

Периодически проверяй, какие платные услуги активированы на твоём номере;

Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;

Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

Online игры

Современные онлайн-игры - это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.

Все эти средства идут на поддержание и развитие игры, а также на самую безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов.

В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

Основные советы по безопасности твоего игрового аккаунта:

1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;
2. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;
3. Не указывай личную информацию в профайле игры;
4. Уважай других участников по игре;
5. Не устанавливай неофициальные патчи и моды;
6. Используй сложные и разные пароли;
7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

Фишинг или кража личных данных

Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет, и продолжают заниматься "любимым" делом.

Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей - логинов и паролей. На английском языке phishing читается как фишинг (от fishing - рыбная ловля, password - пароль).