**Береги свою идентичность**

**Почему не стоит выкладывать в социальные сети фотографии на паспорт и как долго хранится в Интернете удаленная информация?**
 На эти и другие вопросы ответили участники международного семинара, посвященного теме хищения персональных данных. Встреча экспертов состоялась в Вильнюсе. Участие в ней приняли специалисты из Литвы и представители Белорусского общества защиты потребителей.

— Не все знают, что такое защита своей идентичности, — говорит заведующая юридическим отделом Государственной инспекции по защите данных Вильнюса Дангуоле Моркунене. — К нам поступает много жалоб на виртуальных мошенников, ворующих персональные данные и фальсифицирующих документы, на которые оформляются кредиты. Найти злоумышленника практически невозможно.
По словам эксперта, в поле зрения мошенников может попасть каждый. Многие носят в кошельке банковские карты и записки с указанием ПИН-кодов к ним, а, расплачиваясь по карточке в магазинах, редко прикрывают цифры кода ладонью. Банки постоянно усложняют защитные свойства карт, но правонарушители все равно находят, как обойти защиту. Например, устанавливают на банкоматах миниатюрные фотокамеры, которые снимают процесс ввода ПИН-кода, или скиммеры — специальные устройства для получения информации о карте. В качестве скиммера может выступать накладная клавиатура, очень похожая на настоящую.
*Скиммер (накладка) — устройство, предназначенное для копирования информации с магнитных полос банковских карт.*
 Как защитить свои деньги? Эксперт из Литвы советует внимательно осматривать банкомат перед тем, как вставить в него карту. Рекомендует также снимать деньги в банкоматах, расположенных в отделениях банка, и прикрывать клавиатуру рукой при вводе ПИН-кода.
Нередко потерпевшие сами передают свои персональные данные преступникам. Допустим, на мобильный телефон абонента звонит якобы ведущий радио­программы, поздравляет с крупным выигрышем и просит назвать свои контактные данные, а также выслать отсканированный образец банковской карты на электронный ящик. Многие попадаются на эту удочку, а потом удивляются обнуленным счетам.

**Обман в сети**
 — Сегодня в крупнейшей социальной сети «Фейс­бук» зарегистрирован почти 1 миллиард активных пользователей, — рассказывает эксперт Литовского института потребителей Эдита Пятраускайте. — При этом 83 миллиона аккаунтов фальшивые. Мошенники создают по несколько липовых страничек в разных социальных сетях и умело этим пользуются: «стучатся» к пользователям в друзья, а потом их обкрадывают. Средний пользователь социальной сети имеет 150 друзей. У некоторых они исчисляются тысячами, хотя, если подумать, в реальной жизни мы не приглашаем домой малознакомых людей.
Как отмечает специалист, информацию, которой вы делитесь в Интернете, нужно тщательно фильтровать, особенно если не установлено ограничение на про­смотр вашей странички. Предоставлять доступ к частным данным опасно.
— Не стоит делиться в Сети своими планами, — подчеркивает Эдита Пятраускайте. — Если планируете вечеринку, то лучше отправьте приглашение каждому из друзей лично. Не размещайте фотографии детей (для их же безопасности), свой адрес и номер телефона и, конечно же, пароли доступа к банковским счетам и страницам в соцсетях. Многие указывают место своего нахождения, демонстрируют каждый шаг, тем самым провоцируя преступников на противоправные действия.
*Многие сами сообщают мошенникам номера телефонов своих знакомых — оставляют в различных вопросниках, анкетах.*
 Эксперт также советует не выкладывать в социальных сетях фотографии на документы. С помощью специальных программ мошенники могут использовать такие снимки для изготовления фальшивых паспортов. Как показывает практика, узнать ваш идентификационный номер хакеру несложно: у них есть доступ к необходимым для этого базам данных.
Специалист говорит, что «стереть» себя из Интернета невозможно. В электронном пространстве информация останется навсегда, а опытному преступнику не составит труда поднять все данные, которые вы размещали на своей странице год назад, например.
— Тема хищения персональных данных актуальна и в нашей стране, поэтому мы с радостью согласились участвовать в литовском проекте, — отмечает председатель Белорусского общества защиты потребителей Анна Суша. — Нужно учить наших потребителей соблюдать правила безопасного пользования банковскими картами, в частности, осуществлять платежи только на проверенных сайтах, внимательно изучать условия покупки и ее отмены и, конечно же, никогда не указывать ПИН-код электронной карты при работе в Интернете.

По материалам сайта <http://bozp.by/>