ПРАВИЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

При столкновении с мошенничеством не бойтесь обращаться в правоохранительные органы. Правила информационной безопасности в интернете важно знать каждому. Рост киберпреступлений будет только расти все сильнее с каждым годом. Следование правилам информационной безопасности поможет сохранить конфиденциальность, деньги и нервы.

✓ Используйте разные пароли на сайтах. Регулярно их меняйте. Девичья фамилия матери, дата рождения, год и другие простые словосочетания - является плохим паролем. Желательно создание 8-ми значного пароля, с использованием дополнительных символов +, ,_?~@# и разных регистров.

✓ Отдавайте предпочтение **трехфазной аутенфикации**, то есть отправки SMS на ваш личный мобильный телефон.

✓ Вход на сайт в Госуслуг РФ рекомендуется использовать при аутентификации (10-ти значный пароль) и восстановление через SMS.

✓ При работе с почтой **@tatar.ru** не открывайте незнакомые письма, а особенно подозрительные. Не переходите по ссылкам в письме. Все это чревато тем, что подвергается повышенному риску заражения компьютера. Обо всех подозрительных письмах сообщать в отдел информационных технологий Аппарат Совета Бугульминского муниципального района. **Для безопасной работы необходимо:**

1. Внимательно проверяйте адрес отправителя, даже в случае совпадения имени пользователя;

2. Не хранить важные документы в переписке;

3. Проверять письма, в которых содержаться призывы к действиям (открой, прочитай, ознакомься), а также с темами про финансы, банки, геополитическую обстановку и угрозы;

✓ Сразу удаляйте пересланные сканы документов (паспорта снилс и тд). Не отправлять важную информацию и персональные данные через What’s app. Передача может быть осуществлена через **заархивированный файл с паролем**. Пароля отправляется отдельно.

✓ Не отвечайте на спам и подозрительные сообщения,

✓ Регулярно следите за обновлениями антивирусной программы. Это важнейший шаг к улучшению информационной безопасности. В случаи ошибки при работе

антивируса обратиться в отдел информационных технологий Аппарат Совета Бугульминского муниципального района.

✓ На постоянной основе проверяйте компьютер , USB (флеш карты) антивирусным обеспечением. Обращай внимание на подозрительное поведение компьютера.

✓ При работе в браузере не **Обращайте внимание** на слова **«бесплатно», «free», «скидка», «скачать бесплатно и без регистрации».** Регулярно очищайте историю поиска.

✓ Не запускайте неизвестные программы, особенно с расширением .exe или .bat. Установка не лицензионного ПО ***ЗАПРЕЩЕНА.*** Все ПО устанавливаются только сотрудниками ОИТ.

✓ Многие поддельные сайты копируют дизайн известных порталов. Именно так теряют пароли. Лучше всегда вводите ссылки, а не ищите ресурс через поисковые строки.

✓ Никогда не сохраняйте в браузере **пароли и номера банковских карт**.

✓ **Отключите голосовые** интернет-помощники, которые могут использовать данные в своих целях.

✓ В соцсетях не принимайте в друзья незнакомых людей. В лучшем случае это будет спам.

✓ Не делайте репосты про помощь для больных, животных или на другие благие дела. Делать это можно только в том случае, если лично знаете организацию или человека. В противном случае Вы становитесь соучастником киберпреступления.

✓ Вам присылают сообщение, что компьютер был взломан. А теперь нужно выслать им деньги, чтобы компромат с камеры, микрофона или телефона не попал в посторонние руки? Это мошенники. Не принимайте их условия.

✓ Пользуйтесь только драйверами с официальных сайтов производителей.

✓ Все безопасные сайты сейчас начинаются с **«https://», а не «http://».** Особенно при оплате смотрите на это. Также такие сайты помечены закрытым замочком в адресной строке, выходит информационное сообщение о опасности перехода на данный сайт.

✓ Запрещено использовать бесплатные программы **VPN** для закрытых сайтов **Роскомнадзором**

✓ Запрещено использовать бесплатные программы **Team Viewer, RAdmin, Zoom, Skype.**