Памятка пользователю по информационной безопасности

Парольная защита

Не используйте простые пароли, например: *"12345, 123qwe321, 10121980"* и т.п. Пароли должны быть не менее 8 символов, содержать прописные и строчные буквы (a-z, A-Z), цифры и спецсимволы (&*!%).

Сохраняйте в тайне личный пароль. Никогда не сообщайте пароль другим лицам и не храните записанный пароль в общедоступных местах, в том числе на мониторе, клавиатуре.

Если для производственных нужд пароль на время передавался другому сотруднику, то по завершению такой необходимости, при первой возможности самостоятельно смените этот пароль.

Не используйте личные пароли (от соцсетей, личной почты и т.п.) для служебных программ (1С, сервер) и наоборот, не используйте служебные пароли для личных целей.

Никогда не сохраняйте ваши пароли в программах или браузере для интернет - банков, личных кабинетов платежных систем и других сервисов с вашей или чужой персональной, коммерческой и конфиденциальной информацией. Большинство программ хранят пароли в открытом виде и тот, кто получит доступ к вашему компьютеру, тот легко получит доступ и к вашим паролям!

При временном оставлении рабочего места в течение рабочего дня в обязательном порядке блокируйте компьютер нажатием комбинации клавиш «Win + L».

Антивирусная защита

На компьютере, подключенном к локальной сети или Интернет должен быть установлен антивирус, если его нет, то нужно установить немедленно.

Если антивирус перестал обновляться или вовсе работать (на иконке антивируса появились восклицательные знаки, крестики или выдаются об этом сообщения на экране), то обязательно об этом сообщите ИТ - специалисту. Не отключайте антивирус!

Обязательно проверяйте на наличие вирусов все внешние носители информации (диски, флешки, карты памяти, приложения к письмам). Сделать это просто: правой кнопкой мыши на диске, папке или файле и выберите пункт "Проверить на вирусы" (называется по-разному в зависимости от установленного антивируса).

Интернет и электронная почта

Не открывайте вложенные к письму файлы и документы от неизвестных отправителей. В 90% случаев шифровальщики отправляются жертвам в виде спама по электронной почте. Поэтому не открывайте письма от незнакомых адресатов и с подозрительным содержанием. Обычно шифровальщики кочуют по интернету в виде псевдо-pdf. Т.е. вам приходить письмо в которое вложен файл якобы книги в формате pdf, но со странным форматом типа nazvanie.ru.pdf.exe.

Не переходите по ссылкам, не запускайте программы и не открывайте файлы, полученные по электронной почте от неизвестного Вам отправителя.

Всегда проверяйте с какого адреса отправлено письмо, куда ведут ссылки в письме (достаточно навести мышью на ссылку, не нажимая на неё).

Перешлите подозрительное письмо ИТ - специалисту для антивирусной проверки, не открывайте вложения самостоятельно.

Документы и программы

Не устанавливайте самостоятельно программное обеспечение, если это не входит в Ваши обязанности. Запрещается устанавливать и запускать нелицензионное или не относящееся к выполнению Ваших должностных обязанностей программное обеспечение.

Делайте резервные копии важных документов на разные носители (другой диск или внешний носитель, сетевой диск, облачное хранилище и т.п.) или обратитесь к ИТ - специалистам для настройки регулярного резервного копирования вашей ценной информации.