

Как защититься от фишинга

Эта памятка поможет вам защитить личные данные

Обычной кражей денег и документов 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 (от английского слова fishing – рыбная ловля), главная цель которого состоит в получении конфиденциальных данных пользователей – логинов и паролей

Советы по борьбе с фишингом

1. Следите за своим аккаунтом. Если вы подозреваете, что ваша анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее.
2. Используйте безопасные веб-сайты, в том числе интернет-магазинов и поисковых систем.
3. Используйте сложные и разные пароли. Таким образом, если вас взломают, то злоумышленники получат доступ только к одному вашему профилю в сети, а не ко всем.
4. Если вас взломали, то необходимо предупредить всех своих знакомых, которые добавлены у вас в друзьях, о том, что вас взломали и, возможно, от вашего имени будут рассылаться спам и ссылки на фишинговые сайты.
5. Установите надежный пароль (PIN) на мобильный телефон.
6. Отключите сохранение пароля в браузере.
7. Не открывайте файлы и другие вложения в письмах, даже если они пришли от ваших друзей. Лучше уточните у них, отправляли ли они вам эти файлы.