#### Основные советы по безопасности твоего игрового аккаунта:

#### 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 саму 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.

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

**Основные советы по борьбе с фишингом:**

**Фишинг или кража личных данных.  
Обычной кражей денег и документов сегодня уже никого не удивиfшь, 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).**

* Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;
* Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
* Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;
* Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;
* Установи надежный пароль (PIN) на мобильный телефон;
* Отключи сохранение пароля в браузере;
* Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;