Рекомендации по защите идентификационных данных услуги передачи данных

Для предотвращения получения другими лицами доступа к Вашим персональным данным, хранящимся на компьютере либо в сети Интернет, стоит придерживаться ряда важных правил.

Как обеспечить безопасность пароля?

Первый шаг в защите Вашей конфиденциальности в Интернете — создание безопасного пароля, который не сможет легко определить компьютерная программа или настойчивый человек за короткий период времени.

Советы по созданию безопасного пароля:

- Используйте знаки препинания и/или цифры.
- Используйте и прописные, и заглавные буквы.
- Используйте похожие замены, например, ноль вместо буквы 'O' или '$' вместо буквы 'S'.
- Создайте уникальный акроним.
- Используйте фонетическую замену, например: 'Luv 2 Laf' для 'Love to Laugh'.

Чего не следует делать:

- Не следует использовать один пароль для нескольких важных аккаунтов, например Gmail или интернет-банка.
- Не используйте пароль, приведенный в качестве примера.
- Не используйте пароль, включающий личную информацию (имя, дату рождения и т.п.)
- Не используйте слова или акронимы, которые можно найти в словаре.
- Не используйте буквы в порядке клавиатурной раскладки (фыва олдж) или последовательные числа (1234).
- Не составляйте пароль только из цифр, из больших или из маленьких букв.
- Не используйте повторяющиеся символы (aa11).
- **Ни в коем случае не сохраняйте пароли к сайтам в браузерах!**

Как сохранить пароль в тайне:

- Никогда и никому не сообщайте свой пароль (включая членов семьи, друзей, соседей и т.д.)
- Никогда не записывайте свой пароль.
- Никогда не посылайте свой пароль по электронной почте.
- Регулярно проверяйте и меняйте свой пароль.

Вашим интернетом пользуется кто-то другой, Или как избежать взлома (потери) аккаунта.

Как заметить кражу

Каждый абонент ОАО «ГОТТЦ «Гарант» может отслеживать состояние своего лицевого счета и количество проведенного в Интернете времени в личном кабинете пользователя по следующему адресу http://my.garant.by. Желательно хотя бы раз в неделю проверять состояние Вашего лицевого счета и сравнивать время, проведенное в Интернете лично Вами, с временем пользования Вашим аккаунтом (оно отображено в отчетах личного кабинета). Если у Вас возникли подозрения, что кто-то пользовался аккаунтом в Ваше отсутствие (например, в отчете виден сеанс связи в ночное или рабочее время), немедленно свяжитесь с техподдержкой по тел. 434083.

Самые распространенные причины взломов...

В этом руководстве собраны советы, как обезопасить себя от кражи логина и пароля посредством фишинга (англ. phishing, от fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (почте, игровому или форумному логинам, паролям).

1. Фишинг

Одним из примеров является создание сайта или форума с точно таким же интерфейсом, как и официальный.
При переходе по ней и регистрации под вашими данными аккаунта на сайте, этими данными завладеет злоумышленник.

Примеры распространения:

В игровых чатах, форумах

Вас попросят посетить какой-нибудь сайт, например, с бесплатной раздачей, на котором вам предложат ввести данные своего аккаунта (логин и пароль). Такие сайты администрируются мошенниками, поэтому Ваши данные становятся известны злоумышленнику.

На форуме

- Если Вас просят посмотреть какую-либо тему/пост, пожалуйста, всегда внимательно проверяйте адрес в строке браузера, на который Вас перенаправляет браузер.
- Внимательно посмотрите на адресную строку - там указан другой домен, что явно указывает на мошеннический сайт, если Вы введете свои данные, то они попадут злоумышленнику и Вы потеряете аккаунт.

Меры противодействия.

ВСЕГДА смотрите адрес, на который ведет ссылка.
Запомните!
Официальный сайт - http://www.garant.by
Личный кабинет абонента - http://my.garant.by/
Игровой портал - http://portal.garant.by/

Рекомендации:
3.1. Ни в коем случае НЕ регистрируйтесь на сторонних сайтах под тем же логином, что и на официальном сайте.

3.2. Если Вы имеете единую учетную запись на многих сайтах, не посещайте сомнительные сайты под той же учетной записью. Такие сайты администрируются мошенниками и им становятся известны Ваш логин и пароль.
3.3. Защищайте свой аккаунт сложными паролями!
Запомните, доступ к Вашему личному кабинету – это доступ к Вашей учетной записи.

Что делать, если Вы обнаружили, что ввели свои учетные данные на фишинговом сайте?
Если такое все же произошло, не надо паниковать, вот несколько простых шагов, которые могут помочь минимизировать ущерб:

1. Постарайтесь максимально быстро изменить пароль к вашему логину.
2. Если меры не помогли и Вы потеряли контроль над учетной записью (логином и паролем), не теряйте время и обратитесь в **техподдержку по тел. 434083**

2. Передача аккаунта другому человеку (шаринг)

Шаринг (англ. sharing - общий доступ) - разглашение личных данных (почте, игровому логину, паролю, ответу на секретный вопрос и т.д.), в результате которого доступ к аккаунту получают другие лица.

Меры противодействия.

Никому, даже Вашим друзьям по играм, в чатах и т.д., не сообщайте имя Вашей учетной записи и пароль от нее.
Обратите внимание, что согласно договору:
2.2.7.Абонент обязуется хранить в тайне Идентификационные данные и не предоставлять их третьим лицам.
5.3. Абонент полностью ответственен за сохранность своих Идентификационных данных и за убытки, которые могут возникнуть по причине несанкционированного использования его канала доступа. Абоненту рекомендуется регулярно менять свои Идентификационные данные.

3. Использование читов, скриптов на взлом, других сторонних программ (кейлоггеры)

В интернете много сайтов, распространяющих различные программы для якобы модификации клиента, которые, по словам создателей, должны облегчить Вам жизнь. Во всех случаях Вам предлагают скачать файл и установить неизвестное программное обеспечение, которое содержит вирус (кейлоггер) и является распространенным способом взлома пароля от различных сайтов, программ, игр

Пример распространения на форуме:

Вам предлагают скачать и запустить программу у себя на компьютере, после чего происходит одно из следующего:

1. Вирус берет информацию из временных файлов браузеров (все современные браузеры поддерживают так называемое «сохранение пароля» и автологин) и отправляет ее злоумышленнику.
2. У Вас на компьютере остается, так называемый keylogger, который запускается вместе с загрузкой интернет соединения, программы и регистрирует каждое нажатие клавиши. После чего эта информация отправляется взломщику.

Таким образом, взломщик может украсть пароли не только от аккаунта личного кабинета, но и от других Ваших аккаунтов например почты, социальных сетей.
Если Вы не хотите потерять свои деньги и свой аккаунт – придерживайтесь рекомендациям по защите своей учетной записи. Запомните, доступ к аккаунту разрешен только первоначальному владельцу, на чье имя оформлен договор. Попытки использования аккаунта другими лицами и разглашение личных данных являются нарушением данного договора.

Меры противодействия.

- Не скачивайте никакие сомнительные файлы и тем более не запускайте *.exe и *.bat файлы на своем компьютере, если Вы в них не уверены.
- Предварительно проверяйте любые файлы антивирусом с актуальными базами. Также рекомендуется постоянно обновлять интернет браузер и по возможности не сохранять пароли, а вводить их вручную.

5. Лже-администраторы.

Администрация никогда не будет предлагать Вам каких-либо услуг или требовать данные Вашей учетной записи.
Если Вам написали на форуме или в чате и под различным предлогом требуют логин и пароль (покачать, начислить деньги, проверить аккаунт на нарушения, сделать администратором или модератором), запомните - в данном случае люди лишь выдают себя за администрацию.

Меры противодействия.

Сделайте скриншот такого разговора (переписки) и обязательно сообщите в техподдержку по тел. 434083 о таком разговоре (переписке), если он произошел на форуме, или в чате.

Эпилог.

В большинстве случаев потеря аккаунта - следствие халатности и небрежности абонента, не стоит недооценивать важность сетевой безопасности.
Не попадайтесь на уловки мошенников**, не нарушайте правил сетевой безопасности**, не передавайте данные учетной записи и регистрационные данные никогда и никому.