**Памятка информационной безопасности**

Уважаемые Абоненты, во избежание несанкционированного проникновения на ваши сетевые ресурсы, воровства или «взлома» реквизитов доступа в сеть Интернет и других проблем связанных с действиями злоумышленников рекомендуем строго соблюдать следующие правила сетевой безопасности:

1. Ведите постоянный учет своей сетевой активности (всех сеансов связи). Регулярная смена сетевого пароля - это хорошая привычка. Обязательно меняйте пароль после любых работ, связанных с ремонтом, наладкой, установкой или настройкой программного обеспечения на Вашем компьютере третьими лицами.
2. Следует избегать открытия неизвестных файлов, полученных по электронной почте без предварительной проверки их содержания и источника отправки. Письма с вложениями в виде неизвестных файлов лучше удалять немедленно по получении.
3. Рекомендуется устанавливать обновления программ, повышающих безопасность использования приложений, особенно для Microsoft Office, Microsoft Intеrnet Explorer и Netscape Navigator.
4. Не устанавливайте хранители экрана и компьютерные игры без проверки их на безопасность.
5. Создавайте и проверяйте резервные копии данных.
6. Основная цель атаки любого взломщика - это Ваши сетевые реквизиты (пароль и имя пользователя). Храните их в строжайшем секрете.
7. Следует ограничить круг лиц, которому известны сетевые реквизиты.
8. Избегайте сохранения паролей в памяти компьютера. Кратковременный доступ к компьютеру третьих лиц откроет им Ваш ключ к сети.
9. Регулярно проверяйте свой компьютер на наличие вирусов и обновляйте антивирусное программное обеспечение. Вирус - популярный и незаметный способ передачи сетевых реквизитов.
10. При возникновении малейших сомнений в безопасности Вашего сетевого соединения немедленно свяжитесь с администратором сети.

**Абонентам следует знать, что:**

1. Провайдер не несет ответственности за ущерб или убытки любого рода, понесенные Абонентом в связи с подключением его технического комплекса к сети Интернет;

2. Провайдер не имеет лицензионных прав выполнять оперативно-следственные действия в отношении своих Абонентов.

3. Для установления данных хакера необходимо соблюдать строжайшую секретность:
- немедленно обращаться в правоохранительные органы;
- сетевые реквизиты не изменять вплоть до окончания следствия