ИБ-самодиагностика по пунктам

Владимир Безмалый

Похититель личных данных берёт вашу личную информацию и использует её без вашего ведома. Вор может нарастить долги или даже совершить преступления от вашего имени. Следующие советы помогут снизить риск стать жертвой.

Не попадайтесь на удочку

Мошенники обманывают жертв, выдавая себя за банки, магазины или государственные учреждения. Они делают это по телефону, по электронной и обычной почте. Не отвечайте ни на какие запросы о подтверждении номера вашей учётной записи или пароля. Законные компании не запрашивают подобную информацию таким образом.

Итог: никогда не сообщайте личную информацию, если вы не уверены в том, кто её у вас просит.

И снова о паролях

Похитители личных данных любят ваши пароли, потому что они открывают двери для вашей личной информации. Станьте крутыми и организованными. Используйте разные пароли для всех ваших учетных записей. Сделайте эти пароли надёжными, используя не менее восьми символов, включая сочетание букв, цифр и символов ($ + r0 ^ gh @ h @). Надёжно спрячьте их и держите под рукой. Хорошие пароли — это работа, но решение проблемы кражи личных данных — тяжёлый труд! Я прекрасно понимаю, что вы каждый день слышите о необходимости сложных паролей, но ничего не делаете. Что можно рекомендовать? Используйте менеджеры паролей со встроенными генераторами паролей. И главное – не используйте один и тот же пароль на разных интернет-сайтах. Другим способом парольной защиты является применение многофакторной аутентификации. При этом лучше использовать в качестве

второго фактора токен или генератор на вашем смартфоне. Но не SMS!

Меньше болтайте в социальных сетях

То, чем вы делитесь в социальных сетях (ваш домашний адрес или адрес электронной почты; имена детей, дата рождения и т. д.), — это то, что технически подкованные воры используют для мошенничества, фишинга и кражи аккаунтов. Не делитесь слишком многим.

Защитите компьютер и смартфон

Используйте надежные пароли. Используйте брандмауэр, программное обеспечение для защиты от вирусов и шпионского ПО, которое вы регулярно обновляете.

Загружайте бесплатное программное обеспечение только с сайтов, которым вы доверяете. Не устанавливайте программное обеспечение, не зная, что это такое. Не нажимайте ссылки во всплывающих окнах или в спаме.

Думайте, какие по каким ссылкам вы переходите

Делая покупки в Интернете, дважды подумайте, прежде чем вводить номер своей кредитной карты или другую личную информацию. Прочтите политику конфиденциальности и найдите возможности отказаться от обмена информацией. (Если политика конфиденциальности не опубликована, будьте осторожны! Делайте покупки в другом месте.) Вводите личную информацию только на защищённых веб-страницах с «https» в адресной строке. Это признаки того, что ваша информация будет зашифрована или зашифрована, чтобы защитить её от хакеров.

Проверьте свои утверждения

Регулярно проверяйте ваши счета и банковские выписки сразу. Внимательно проверяйте наличие любых несанкционированных списаний или снятия средств и немедленно сообщайте о них в банк. Звоните, если счета не приходят вовремя. Это может означать, что кто-то изменил

контактную информацию, чтобы скрыть мошеннические платежи.

Задавайте вопросы

Не бойтесь задавать вопросы, когда компания или агентство запрашивают вашу личную информацию. Спросите, как это будет использоваться. Спросите, как он будет распространяться и как он будет защищен. Объясните, что вас беспокоит кража личных данных. Если вас не устраивают ответы, подумайте о том, чтобы перенести свой бизнес в другое место.

https://ib-bank.ru/bisjournal/news/14396