Правила кибербезопасности на работе

НЕ УСТАНАВЛИВАТЬ ПРОГРАММЫ САМОСТОЯТЕЛЬНО	Используйте только одобренные IT-отделом ресурсы и программное обеспечение. Если есть сомнения или нужна особенная программа, обратитесь к админам
ПРОВЕРЯТЬ АДРЕСА ПОДОЗРИТЕЛЬНЫХ ПИСЕМ	Будьте осторожны, когда открываете электронные письма или сообщения в мессенджерах, это может быть фишинг
СООБЩАТЬ О ВОЗМОЖНЫХ УГРОЗАХ В IT-СЛУЖБУ	О подозрительных письмах или сообщениях сообщайте в службу безопасности или системным администраторам. Если подозреваете заражение компьютера или утечку данных, сразу сообщайте в IT-отдел или службу безопасности
ИСПОЛЬЗОВАТЬ ПАРОЛИ ДЛЯ ПАПОК И ДИСКОВ	Храните конфиденциальные и персональные данные только на защищенных серверах и устройствах
СВОЕВРЕМЕННО ВЫПОЛНЯЙТЕ ТРЕБОВАНИЯ IT-ОТДЕЛА	Если вас попросили сменить пароль, не оттягивайте и выполните эту задачу в течение дня. Постарайтесь подобрать пароль, который существенно отличается от предыдущего
НЕ ХРАНИТЕ ЛОГИН И ПАРОЛЬ НА СТИКЕРАХ ИЛИ В БЛОКНОТАХ РЯДОМ С КОМПЬЮТЕРОМ	Не сохраняйте данные, по которым можно войти в ваш рабочий компьютер или в аккаунт, на бумажных носителях. Особенно – рядом с компьютером. Так третьи лица не смогут получить доступ к вашим данным
НЕ РАБОТАЙТЕ ЧЕРЕЗ ОБЩЕСТВЕННУЮ СЕТЬ	Не спешите подключаться к общественному Wi-Fi, если рабочая задача застала вас вне дома или рабочего компьютера. Если есть возможность отложить дело – сделайте работу в комфортных и безопасных условиях дома или в кабинете. Если дело срочное, безопаснее будет воспользоваться мобильным интернетом. Но не забудьте обезопасить сеть паролем

Памятка для педагогов