ОСНОВНЫЕ ПРАВИЛА ПРИ РАБОТЕ В ИНТЕРНЕТЕ

Правила использования паролей:

- Не использовать типичные пароли (Например: 123456), а также свои имена и фамилии на латинице или в английской раскладке, имена детей, номера телефонов в качестве паролей
- Не использовать одни пароли и логины для разных сайтов
- НИКОГДА не передавайте свои пароли ни человеку, ни в службу поддержки, ни в банк (для решения технической проблемы службе поддержки **не нужен** Ваш пароль)
- Храните пароли и ответы на секретные вопросы в блокноте, а не на компьютере
- Не храните пароли к сайтам в почтовом ящике, либо храните файл с паролями на флэшке
- У себя на компьютере в браузере можно сохранить пароли от социальных сетей и форумов, но НИКОГДА не сохранять пароли от электронного ящика (т.к. через него можно получить доступ ко всем Вашим учетным записям), интернет-банка, электронных кошельков
- Если возникло подозрение, что произошел взлом вашей учетной записи, меняйте все пароли, не забудьте их переписать в блокноте
- На чужих компьютерах никогда не сохраняйте свои пароли, убирайте галочку *Запомнить* и ставьте галочку чужой компьютер

Идеальный пароль:

- Забудьте о красивых и запоминающихся паролях, они удобны и для злоумышленников
- Придумайте сложный пароль (состоит не менее чем из 11 символов)
- Идеальный вариант: случайный набор букв, цифр и символов, обязательно включающих цифры и буквы разных регистров, например: e&2m@k1E#39DJ8we
- Например, можно придумать несуразную фразу, но понятную для Вас и набрать ее в английской раскладке, добавив разный регистр, цифры и символы.

Фишинг (подделка) - вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. (Фишинговый адрес vkontacte.ru, настоящий адрес vkonta**k**te.ru или **vk.com**). Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на **сайт**, внешне неотличимый от настоящего. Например, вы вводите пароль от аккаунта в социальной сети на поддельном сайте и нажимаете «Войти» – этот процесс называется фишингом.

Общие правила:

- Использовать обновляемые антивирусы
- Не открывать письма неизвестных адресатов
- Не открывать письма из папки спам, они могут содержать вирусы
- Не реагировать на сообщения от друзей: «Меня взломали, теперь это моя новая страница»
- В таких письмах может идти речь о потери данных на сервере или других проблемах. Если у вас попросят пароль, сразу добавляйте в черный список - это мошенники
- Если пришло письмо с банка с просьбой перейти по ссылке и подтвердить свой логин и пароль – удаляйте его и никогда не отвечайте
- Посмотрите на адрес сайта в адресной строке, адрес может отличаться на 1 символ

- Письмо от банка может прийти только в момент регистрации, далее никаких «неожиданных» писем не должно быть, перейдя по ссылке Вы можете открыть шпионскую программу, которая ворует пароли
- Лишний раз не скачивайте бесплатные программы, они могут содержать вирусы (под видом программы можно скачать и установить вирус) не покупайтесь на объявления о быстром заработке
- Не включайтесь в игры "волшебные кошельки", "чтение писем - высокооплачиваемая дистанционная работа в интернете", "пришли нам 100 баксов и получишь 1000"
- Если Вы еще ничего не заработали, а некий "работодатель" у Вас уже просит денег, то это однозначно обман!
- Если Вам предлагают "зарабатывать" приличные деньги, но при этом нет реального товара или услуги (которые были бы действительно нужны людям и продавались бы), то это мошенничество.
- Никогда не предоставляйте ваши персональные данные людям, в личности которых вы недостаточно уверены. Это все равно, что отдать чужому человеку свой паспорт или ключи от дома.
- Посмотрите, от кого пришла информация с просьбой о подтверждении личных данных. В, казалось бы, известном вам адресе сайта крупной компании может быть изменена лишь одна буква.
- Внимательно относитесь к присланным вам ссылкам на сайты. Иногда это могут быть сообщения от хорошо знакомых вам людей. Просто их почтой или аккаунтом воспользовались мошенники. Если сомневаетесь, позвоните знакомым или напишите, поинтересовавшись, что он вам прислал.
- Игнорируйте спам. Старайтесь эти письма не открывать.
- Игнорируйте сообщения во всплывающих окнах.
- Запомните ваши пароли и PIN-коды. Не храните пароли в компьютере. Придумайте надежный пароль и запишите его в блокнот.
- Безопасность должна быть многоуровневой. Установите и регулярно обновляйте программные продукты, обеспечивающие безопасность компьютера.

Безопасность при расчетах в Сети

Будьте осторожны при совершении онлайн-покупок. Мошенник может узнать номер вашей банковской карты. Используйте веб-сайты, которые обеспечивают безопасность сделок. Также ознакомьтесь с политикой конфиденциальности сайта.

- Все действия с денежными средствами должны подтверждаться банком – например, с помощью СМС.
- НИКОГДА банк не попросит у Вас пароль от входа в личный кабинет.
- Никогда не передавайте ПИН-код от Вашей пластиковой карточки.
- Никогда никому не говорите код с обратной стороны карты (CVC и CVV –код) и пароли из СМС-сообщений от банка — их никогда не спросят сотрудники банка или службы поддержки сайта, где вы покупаете или продаете.
- Во время работы с денежными средствами не должны запускаться иные программы.
- При выборе интернет-магазина обращайте внимание на репутацию компании, положительные отзывы на форумах и контактную информацию для решения вопросов в случае каких-либо нештатных ситуаций.

- При оплате на сайте всегда проверяйте адрес страницы оплаты — он написан в строке браузера вверху страницы. Символы в адресной строке должны начинаться с https — это значит, что данные, которые вы введете в поля для оплаты, будут защищены. Также убедитесь, что в адресной строке корректно написано название сайта, на котором вы совершаете покупку — ошибка даже в одну букву означает, что перед вами подделка.
- Никогда не переходите по ссылкам, которые прислали вам другие пользователи сети, даже если это покупатели или продавцы.
- Не используйте для расчетов через интернет свою основную банковскую карту. Предпочтительно использовать специальные виртуальные карты необходимого номинала.
- Лучше не совершайте платежи с мобильного устройства, особенно если на нем не установлен антивирус. Не работайте со своим счетом в сетях общественного доступа.