
Data Breach
Cyber Attack
КИБЕРБЕЗОПАСНОСТЬ
System Safety Compromised

Что такое кибербезопасность?

- Кибербезопасность — **это область, включающая различные аспекты защиты информации, систем и сетей от несанкционированного доступа, утечек данных, вредоносных программ и других киберугроз**.
- Цель кибербезопасности — обеспечить целостность, доступность и конфиденциальность данных в цифровой среде.

Кибербезопасность

Компьютерная безопасность

Безопасность в Интернете

Чтобы защититься от кибератак, можно использовать следующие меры:

Использовать антивирусное программное обеспечение. Антивирусы ищут и нейтрализуют вирусы, червей, трояны и другие вредоносные программы.

Использовать сетевой экран (брандмауэр или файрвол). Это шлюз, который отделяет информационную систему от интернета. Он анализирует проходящий через него трафик и ищет в нём опасности.

Регулярно обновлять программное обеспечение, устройства и плагины. В старых версиях могут быть уязвимости, которые уже устранили в новых.

Не передавать важные данные по незащищённым каналам. В таком случае даже если злоумышленник перехватит трафик, ему придётся дополнительно расшифровывать данные.

Использовать двухфакторную или многофакторную аутентификацию. Помимо пароля для получения доступа к данным нужно будет подтвердить свою личность ещё одним или несколькими способами: СМС-кодом, биометрией, специальной USB-флешкой и так далее.

Проверять ссылки, по которым переходите. Злоумышленники могут использовать фейковые сайты, которые имитируют настоящие и собирают данные. Отличить их можно по URL-адресам.

Создавать резервные копии данных. Если что-то пойдёт не так (например, заражение вирусом-вымогателем), резервная копия данных позволит восстановить всю важную информацию.

Добиться 100%-й защиты от компьютерных атак нельзя. Но если заботиться о своей информационной безопасности, шанс стать жертвой киберпреступников значительно снизится.

- Основой кибератак являются зараженные компьютеры пользователей либо зараженные серверы. В дальнейшем объединяются в сеть под управлением какого-то злоумышленника, и впоследствии они используют компьютеры жертв, чтобы рассылать спам, осуществлять хакерские атаки

Основные правила защиты от киберугроз

* 1. Не входите на незнакомые сайты.
* 2. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на вирусы.
* 3. Если пришло незнакомое вложение, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину.
* 4. Никогда не посылайте никому свой пароль.
* 5. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.
* 6. При общении в Интернет не указывать свои личные данные, а использовать псевдоним (ник).
* 7. Ни в коем случае не встречаться с людьми, с которыми познакомились в сети Интернет.
* 8. Если в сети необходимо пройти регистрацию, то должны сделать ее так, чтобы в ней не было указано никакой личной информации.
* 9. В настоящее время существует множество программ, которые производят фильтрацию содержимого сайтов. Между членами семьи должны быть доверительные отношения, чтобы вместе просматривать содержимое сайтов.
* 10. Не всей той информации, которая размещена в Интернете, можно верить.

PHISHING

Фишинг (англ. phishing от fishing — «рыбная ловля, выуживание») — вид киберпреступления, целью которого является получение доступа к конфиденциальным данным пользователей, таким как логины, пароли, номера банковских карт и другие личные данные.

Доступ достигается путём массовой рассылки поддельных электронных писем, сообщений в социальные сети или SMS, которые имитируют сообщения от известных компаний, банков или сервисов.

Виды фишинга:

Почтовый. Заключается в массовой рассылке писем с привлекательными сообщениями.
Целевой. Предполагает отправку персонализированных писем конкретным людям, представляющим ценность для мошенника.
Смишинг. Подразумевает отправку текстовых сообщений на телефон жертвы.
Вишинг. Способ голосового мошенничества, основанный на социальной инженерии и реализуемый звонком на телефон жертвы.
Фарминг. Злоумышленник изменяет запись в системе доменных имён (DNS), чтобы посетителей перенаправляли на поддельный сайт вместо подлинного.
Клон-фишинг. Заключается в отправке на электронную почту жертвы скопированного и воспроизведённого письма, которое было получено до этого от легитимного отправителя.

Социальный. Реализуется на базе популярных социальных сетей.

«Злой двойник». Фишинговая атака сводится к созданию поддельной копии WiFi-сети, куда заманивают жертв бесплатным интернетом и доступом к сетевым ресурсам, после чего происходит кража данных учётных записей пользователей.

Поисковой фишинг. Злоумышленники создают сайты-однодневки, копирующие продукцию известных брендов.

Чтобы не стать жертвой фишинга, рекомендуется не переходить по ссылкам напрямую, проверять достоверность информации на официальном сайте компании или по её каналам, использовать инструменты защиты, такие как антивирусные программы, файерволы и спам-фильтры.

Спасибо за внимание!