Наш адрес:

Публичный центр правовой информации

Центральная районная библиотека

г. Лунинец,

ул. Фрунзе, 12

тел. 20-622

электронная почта: lncrb@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.);

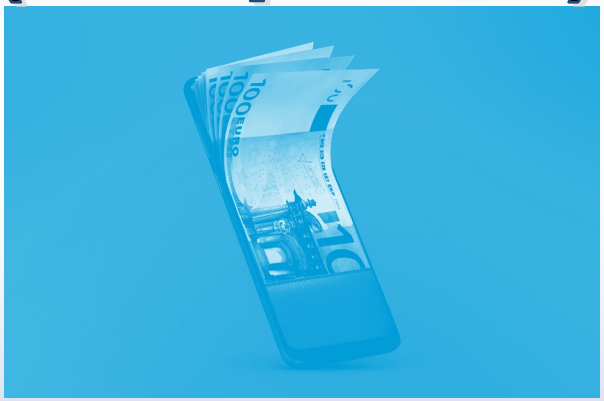
Примечание: При наличии полных сведений о документе: вид документа (закон, декрет, указ, постановление, положение и т.д.), орган принятия (Президент Республики Беларусь, Совет Министров, отраслевое министерство и т.д.), точное название, дата принятия, поиск производится бесплатно.

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

Лунинецкая центральная районная библиотека

Публичный центр правовой информации

СМИШИНГ (смс-фишинг)



Смишинг – это разновидность фишинга, когда мошенники рассылают свои сообщения не электронной почтой, а телефонными смс. Сам термин это смешение двух слов SMS и phishing, получается smishing.

В сообщение помещается Интернет-ссылка, перейдя по которой вы попадете на фишинговый сайт или на смартфон загрузится троянская программа. В любом случае результат окажется плачевным. Запомните правило: не кликать по ссылкам в сообщениях от неизвестных людей и не звонить на указанные номера.

Цель преступников — выманить у жертвы важную личную информацию, чаще всего это пароль от интернет-банка или данные банковской карты. Для этого мошенники присылают SMS, как правило, о какой-нибудь выдуманной проблеме: застрявшей посылке, неоплаченном счете или заблокированном аккаунте. Чтобы решить проблему, нужно перейти по ссылке. Дальше возможны два варианта развития событий:

- первый вариант: вас заражают зловредом, который маскируется под легитимное приложение какого-нибудь сервиса и настойчиво предлагает вбить в себя все важные данные;
- второй вариант: вас заманивают на сайт, который маскируется под легитимный сайт какого-нибудь сервиса и, ну да, предлагает вбить в себя все важные данные.

По большому счету все зависит от того, с чем данным конкретным мошенникам удобнее работать — с вредоносным ПО или сайтами. Итог для жертвы в обоих случаях одинаковый — потеря денег, нередко довольно ощутимых.

Для защиты от смишинга на телефон нужно установить мобильный антивирус, имеющий функцию сканирования входящих сообщений.

Если обнаружится интернет-ссылка на вредоносный сайт, антивирусная программа проинформирует об этом.

Можно просто игнорировать смишинг атаки, не предпринимая никаких действий. В случае реальных проблем вам перезвонят или найдут другой способ связаться лично.

Не стоит хранить на телефоне информацию о банковских картах. Если проникнет троян, он не сможет ничего украсть.