

Наш адрес:

Публичный центр правовой информации

Центральная районная библиотека

г. Лунинец,

ул. Фрунзе, 12

тел. 20-622

электронная почта: Incrb@brest.by

сайт: <http://lrcbs.by>



Услуги публичного центра правовой информации

Бесплатные:

- предоставление доступа к эталонной правовой информации;
- предоставление полной информации о составе фондов и информационных ресурсах ПЦПИ;
- консультационная помощь в поиске источников правовой информации;
- выдача документов из фонда ПЦПИ для временного пользования;

Платные

- поиск правовых актов в ИПС «ЭТАЛОН» (по теме, дате, ключевому слову и т.д.);

Примечание: При наличии полных сведений о документе: вид документа (закон, декрет, указ, постановление, положение и т.д.), орган принятия (Президент Республики Беларусь, Совет Министров, отраслевое министерство и т.д.), точное название, дата принятия, поиск производится бесплатно.

- распечатка найденной информации на принтере;
- ксерокопирование документов из фонда ПЦПИ.



Лунинецкая центральная районная библиотека
Публичный центр правовой информации

ФИШИНГ: как распознать и как защититься



Фишинг (phishing, от fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение идентификационных данных пользователей (логины и пароли к банковским картам, учетным записям).

Чаще всего фишинг представляет собой массовые рассылки писем и уведомлений от имени известных брендов, банков, платежных систем, почтовых сервисов, социальных сетей. Такие письма, как правило, содержат логотип, сообщение и прямую ссылку на сайт, внешне неотличимый от настоящего. По ссылке требуется перейти на сайт «сервиса» и под различными предложениями ввести конфиденциальные данные в соответствующие формы. В результате мошенники получают доступ к аккаунтам и банковским счетам пользователей.



Несколько самых важных правил, которые помогут Вам не попасться на крючок мошенников:

- Не открывайте электронные письма от неизвестных отправителей.
- Нажимайте на ссылку внутри электронного письма только в том случае, если Вы точно знаете, куда она ведет.
- Получив письмо от сомнительного отправителя, перейдите по прилагаемой ссылке вручную — введите адрес законного веб-сайта в адресную строку браузера с помощью клавиатуры, так Вы обеспечите для себя еще один уровень безопасности.
- Проверяйте цифровые сертификаты веб-сайтов.
- Если Вас просят раскрыть конфиденциальные данные, убедитесь, что URL-адрес веб-страницы начинается с «HTTPS», а не просто с «HTTP». Буква «S» обозначает «secure» (безопасно), то есть подключение с таким адресом является защищенным. Вместе с тем, это не дает гарантии, что веб-сайт является законным, однако большинство законных веб-сайтов используют именно протокол HTTPS в силу его большей безопасности. При этом даже законные веб-сайты, использующие протокол HTTP, уязвимы перед атаками хакеров.

- Если Вы подозреваете, что полученное электронное письмо было отправлено мошенником, введите имя отправителя или отрывок текста письма в поисковую систему — и Вы увидите, связаны ли с этим письмом какие-либо фишинговые атаки.
- Наводите курсор мыши на ссылки, чтобы убедиться в их надежности.

