

Утечки данных

Узнайте, что следует делать в случае утечки данных.

1. Что такое утечка данных?

Утечка данных — это нарушение безопасности, при котором конфиденциальная, частная или персональная информация копируется или похищается несанкционированным пользователем.

Злоумышленники могут завладевать информацией с целью ее продажи в даркнете или для осуществления мошеннических и фишинговых атак. Некоторые типы данных, которые пытаются похищать злоумышленники при утечке данных:

- пароли;
- электронные письма;
- финансовые данные;
- персональная информация, например номер социального страхования или адрес.

Утечки данных становятся все более распространенным явлением, и их трудно избежать. Не расстраивайтесь, если это случится с вами! Чтобы защитить свои данные и справиться с утечкой, вы можете предпринять ряд действий.

2. Защита от утечки данных

Планируйте защиту вашей информации заранее, оценив безопасность ваших персональных данных. Рекомендации по защите персональных данных в Интернете могут помочь обеспечить безопасность вашей информации и предотвратить ее рассекречивание. Используйте место на следующих двух страницах, чтобы записать свои мысли по следующим вопросам и возможные улучшения.

Надежность и уникальность ваших паролей:

Использование всех доступных средств и способов многофакторной аутентификации:

Использование менеджера паролей (помните, что существуют и бесплатные версии):

Регулярная проверка учетных записей: пользуетесь ли вы регулярно такими сервисами, как haveibeenpwned.com, чтобы проверить, не произошла ли утечка вашей информации? Составьте план действий в отношении этого в дальнейшем:

NYC Digital Safety

Privacy & Security

Минимизация данных: вы сообщаете только необходимые данные в Интернете и физическом пространстве, например в магазинах? Опишите ваш подход к сообщению данных:

3. Кто-то получил доступ к моим данным?

Проверьте следующие пункты, чтобы определить, получил ли кто-либо доступ к вашим данным:

- уведомление от источника утечки данных;
- новости (о крупных утечках часто сообщается в главных СМИ);
- подозрительные действия с учетной записью, например письма о восстановлении пароля, которые вы не запрашивали;
- ваша учетная запись показывается в результатах поиска на сайте <https://haveibeenpwned.com/>.

4. Что делать, если кто-то получил доступ к вашим данным

Сразу после этого:

- определите, какая информация была похищена;
- смените пароль;
- в случае необходимости закройте учетные записи, особенно в случае утечки данных банковских карт;
- сообщите друзьям и лицам в списке ваших контактов в случае взлома вашей электронной почты или учетной записи в социальных сетях.

NYC Digital Safety

Privacy & Security

По прошествии времени:

- остерегайтесь попыток фишинга;
- повысьте надежность паролей;
- используйте многофакторную аутентификацию;
- обратите внимание на выписки по банковским картам и действия в вашей учетной записи.

Что еще вы можете порекомендовать?