно, но может сработать.